Consiglio dell'Unione europea

Bruxelles, 6 giugno 2025
(OR. en)

9794/25

Fascicolo interistituzionale: 2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	6 giugno 2025
Destinatario:	Delegazioni
Oggetto:	Raccomandazione del Consiglio relativa a un programma dell'UE per la gestione delle crisi informatiche - Raccomandazione del Consiglio approvata dal Consiglio nella sessione del 6 giugno 2025

Si allega per le delegazioni la raccomandazione del Consiglio in oggetto, approvata dal Consiglio nella sessione del 6 giugno 2025.

ALLEGATO

RACCOMANDAZIONE DEL CONSIGLIO

relativa a un programma dell'UE per la gestione delle crisi informatiche

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 114 e 292,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) La tecnologia digitale e la connettività globale rappresentano la colonna portante della crescita economica, della competitività e della trasformazione delle infrastrutture critiche dell'Unione. Tuttavia, con un'economia interconnessa e sempre più digitale aumenta anche il rischio di incidenti di cibersicurezza e attacchi informatici. Inoltre, le crescenti tensioni geopolitiche, i conflitti e la rivalità strategica si riflettono nell'impatto, nel volume e nella sofisticazione delle attività informatiche dolose. Tali attività possono far parte di campagne ibride o di operazioni militari. Possono anche incidere direttamente sulla sicurezza, sull'economia e sulla società dell'Unione. Inoltre, possono avere effetti di ricaduta, in particolare quando sono destinate a paesi partner strategici internazionali come i paesi candidati o limitrofi.

(2) Un incidente di cibersicurezza su vasta scala può causare un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o ha un impatto significativo su più di uno Stato membro. Un simile incidente, a seconda della sua causa e del relativo impatto, potrebbe degenerare e trasformarsi in una vera e propria crisi che compromette il corretto funzionamento del mercato interno o che comporta gravi rischi di pubblica sicurezza per soggetti o cittadini in diversi Stati membri o nell'intera Unione. Una gestione efficace delle crisi è essenziale per mantenere la stabilità economica e proteggere i governi, le infrastrutture critiche, le imprese e i cittadini europei, nonché per contribuire alla sicurezza e alla stabilità internazionali nel ciberspazio. La gestione delle crisi informatiche è pertanto parte integrante del quadro generale dell'UE per la gestione delle crisi.

(3) Date le interdipendenze e le interconnessioni tra gli ambienti TIC dei soggetti dell'Unione e quelli degli Stati membri, un incidente in un soggetto dell'Unione potrebbe comportare un rischio di cibersicurezza per gli Stati membri e viceversa. La condivisione di informazioni pertinenti e il coordinamento in relazione sia agli incidenti di cibersicurezza su vasta scala che agli incidenti gravi, quali definiti all'articolo 3, punto 8), del regolamento (UE, Euratom) 2023/2841[1], sono fondamentali nel contesto del programma dell'UE per la gestione delle crisi informatiche ("programma per la cibersicurezza").

[1] Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (GU L, 2023/2841, 18.12.2023, pag. 1).

(4) In caso di crisi per la quale sono stati attivati i dispositivi integrati dell'UE per la risposta politica alle crisi ("IPCR") a norma della decisione di esecuzione (UE) 2018/1993 del Consiglio[2] ("dispositivi IPCR"), il programma per la cibersicurezza dovrebbe rispettare pienamente i dispositivi IPCR per il coordinamento e la risposta. Il coordinamento politico e strategico si svolgerebbe nell'ambito degli IPCR. I dispositivi IPCR sono lo strumento per il coordinamento orizzontale e la risposta a livello politico dell'Unione. In conformità dei dispositivi IPCR, la decisione di attivare o disattivare gli IPCR è adottata dalla presidenza del Consiglio dell'Unione europea. Le relazioni sulla conoscenza e l'analisi integrate della situazione ("ISAA") elaborate dai servizi della Commissione e dal servizio europeo per l'azione esterna ("SEAE") sostengono il lavoro degli IPCR in entrambe le modalità previste, vale a dire scambio di informazioni e piena attivazione.

(5) Gli Stati membri hanno la responsabilità primaria della gestione degli incidenti di cibersicurezza e delle crisi informatiche. Tuttavia, la potenziale natura transfrontaliera e intersettoriale degli incidenti di cibersicurezza impone agli Stati membri e ai pertinenti soggetti dell'Unione di cooperare a livello tecnico, operativo e politico per coordinarsi efficacemente in tutta l'Unione. La gestione delle crisi informatiche durante l'intero ciclo richiede preparazione e conoscenza situazionale condivisa per anticipare gli incidenti di cibersicurezza su vasta scala, le dovute capacità di individuazione per identificare gli strumenti di risposta e ripristino necessari ai fini della mitigazione e del contenimento di tali incidenti, nonché capacità di reazione ai fini della deterrenza e della prevenzione di ulteriori incidenti.

[2] Decisione di esecuzione (UE) 2018/1993 del Consiglio, dell'11 dicembre 2018, relativa ai dispositivi integrati dell'UE per la risposta politica alle crisi (GU L 320 del 17.12.2018, pag. 28).

(6) La raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala[3] ha definito gli obiettivi e le modalità di cooperazione tra gli Stati membri e i soggetti dell'Unione nella risposta agli incidenti di cibersicurezza su vasta scala e alle crisi informatiche. Ha realizzato una mappatura degli attori pertinenti a livello tecnico, operativo e politico e ha spiegato in che modo sono stati integrati nei meccanismi esistenti di gestione delle crisi dell'Unione, come i dispositivi IPCR. I principi fondamentali stabiliti nella raccomandazione (UE) 2017/1584 restano validi, segnatamente la sussidiarietà, la complementarità e la riservatezza delle informazioni, nonché l'approccio a tre livelli (tecnico, operativo e politico). La presente raccomandazione si basa su tali principi fondamentali ed è intesa a sostituire la raccomandazione (UE) 2017/1584, istituendo un nuovo quadro dell'Unione per la gestione delle crisi di cibersicurezza.

(7) Alcune definizioni utilizzate nella presente raccomandazione si basano su definizioni e termini utilizzati nella direttiva (UE) 2022/2555[4]. Tuttavia, l'ambito di applicazione della presente raccomandazione è diverso da quello della direttiva (UE) 2022/2555. La presente raccomandazione definisce il quadro dell'Unione per la gestione delle crisi di cibersicurezza nel contesto della preparazione generale dell'UE agli incidenti di cibersicurezza su vasta scala e alle crisi informatiche derivanti da tali incidenti, a prescindere dal settore o dal soggetto interessato. Nella misura del possibile, le definizioni si basano su quelle contenute nella direttiva (UE) 2022/2555.

---

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

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

(8) Un programma per la cibersicurezza aggiornato è necessario per fornire orientamenti chiari e accessibili che spieghino in cosa consiste un incidente di cibersicurezza su vasta scala o una crisi informatica a livello dell'Unione, in che modo è attivato il quadro di gestione delle crisi e quali sono i ruoli delle reti, degli attori e dei meccanismi pertinenti a livello dell'Unione, nonché qual è l'interazione tra tali attori e meccanismi durante l'intero ciclo della crisi informatica. Il programma per la cibersicurezza mira a sostenere il più ampio quadro delle relazioni civili-militari dell'UE nell'ambito della gestione delle crisi informatiche, anche nel contesto dell'approfondimento delle relazioni UE-NATO, ove possibile anche attraverso meccanismi rafforzati di condivisione delle informazioni inclusivi, reciproci e non discriminatori nella gestione delle crisi informatiche.

(9) La gestione intersettoriale delle crisi a livello dell'Unione dovrebbe essere rafforzata per consentire una risposta integrata alle crisi, in particolare nei casi in cui gli incidenti e le crisi di cibersicurezza su vasta scala causano conseguenze fisiche. La presente raccomandazione integra i dispositivi IPCR e altri meccanismi di gestione delle crisi dell'Unione, tra cui il sistema generale di allarme rapido della Commissione ARGUS, il meccanismo unionale di protezione civile ("UCPM") sostenuto dal Centro di coordinamento della risposta alle emergenze ("ERCC"), istituito nell'ambito dell'UCPM dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio su un meccanismo unionale di protezione civile[5] ("decisione UCPM"), il meccanismo di risposta alle crisi ("CRM") del SEAE, nonché altri processi, come quelli descritti nel pacchetto di strumenti della diplomazia informatica dell'UE[6], nel pacchetto di strumenti contro le minacce ibride[7] e nel protocollo riveduto dell'UE per contrastare le minacce ibride[8]. Inoltre, integra la raccomandazione (UE) 2024/4371 del Consiglio relativa a un programma per coordinare una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera[9] ("programma UE per le infrastrutture critiche"), che riguarda la resilienza fisica non informatica e mira a migliorare il coordinamento della risposta a livello dell'Unione in questo settore, e dovrebbe essere coerente con la stessa.

---

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

6 Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose (doc. 9916/17).

7 Conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride (22 giugno 2022).

8 Documento di lavoro congiunto dei servizi – Protocollo dell'UE per contrastare le minacce ibride (SWD(2023) 116 final).

9 GU C, C/2024/4371, 5.7.2024.

(10) La rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe") è la rete per il coordinamento della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala a livello operativo, anche in caso di incidenti di cibersicurezza su vasta scala e crisi informatiche a livello intersettoriale. Per non complicare ulteriormente i quadri esistenti, è opportuno evitare la creazione di strutture settoriali che duplicherebbero i compiti di EU-CyCLONe. EU-CyCLONe dovrebbe ricevere informazioni operative relative alla cibersicurezza anche dai settori e trasmetterle al livello politico.

(11) Si incoraggiano gli Stati membri a utilizzare appieno le risorse finanziarie disponibili per la cibersicurezza previste dai pertinenti programmi dell'Unione. È opportuno fare in modo che tali programmi impongano oneri amministrativi minimi ai richiedenti il finanziamento e che la partecipazione degli Stati membri a tali programmi sia agevolata fornendo orientamenti pertinenti sulle opzioni di sostegno finanziario praticabili.

(12) La presente raccomandazione contribuisce alle più ampie azioni di preparazione necessarie affinché l'Unione possa far fronte a crisi intersettoriali, in linea con i principi integrati nella strategia dell'UE in materia di preparazione, vale a dire un approccio integrato multirischio, esteso a tutta l'amministrazione e a tutta la società, in particolare per quanto riguarda il miglioramento della consapevolezza dei rischi e delle minacce nonché della risposta intersettoriale alle crisi,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

I: obiettivo, ambito di applicazione e principi guida del quadro per la gestione delle crisi informatiche dell'UE

Obiettivo e ambito di applicazione

1) La presente raccomandazione relativa a un programma dell'UE per la gestione delle crisi informatiche ("programma per la cibersicurezza") stabilisce il quadro dell'Unione per la gestione delle crisi di cibersicurezza nel contesto della preparazione generale dell'UE agli incidenti di cibersicurezza su vasta scala e alle crisi informatiche. Il quadro riflette i ruoli sia degli Stati membri che delle istituzioni, degli organi e degli organismi dell'Unione ("soggetti dell'Unione") nell'ambito delle rispettive competenze, nel pieno rispetto del diritto nazionale e delle norme interne, al fine di garantire un'azione globale e coordinata a livello dell'Unione.

2) Il programma per la cibersicurezza dovrebbe essere applicato coerentemente con il programma UE per le infrastrutture critiche, in particolare in caso di incidenti che interessano sia la resilienza fisica che la cibersicurezza delle infrastrutture critiche[10].

3) Il programma per la cibersicurezza fornisce orientamenti per la risposta agli incidenti di cibersicurezza su vasta scala o alle crisi informatiche e dovrebbe essere utilizzato in complementarità con i pertinenti meccanismi settoriali di risposta, come quelli elencati nell'allegato II. I pertinenti portatori di interessi in materia di cibersicurezza dovrebbero fornire aiuto e assistenza nel conseguimento degli obiettivi di tali meccanismi settoriali, a livello sia nazionale che dell'Unione.

4) Nel caso di una crisi intersettoriale a livello dell'UE che presenta aspetti informatici e per la quale sono attivati gli IPCR, il coordinamento della risposta a livello politico dell'Unione dovrebbe essere effettuato dal Consiglio, ricorrendo ai dispositivi IPCR. Una volta attivati gli IPCR, le misure nell'ambito del programma per la cibersicurezza dovrebbero sostenere la risposta dell'UE a livello politico, fornendo un sostegno specifico in materia di cibersicurezza.

---

[10] Il programma UE per le infrastrutture critiche precisa ulteriormente il coordinamento in tali casi nella parte I, sezione 4, del suo allegato.

Principi guida

5) Alla gestione delle crisi informatiche a livello dell'Unione si applicano i principi guida seguenti.

a) *Proporzionalità*: la maggior parte degli incidenti di cibersicurezza che interessano gli Stati membri ha una portata inferiore a quella che permetterebbe di considerarli alla stregua di un incidente di cibersicurezza su vasta scala o di una crisi informatica a livello nazionale o dell'Unione. In caso di incidenti di cibersicurezza e minacce alla cibersicurezza, gli Stati membri cooperano e scambiano informazioni, su base volontaria e con cadenza regolare, nell'ambito della rete di gruppi di intervento per la sicurezza informatica in caso di incidente ("rete di CSIRT") e di EU-CyCLONe, in linea con le procedure operative standard ("POS") delle reti.

b) *Sussidiarietà*: gli Stati membri hanno la responsabilità primaria di risposta e ripristino in caso di incidente di cibersicurezza, di incidente di cibersicurezza su vasta scala o di crisi informatica che li riguardi. Alla luce dei potenziali effetti transfrontalieri, il Consiglio, la Commissione, l'alto rappresentante, l'Agenzia dell'Unione europea per la cibersicurezza ("ENISA"), il servizio per la cibersicurezza delle istituzioni, degli organi e degli organismi dell'Unione ("CERT-UE"), Europol e tutti gli altri soggetti pertinenti dell'Unione dovrebbero cooperare durante l'intero ciclo della crisi. Tale ruolo deriva dal diritto dell'Unione e riflette il modo in cui gli incidenti di cibersicurezza su vasta scala e le crisi informatiche si ripercuotono su uno o più settori dell'attività economica nel mercato unico, sulla sicurezza e sulle relazioni internazionali dell'Unione, nonché sui soggetti stessi dell'Unione.

c) *Complementarietà*: la presente raccomandazione tiene pienamente conto dei meccanismi di gestione delle crisi esistenti a livello dell'Unione elencati nell'allegato II, segnatamente i dispositivi IPCR, ARGUS e il CRM del SEAE. La presente raccomandazione tiene conto dei mandati della rete di CSIRT e di EU-CyCLONe nonché del regolamento (UE, Euratom) 2023/2841. In caso di attivazione degli IPCR, il lavoro delle pertinenti reti ed entità e dei pertinenti meccanismi settoriali attivati dovrebbe proseguire e confluire nel coordinamento politico e strategico che si svolge nell'ambito degli IPCR, sostenendolo.

d) *Riservatezza delle informazioni*: tutti gli scambi di informazioni nel contesto della presente raccomandazione dovrebbero essere conformi alle norme applicabili in materia di sicurezza e di protezione dei dati personali. Se del caso, dovrebbero essere presi in considerazione accordi di non divulgazione informali quali il protocollo TLP (*Traffic Light Protocol*) per contrassegnare le informazioni sensibili. Per lo scambio di informazioni classificate, indipendentemente dal sistema di classificazione applicato, si dovrebbero utilizzare le norme e gli accordi vincolanti esistenti in materia di trattamento delle informazioni classificate, oltre agli strumenti accreditati disponibili.

6) Conformemente ai principi guida summenzionati, gli Stati membri e i soggetti dell'Unione dovrebbero approfondire la loro cooperazione in materia di gestione delle crisi informatiche, promuovendo la fiducia reciproca e prendendo le mosse dalle reti e dai meccanismi esistenti. Tale cooperazione, nel quadro del programma per la cibersicurezza, beneficia dell'attuazione degli articoli 22 e 23 del regolamento (UE, Euratom) 2023/2841. In particolare, il piano di gestione delle crisi informatiche istituito sulla base dell'articolo 23 del regolamento (UE, Euratom) 2023/2841 contribuisce, tra l'altro, allo scambio regolare di informazioni pertinenti tra i soggetti dell'Unione e con gli Stati membri e stabilisce disposizioni relative al coordinamento e al flusso di informazioni tra i soggetti dell'Unione.

II: definizioni

7) Ai fini del presente programma per la cibersicurezza si applicano le definizioni seguenti:

a) "incidente": un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

b) "incidente significativo": un incidente che:

   a. ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

   b. si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli;

c) "incidente di cibersicurezza su vasta scala": un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

d) "crisi informatica": un incidente di cibersicurezza su vasta scala che degenera in una vera e propria crisi che non consente il corretto funzionamento del mercato interno, o che comporta gravi rischi di pubblica sicurezza per soggetti o cittadini in diversi Stati membri o nell'intera Unione.

III: strutture nazionali di gestione delle crisi informatiche e responsabilità

8) Gli Stati membri hanno la responsabilità primaria di risposta in caso di incidenti di cibersicurezza su vasta scala o di crisi informatiche che li riguardino. In linea con la direttiva (UE) 2022/2555, ciascuno Stato membro dispone di una o più autorità di gestione delle crisi informatiche, nonché di uno o più CSIRT.

9) Con l'adozione della direttiva (UE) 2022/2555 e di altri strumenti legislativi e non legislativi in materia di cibersicurezza, gli Stati membri stanno allineando i rispettivi quadri di cibersicurezza stabilendo norme minime concernenti il funzionamento del quadro normativo coordinato, istituendo meccanismi per una cooperazione efficace tra le autorità responsabili di ciascuno Stato membro e fornendo azioni correttive e misure di esecuzione efficaci, che sono fondamentali per l'effettiva applicazione di tali obblighi.

10) Conformemente all'articolo 9, paragrafo 4, della direttiva (UE) 2022/2555, gli Stati membri dovrebbero adottare piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala. Tali piani comprendono, tra l'altro, misure nazionali di preparazione, procedure di gestione delle crisi informatiche e procedure nazionali e accordi tra gli organismi e le autorità nazionali al fine di garantire il loro sostegno e la loro partecipazione effettivi alla gestione coordinata degli incidenti di cibersicurezza su vasta scala e delle crisi informatiche a livello dell'Unione. Le procedure di gestione delle crisi informatiche includono anche disposizioni sulla loro integrazione nel quadro nazionale generale di gestione delle crisi e i canali di scambio di informazioni.

11) Conformemente all'articolo 9, paragrafo 1, della direttiva (UE) 2022/2555, gli Stati membri dovrebbero assicurare la coerenza con i quadri nazionali esistenti di gestione generale delle crisi. In caso di attivazione degli IPCR, le autorità nazionali di gestione delle crisi dovrebbero, al fine di informare gli IPCR, raccogliere contributi dalle autorità di gestione delle crisi informatiche e dai meccanismi settoriali nazionali di gestione delle crisi.

12) Conformemente all'articolo 9, paragrafo 5, della direttiva (UE) 2022/2555, su richiesta di uno Stato membro interessato, EU-CyCLONe dovrebbe scambiare informazioni sulle parti pertinenti dei piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, in particolare sulle disposizioni volte a garantire il sostegno e la partecipazione effettivi alla gestione coordinata degli incidenti di cibersicurezza su vasta scala e delle crisi informatiche a livello dell'Unione, al fine di scambiare migliori pratiche e valutare il funzionamento del quadro generale nella pratica.

13) EU-CyCLONe e il comitato interistituzionale per la cibersicurezza ("IICB") sono invitati a tenere scambi, se del caso, in merito alla coerenza del piano di gestione delle crisi stabilito dall'IICB conformemente all'articolo 23 del regolamento (UE, Euratom) 2023/2841 con i piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala.

14) EU-CyCLONe, con il sostegno dell'ENISA in qualità di segretariato, dovrebbe tenere un elenco aggiornato delle autorità nazionali di gestione delle crisi informatiche corredato dei recapiti dei funzionari e dei dirigenti di EU-CyCLONe e metterlo a disposizione dei membri di EU-CyCLONe.

IV: reti e attori principali nell'ecosistema dell'UE di gestione delle crisi informatiche

15) La rete di CSIRT è la principale rete tecnica per lo scambio di informazioni pertinenti sugli incidenti, in particolare nell'ambito di applicazione della presente raccomandazione, conformemente ai compiti pertinenti di cui all'articolo 15, paragrafo 3, della direttiva (UE) 2022/2555. Contribuisce allo sviluppo della fiducia e promuove una cooperazione operativa rapida ed efficace fra gli Stati membri. Il presidente della rete di CSIRT può partecipare all'IICB in qualità di osservatore.

16) Il CERT-UE è il servizio di cibersicurezza per tutti i soggetti dell'Unione. Il CERT-UE funge da piattaforma per lo scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti per i soggetti dell'Unione conformemente all'articolo 13 del regolamento (UE) 2023/2841. Il CERT-UE è membro della rete di CSIRT e sostiene la Commissione nell'ambito di EU-CyCLONe. Il CERT-UE opera a livello tecnico ed è responsabile del coordinamento della gestione degli incidenti gravi che colpiscono i soggetti dell'Unione.

17) EU-CyCLONe funge da intermediario tra il livello tecnico e politico, in particolare durante gli incidenti di cibersicurezza su vasta scala e le crisi informatiche. Sostiene la gestione coordinata a livello operativo degli incidenti di cibersicurezza su vasta scala e delle crisi informatiche e garantisce il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione, conformemente all'articolo 16 della direttiva (UE) 2022/2555. Il presidente di EU-CyCLONe può partecipare all'IICB in qualità di osservatore.

18) L'ENISA è l'agenzia dell'Unione che svolge i compiti attribuitile ai sensi del regolamento (UE) 2019/881[11] allo scopo di conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione. L'ENISA svolge, tra l'altro, le funzioni di segretariato della rete di CSIRT e di EU-CyCLONe, presta servizi in materia di conoscenza situazionale e assiste gli Stati membri organizzando periodicamente esercitazioni di cibersicurezza a livello dell'Unione. Conformemente alla direttiva (UE) 2022/2555 e al regolamento (UE) 2024/2847[12], l'ENISA riceve informazioni sugli incidenti significativi transfrontalieri e sulle vulnerabilità attivamente sfruttate e gli incidenti che incidono sui prodotti digitali.

19) Il Consiglio dell'Unione europea ("Consiglio") è l'istituzione che, a norma dell'articolo 16 del trattato sull'Unione europea ("TUE"), esercita funzioni di definizione delle politiche e di coordinamento, ed è incaricato degli IPCR, che riguardano il coordinamento e la risposta a livello politico dell'Unione. Il Consiglio opera attraverso le formazioni del Consiglio, il Comitato dei rappresentanti permanenti e i pertinenti organi preparatori del Consiglio, in particolare il gruppo orizzontale "Questioni riguardanti il ciberspazio", nonché, se del caso, i dispositivi IPCR.

---

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

[12] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, pag.1).

20) La Commissione, in quanto istituzione che promuove l'interesse generale dell'Unione, adotta iniziative appropriate a tal fine e assicura l'applicazione dei trattati e delle misure adottate dalle istituzioni a norma dell'articolo 17 TUE, è responsabile di determinate azioni di preparazione generali a livello dell'Unione e di determinate azioni di conoscenza situazionale, compresa la gestione dell'ERCC e del sistema comune di comunicazione e informazione in caso di emergenza ("CECIS"), in linea con la decisione UCPM. Facilita la coerenza delle azioni di risposta alle crisi a livello dell'Unione collegate e il loro coordinamento a livello operativo. Viene consultata in merito alle decisioni di attivare o disattivare gli IPCR. I servizi della Commissione elaborano, insieme al SEAE, le relazioni ISAA. La Commissione è membro di EU-CyCLONe nei casi in cui un incidente di cibersicurezza su vasta scala, potenziale o in corso, abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555 e negli altri casi partecipa in qualità di osservatore. È il punto di contatto per EU-CyCLONe presso l'IICB. Svolge il ruolo di osservatore presso la rete di CSIRT.

21) L'alto rappresentante per gli affari esteri e la politica di sicurezza ("alto rappresentante"), con l'assistenza del SEAE, guida la politica estera e di sicurezza comune ("PESC") dell'Unione e contribuisce con le sue proposte all'elaborazione di detta politica, compresa la politica di sicurezza e di difesa comune ("PSDC"). Ciò comprende strutture e meccanismi diplomatici, di intelligence e militari, in particolare la capacità unica di analisi dell'intelligence ("SIAC") quale punto di accesso unico per l'intelligence degli Stati membri, lo Stato maggiore dell'UE ("EUMS") come fonte di consulenza militare, il pacchetto di strumenti della diplomazia informatica dell'UE nonché la rete delle delegazioni dell'UE, che possono contribuire alla gestione delle crisi da una dimensione esterna. Il SEAE inoltre elabora, insieme alla Commissione, le relazioni ISAA.

22) L'allegato II descrive i ruoli e le competenze dei pertinenti attori a livello dell'Unione in relazione alla gestione delle crisi informatiche, compresi le reti e gli attori principali.

V: preparazione a incidenti di cibersicurezza su vasta scala e a una crisi informatica

Panorama delle minacce

23) Gli Stati membri e i soggetti pertinenti dell'Unione dovrebbero adottare le misure necessarie per migliorare la conoscenza situazionale, riconoscendo che il panorama delle minacce e la conoscenza situazionale specifica per gli incidenti richiedono modalità operative distinte. Gli Stati membri e i soggetti pertinenti dell'Unione dovrebbero collaborare sulla base di dati verificati e affidabili, comprese le tendenze in materia di incidenti, tattiche, tecniche e procedure, nonché le vulnerabilità attivamente sfruttate.

24) Nel condividere informazioni a livello dell'UE, gli Stati membri dovrebbero sfruttare appieno le piattaforme esistenti per la cooperazione tecnica e operativa, come quelle utilizzate dalla rete di CSIRT e da EU-CyCLONe.

25) Al fine di migliorare la conoscenza situazionale condivisa e facilitare la valutazione dell'impatto dell'UE, EU-CyCLONe e la rete di CSIRT, con il sostegno dell'ENISA, dovrebbero utilizzare un meccanismo di segnalazione concordato internamente per tracciare una panoramica UE delle attività tecniche e operative sulla base delle informazioni raccolte a livello nazionale.

26) EU-CyCLONe e la rete di CSIRT dovrebbero:

a) cooperare per migliorare la condivisione delle informazioni tra il livello tecnico e operativo e la conoscenza situazionale nel suo complesso;

b) continuare a creare un clima di fiducia tra i rispettivi membri e tra le reti;

c) sfruttare appieno gli strumenti disponibili per la condivisione delle informazioni, con il sostegno dell'ENISA, riflettere su come migliorare tali strumenti e garantire l'interoperabilità tra le reti.

27) EU-CyCLONe, la rete di CSIRT e l'IICB dovrebbero cooperare per garantire uno scambio efficace delle informazioni pertinenti.

28) L'ENISA, in qualità di segretariato della rete di CSIRT e di EU-CyCLONe, svolge un ruolo centrale nel sostenere gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione al fine di conseguire una conoscenza situazionale comune dell'UE a livello tecnico e operativo per sostenere la preparazione agli incidenti e alle crisi di cibersicurezza su vasta scala.

29) Conformemente alla direttiva (UE) 2022/2555 e al regolamento (UE) 2019/881, gli Stati membri e i pertinenti soggetti dell'Unione dovrebbero coordinarsi con il settore privato, comprese le comunità open source e i produttori, al fine di migliorare la condivisione delle informazioni. In particolare, l'ENISA dovrebbe utilizzare il proprio programma di partenariato a tale riguardo. Inoltre, gli Stati membri e i soggetti pertinenti dell'Unione potrebbero anche basarsi sui centri di condivisione e di analisi delle informazioni ("ISAC") attualmente esistenti a livello nazionale e dell'UE per rafforzare la capacità di cibersicurezza e rispondere agli incidenti di cibersicurezza, anche attraverso riunioni congiunte tra il settore privato e EU- CyCLONe o la rete di CSIRT.

30) Per migliorare la condivisione delle informazioni all'interno delle reti e tra di esse, come anche per chiarire le aspettative reciproche riguardo a tale condivisione, entro 24 mesi dall'adozione della presente raccomandazione EU-CyCLONe dovrebbe concordare una tassonomia comune allineata dei livelli di gravità degli incidenti, con il sostegno dell'ENISA in qualità di segretariato e previa consultazione della rete di CSIRT e del gruppo di cooperazione NIS. Tale tassonomia dovrebbe permettere di comparare la gravità degli incidenti tra gli Stati membri tenendo conto dell'impatto sulla prestazione dei servizi, del numero di soggetti interessati e della loro rispettiva rilevanza, dell'impatto su altri servizi e infrastrutture, nonché dei danni monetari, reputazionali e politici inflitti. Dovrebbe basarsi su scale o tassonomie esistenti pertinenti, come la tassonomia di riferimento per la classificazione degli incidenti.

Livello tecnico

31) La rete di CSIRT è la piattaforma per la cooperazione tecnica e la condivisione di informazioni tra tutti gli Stati membri e, attraverso il CERT-UE, con i soggetti dell'Unione.

32) Conformemente alla direttiva (UE) 2022/2555, ciascun CSIRT ha il compito di monitorare e analizzare le minacce informatiche, le vulnerabilità e gli incidenti a livello nazionale. I CSIRT dovrebbero scambiarsi, sia all'interno della rete di CSIRT che a livello bilaterale, informazioni pertinenti relative a incidenti, quasi incidenti, minacce informatiche, rischi e vulnerabilità per conseguire una conoscenza situazionale condivisa.

33) Al fine di rafforzare la cooperazione operativa a livello di Unione, la rete di CSIRT dovrebbe prendere in considerazione la possibilità di invitare a partecipare ai suoi lavori organismi e agenzie dell'Unione coinvolti nella politica in materia di cibersicurezza, quali Europol.

34) Ai sensi del regolamento (UE) 2023/2841, il CERT-UE dovrebbe raccogliere, gestire, analizzare e condividere informazioni con le istituzioni, gli organi e gli organismi dell'Unione sulle minacce informatiche, le vulnerabilità e gli incidenti riguardanti le infrastrutture TIC non riservate e, se necessario, presentare all'IICB proposte specifiche di indirizzi e raccomandazioni destinati alle istituzioni, agli organi e agli organismi dell'Unione. Il CERT-UE dovrebbe cooperare e scambiare informazioni con omologhi degli Stati membri, anche attraverso la rete di CSIRT.

Livello operativo

35) Conformemente alla direttiva (UE) 2022/2555, EU-CyCLONe dovrebbe fungere da piattaforma per la cooperazione tra le autorità di gestione delle crisi informatiche degli Stati membri e, attraverso la Commissione, con i soggetti pertinenti dell'Unione, al fine di aumentare il livello di preparazione per la gestione di incidenti di cibersicurezza su vasta scala e crisi informatiche e di sviluppare una conoscenza situazionale condivisa in merito agli incidenti di cibersicurezza su vasta scala e alle crisi informatiche.

36) Conformemente alla direttiva (UE) 2022/2555 e al regolamento (UE) 2024/2847, l'ENISA riceve informazioni sugli incidenti significativi transfrontalieri e sulle vulnerabilità attivamente sfruttate e gli incidenti che incidono sui prodotti digitali. L'ENISA, che funge da segretariato, dovrebbe fornire consulenza alla rete di CSIRT e a EU-CyCLONe con l'obiettivo di sostenere le reti nel valutare l'opportunità di intraprendere ulteriori azioni e contribuire alla conoscenza situazionale condivisa.

Livello politico

37) Gli Stati membri e i pertinenti soggetti dell'Unione dovrebbero monitorare gli sviluppi internazionali che incidono sulla cibersicurezza (comprese le minacce informatiche, le minacce ibride e la manipolazione delle informazioni e le ingerenze da parte di attori stranieri (*foreign information manipulation and interference* – "FIMI"), compresa la disinformazione, se del caso). Dovrebbero essere prese in considerazione iniziative quali le relazioni di valutazione congiunta per il ciberspazio ("J-CAR"), le analisi fornite dalla SIAC e altri prodotti pertinenti che forniscono indicazioni specializzate.

38) L'alto rappresentante dovrebbe continuare a informare gli Stati membri e a coinvolgerli per quanto riguarda gli sforzi diplomatici dell'Unione in materia di minacce informatiche, in particolare quelle che interessano attori statali, il suo dialogo con i paesi terzi e le organizzazioni internazionali, compresa la NATO, e l'attuazione di misure diplomatiche, comprese le misure restrittive.

39) La presidenza del Consiglio dell'Unione europea può creare una pagina dedicata al monitoraggio sulla piattaforma web IPCR nella quale gli Stati membri e le istituzioni e gli organi dell'UE possono scambiare informazioni su una crisi che potrebbe svilupparsi.

Esercitazioni comuni

40) La Commissione, in coordinamento con l'alto rappresentante, con il sostegno dell'ENISA e previa consultazione di EU-CyCLONe e della rete di CSIRT, dovrebbe elaborare un efficiente programma continuo annuale di esercitazioni informatiche per prepararsi alle crisi informatiche e migliorare l'efficienza organizzativa. Il programma continuo di esercitazioni informatiche dovrebbe tenere conto delle esercitazioni dell'UCPM e di altre esercitazioni di meccanismi di risposta alle crisi a livello dell'Unione, compresa l'esercitazione descritta nel programma UE per le infrastrutture critiche. Il primo programma continuo dovrebbe essere elaborato entro 12 mesi dall'adozione del programma per la cibersicurezza e i programmi successivi dovranno essere completati entro il 31 marzo di ogni anno. Il programma continuo dovrebbe essere presentato al Consiglio per informazione.

41) Il programma continuo dovrebbe comprendere anche esercitazioni sviluppate utilizzando gli scenari derivanti da valutazioni dei rischi coordinate a livello dell'UE, come pure esercitazioni che coinvolgano tutti gli attori pertinenti, in particolare il settore privato e la NATO.

42) L'ENISA, nel suo ruolo di segretariato della rete di CSIRT e di EU-CyCLONe, dovrebbe provvedere alla raccolta sistematica degli insegnamenti tratti dalle esercitazioni, come pure all'individuazione delle azioni che ne derivano, e proporre modalità di attuazione di tali azioni al fine di garantirne l'effettiva esecuzione e l'impatto positivo sulla resilienza comune dell'UE, comprese le rispettive POS.

43) Tutti gli attori e tutte le reti dovrebbero migliorare il coordinamento in caso di incidente di cibersicurezza su vasta scala o di crisi informatica sulla base degli insegnamenti tratti dalle esercitazioni. In particolare, EU-CyCLONe e la rete di CSIRT dovrebbero affrontare le sfide individuate durante le esercitazioni per migliorare il coordinamento, soprattutto quelle riguardanti la cooperazione tra le reti, e, se necessario, adeguare rapidamente le POS.

44) Il gruppo di cooperazione NIS dovrebbe invitare la rete di CSIRT, EU-CyCLONe e l'ENISA a presentare gli insegnamenti tratti dalle esercitazioni, come pure l'individuazione delle azioni che ne derivano e le modalità proposte di attuazione di tali azioni.

45) Il Consiglio può invitare i presidenti della rete di CSIRT, di EU-CyCLONe, del gruppo di cooperazione NIS e dell'ENISA a presentare le modalità di attuazione degli insegnamenti tratti dalle esercitazioni.

46) L'ENISA, in cooperazione con la Commissione e l'alto rappresentante, è invitata a organizzare un'esercitazione per testare il programma per la cibersicurezza durante la prossima esercitazione Cyber Europe. L'esercitazione dovrebbe coinvolgere tutti gli attori pertinenti, compreso il livello politico. L'ENISA è invitata a coordinare con la presidenza del Consiglio dell'Unione europea il coinvolgimento del livello politico. L'esercitazione può includere anche il settore privato e la NATO.

VI: individuazione di un incidente che potrebbe degenerare in un incidente di cibersicurezza su vasta scala o in una crisi informatica

47) Conformemente ai rispettivi mandati e sulla base dell'approccio multirischio, tutti gli attori dovrebbero fornire alle reti pertinenti informazioni che indicano un potenziale incidente di cibersicurezza su vasta scala o una potenziale crisi informatica.

48) In conformità del regolamento (UE) 2025/38[13], quando ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, i poli informatici transfrontalieri dovrebbero garantire, ai fini della conoscenza situazionale comune, che le informazioni pertinenti siano fornite senza indebito ritardo alle autorità degli Stati membri e alla Commissione attraverso EU-CyCLONe e la rete di CSIRT.

[13] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (GU L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49) Qualora si osservi un incidente significativo, in particolare se causa un impatto immediato, tale incidente potrebbe essere notificato a un CSIRT, alle autorità di gestione delle crisi informatiche degli Stati membri o ad altre autorità settoriali o da essi rilevato. Si incoraggiano gli Stati membri a condividere le informazioni relative a tali incidenti all'interno delle reti, le quali dovrebbero prendere in considerazione l'adozione di misure adeguate. L'attivazione della rete di CSIRT e quella di EU-CyCLONe possono essere indipendenti l'una dall'altra in funzione della natura dell'incidente e della risposta richiesta. Tuttavia, entrambe le reti sono incoraggiate a proseguire la cooperazione reciproca sulla base di modalità procedurali concordate. La decisione relativa all'attivazione è di competenza esclusiva di ciascuna rete e presa in modo indipendente.

50) La rete di CSIRT dovrebbe fornire consulenza a EU-CyCLONe in merito all'eventualità che un incidente di cibersicurezza osservato possa essere considerato un incidente di cibersicurezza su vasta scala potenziale o in corso.

51) Come indicato nella direttiva (UE) 2022/2555, la rete di CSIRT ed EU-CyCLONe dovrebbero definire, senza ritardo, modalità procedurali in caso di incidente di cibersicurezza su vasta scala potenziale o in corso, al fine di garantire il coordinamento tecnico-operativo e la disponibilità di informazioni tempestive e pertinenti al livello politico.

VII: rispondere a un incidente di cibersicurezza su vasta scala o a una crisi informatica a livello dell'Unione

Risposta a un incidente di cibersicurezza su vasta scala o a una crisi informatica per cui gli IPCR non sono attivati in modalità piena attivazione

52) L'efficacia della risposta agli incidenti di cibersicurezza su vasta scala o alle crisi informatiche a livello dell'UE dipende da un'efficace cooperazione tecnica, operativa e politica nell'ambito di un approccio esteso a tutta l'amministrazione, comprese, ove possibile, le autorità di contrasto.

53) A ciascun livello, gli attori coinvolti dovrebbero svolgere attività specifiche per conseguire una conoscenza situazionale condivisa e una risposta coordinata. Tali misure garantiscono una diffusione ordinata ed efficace delle informazioni.

54) La risposta dovrebbe essere proporzionata all'impatto dell'incidente di cibersicurezza su vasta scala o della crisi informatica. Conformemente alla direttiva (UE) 2022/2555, le autorità di gestione delle crisi informatiche degli Stati membri dovrebbero garantire la coerenza e il coordinamento nazionali tra le risposte settoriali alle crisi informatiche.

55) Nel caso di un incidente di cibersicurezza su vasta scala o di crisi informatica, tutti gli attori e tutte le reti dovrebbero rispondere in stretto coordinamento nel modo seguente:

a) a livello tecnico:

i. gli Stati membri interessati e i rispettivi CSIRT dovrebbero cooperare con i soggetti interessati per rispondere agli incidenti e fornire assistenza, se del caso;

ii. i CSIRT dovrebbero cooperare attraverso la rete di CSIRT per condividere le informazioni tecniche pertinenti sull'incidente; i CSIRT collaborano negli sforzi volti ad analizzare gli artefatti tecnici disponibili e altre informazioni tecniche relative all'incidente, al fine di stabilirne le cause e le possibili misure tecniche di mitigazione;

iii. quando vengono a conoscenza di un incidente significativo, un CSIRT o un'autorità di gestione delle crisi informatiche di uno Stato membro sono incoraggiati a segnalarlo nell'ambito della rete di CSIRT o di EU-CyCLONe;

iv. la rete di CSIRT, con il sostegno dell'ENISA, dovrebbe aggregare le relazioni nazionali fornite dai CSIRT, e il risultato dovrebbe essere presentato a EU-CyCLONe;

v. qualora un incidente di cibersicurezza sia potenzialmente in grado di degenerare in un incidente di cibersicurezza su vasta scala o in una crisi informatica, la rete di CSIRT dovrebbe condividere le opportune informazioni con EU-CyCLONe. EU-CyCLONe dovrebbe utilizzare tali informazioni per aggiornare il Consiglio;

vi. la rete di CSIRT dovrebbe essere in stretto contatto con Europol per garantire lo scambio di informazioni tecniche pertinenti. La rete di CSIRT ed Europol dovrebbero istituire punti di contatto per migliorare la condivisione delle informazioni, ove opportuno, in caso di incidente di cibersicurezza su vasta scala;

b) a livello operativo:

i. gli Stati membri dovrebbero mitigare l'impatto dell'incidente a livello nazionale prendendo le misure adeguate;

ii. la rete di CSIRT dovrebbe trasmettere a EU-CyCLONe valutazioni tecniche degli incidenti in corso, che possono essere utilizzate da EU-CyCLONe;

iii. EU-CyCLONe dovrebbe valutare le conseguenze e l'impatto degli incidenti di cibersicurezza su vasta scala e delle crisi informatiche in questione, proporre possibili misure di mitigazione e sostenere la gestione coordinata degli incidenti di cibersicurezza su vasta scala e delle crisi informatiche, nonché sostenere il processo decisionale a livello politico;

iv. qualora si verifichi un incidente di cibersicurezza su vasta scala con un impatto intersettoriale, che richiede l'attivazione di azioni di risposta a livello dell'Unione, in particolare dei pertinenti meccanismi orizzontali e settoriali di gestione delle crisi a livello dell'Unione elencati nell'allegato II,

(a) gli attori appropriati possono, a seconda del tipo di meccanismi settoriali di gestione delle crisi a livello dell'Unione, chiedere l'attivazione di tale meccanismo;

(b) in caso di attivazione di tale meccanismo settoriale, i soggetti pertinenti sostengono i soggetti settoriali nella mitigazione dell'impatto dell'incidente;

(c) la Commissione dovrebbe agevolare il flusso di informazioni necessarie tra i punti di contatto per i pertinenti meccanismi orizzontali e settoriali di gestione delle crisi a livello dell'Unione di cui all'allegato II ed EU-CyCLONe, perseguire un'analisi intersettoriale integrata e proporre opzioni per un adeguato piano di risposta integrato;

(d) la Commissione, attraverso EU-CyCLONe, se del caso, in cooperazione con l'alto rappresentante, dovrebbe garantire la coerenza e il coordinamento delle misure operative a livello dell'UE nel settore informatico con le corrispondenti azioni di risposta a livello dell'Unione, in particolare in relazione alle richieste di assistenza attraverso l'UCPM;

(e) se è stata creata una pagina di monitoraggio IPCR, le informazioni sull'incidente, sul relativo impatto e sulle misure adottate dovrebbero essere condivise anche tra gli Stati membri e i soggetti dell'Unione attraverso la piattaforma web IPCR;

v. gli Stati membri possono richiedere servizi della riserva dell'UE per la cibersicurezza conformemente all'articolo 15 del regolamento (UE) 2025/38. Fatti salvi eventuali futuri atti di esecuzione a norma di tale regolamento, i servizi della riserva dell'UE per la cibersicurezza dovrebbero essere mobilitati entro 24 ore dalla richiesta;

c) a livello politico:

i. il Consiglio può chiedere resoconti ai principali portatori di interessi, in particolare la Commissione, l'alto rappresentante ed EU-CyCLONe, al fine di dare una risposta politica e strategica adeguata;

ii. il Consiglio, sostenuto dalla Commissione e dall'alto rappresentante, potrebbe decidere in merito alle misure adeguate per rispondere all'incidente di cibersicurezza su vasta scala, comprese le possibili risposte diplomatiche in linea con il capo IX;

iii. gli Stati membri possono attivare ulteriori meccanismi o strumenti di gestione delle crisi informatiche a seconda della natura e dell'impatto dell'incidente;

iv. quando gli IPCR sono attivati in modalità scambio di informazioni, viene attivata la capacità di sostegno all'ISAA, aumentando gli scambi di informazioni attraverso la piattaforma web IPCR e garantendo una panoramica condivisa della situazione. Le relazioni sulla situazione elaborate da EU-CyCLONe e dalla rete di CSIRT dovrebbero continuare a rappresentare gli strumenti principali per la presentazione della conoscenza situazionale comune, rispettivamente a livello operativo e a livello tecnico. Tali relazioni possono servire da base per le relazioni ISAA;

v. nel caso di un incidente che richiede l'attivazione di azioni di risposta a livello dell'Unione, in particolare i pertinenti meccanismi orizzontali e settoriali di gestione delle crisi a livello dell'Unione elencati nell'allegato II, il Consiglio, in cooperazione con la Commissione e l'alto rappresentante, dovrebbe garantire la coerenza e il coordinamento tra le risposte alla crisi informatica e le relative azioni di risposta a livello dell'Unione;

vi. qualora siano richiesti meccanismi pertinenti, in particolare i servizi della riserva per la cibersicurezza, i servizi della Commissione e, se del caso, il SEAE, nonché i pertinenti organi del Consiglio, in particolare il gruppo orizzontale "Questioni riguardanti il ciberspazio" e il gruppo orizzontale "Rafforzare la resilienza e contrastare le minacce ibride", a seconda dei casi, dovrebbero coordinare l'elaborazione e l'attuazione delle misure, nonché il processo decisionale appropriato per misure supplementari, in linea con il pacchetto di strumenti contro le minacce ibride[14] in caso di attività informatiche dolose che fanno parte di una campagna ibrida più ampia.

Risposta a un incidente di cibersicurezza su vasta scala o a una crisi informatica per cui gli IPCR sono attivati in modalità piena attivazione

56) È opportuno attuare le misure elencate nella precedente sezione "*Risposta a un incidente di cibersicurezza su vasta scala o a una crisi informatica per cui gli IPCR non sono attivati in modalità piena attivazione"*.

57) Quando gli IPCR sono attivati in modalità piena attivazione, le relazioni ISAA servono a garantire una conoscenza situazionale comune a livello politico. Le relazioni sulla situazione elaborate da EU-CyCLONe e dalla rete di CSIRT dovrebbero continuare a rappresentare gli strumenti principali per la presentazione della conoscenza situazionale comune, rispettivamente a livello operativo e a livello tecnico. Tali relazioni possono servire da base per le relazioni ISAA.

58) Qualora si verifichi un incidente di cibersicurezza su vasta scala o una crisi informatica che comporti l'attivazione degli IPCR in modalità piena attivazione, tutti gli attori dovrebbero rispondere in stretto coordinamento con un approccio esteso a tutta l'amministrazione nel modo seguente:

a) il coordinamento della risposta a livello politico dell'Unione è effettuato dal Consiglio utilizzando i dispositivi IPCR;

---

14 Il pacchetto di strumenti contro le minacce ibride è un quadro per una risposta coordinata alle campagne ibride che interessano l'UE e i suoi Stati membri, che comprende ad esempio misure preventive, di cooperazione, di stabilità, restrittive e di ripresa, e sostiene la solidarietà e l'assistenza reciproca.

b) EU-CyCLONe, in cooperazione con la rete di CSIRT, dovrebbe fornire informazioni chiare a livello politico sull'impatto, sulle possibili conseguenze e sulle misure di risposta e ripristino in relazione all'incidente, anche contribuendo alle relazioni ISAA;

c) oltre ad avvalersi della capacità ISAA, la presidenza del Consiglio dell'Unione europea convocherebbe tavole rotonde IPCR per consentire il coordinamento politico e strategico della risposta dell'UE, in cui le azioni nell'ambito del programma per la cibersicurezza e il lavoro dei pertinenti meccanismi settoriali contribuirebbero al lavoro degli IPCR. Le tavole rotonde possono inoltre individuare alcune lacune specifiche nella risposta e invitare determinati attori dell'UE a colmarle e a riferire in merito in occasione delle future tavole rotonde, al fine di sostenere il coordinamento politico e strategico nell'ambito degli IPCR;

d) la presidenza del Consiglio dell'Unione europea dovrebbe valutare la possibilità di invitare EU-CyCLONe alle pertinenti riunioni, comprese le tavole rotonde nell'ambito dei dispositivi IPCR e altre pertinenti riunioni del Consiglio;

e) le autorità di gestione delle crisi degli Stati membri dovrebbero garantire la coerenza e il coordinamento tra le risposte settoriali alle crisi informatiche con il sostegno delle autorità di gestione delle crisi informatiche;

f) le possibili risposte diplomatiche dovrebbero essere prese in considerazione e poste in atto in linea con il capo IX.

VIII: sforzi di comunicazione pubblica

59) Sebbene la comunicazione di informazioni alla popolazione di un singolo Stato membro in merito a un incidente di cibersicurezza su vasta scala o a una crisi informatica in corso, anche nell'ambito di iniziative di sensibilizzazione, rientri nelle competenze nazionali, gli Stati membri, la Commissione e l'alto rappresentante dovrebbero mirare a coordinare la loro comunicazione pubblica nella misura del possibile. Se del caso, è possibile coinvolgere la rete informale dei responsabili della comunicazione in caso di crisi degli IPCR.

60) Ai fini della preparazione agli incidenti di cibersicurezza su vasta scala e alle crisi informatiche, gli Stati membri e, se del caso, la Commissione e il CERT-UE sono invitati a scambiarsi informazioni sui rispettivi sforzi di comunicazione nell'ambito di EU-CyCLONe e della rete di CSIRT, comprese le migliori pratiche, quali avvisi o campagne di sensibilizzazione. L'ENISA dovrebbe fornire strumenti che favoriscano tale scambio e garantiscano un facile accesso.

61) Qualora si verifichi un incidente di cibersicurezza su vasta scala o una crisi informatica, gli Stati membri sono invitati a condividere, nell'ambito di EU-CyCLONe, informazioni sui rispettivi sforzi di comunicazione pubblica per creare una consapevolezza comune e coordinare le azioni. EU-CyCLONe, di propria iniziativa o su richiesta del Consiglio, può condividere con il Consiglio una panoramica di tali approcci.

IX: risposta diplomatica e cooperazione con i partner strategici

62) L'alto rappresentante, in stretta cooperazione con la Commissione e altri soggetti pertinenti dell'Unione, dovrebbe:

a) sostenere il processo decisionale in seno al Consiglio, anche attraverso analisi, relazioni e proposte, in merito al ricorso a possibili misure nell'ambito del pacchetto di strumenti della diplomazia informatica dell'UE. In tal modo sarà possibile utilizzare l'intera gamma di strumenti dell'Unione disponibili ai fini della prevenzione, della deterrenza e della risposta alle attività informatiche dolose, rafforzando la sua posizione in materia di deterrenza informatica e promuovendo la pace, la sicurezza e la stabilità internazionali nel ciberspazio;

b) agevolare il flusso delle informazioni necessarie con i partner strategici, se del caso anche con la NATO, nel caso in cui sia individuato un incidente pertinente;

c) rafforzare il coordinamento con i partner strategici, se del caso anche con la NATO, per quanto riguarda la risposta ad attività informatiche dolose da parte di autori di minacce persistenti, in particolare quando si avvale del pacchetto di strumenti della diplomazia informatica dell'UE, in linea con gli orientamenti di attuazione.

63) Gli Stati membri, l'alto rappresentante, la Commissione e altri soggetti pertinenti dell'Unione dovrebbero cooperare con i partner strategici e le organizzazioni internazionali per promuovere le buone pratiche e il comportamento responsabile degli Stati nel ciberspazio e garantire una risposta rapida e coordinata in caso di incidenti di cibersicurezza potenziali o su vasta scala.

64) La cooperazione tra l'Unione europea e la NATO dovrebbe essere condotta conformemente ai principi guida concordati di inclusività, reciprocità e trasparenza e nel pieno rispetto dell'autonomia decisionale dell'Unione.

65) La Commissione e l'alto rappresentante, tenendo conto degli accordi esistenti quali l'accordo tecnico CERT-UE/NATO del 2016, dovrebbero istituire punti di contatto per il coordinamento con la NATO in caso di crisi informatica al fine di scambiare le informazioni necessarie sulla situazione e sull'impiego dei meccanismi di risposta alle crisi per intensificare la cooperazione nella risposta e aumentare l'efficacia di quest'ultima. A tal fine, l'Unione dovrebbe valutare modalità per migliorare la condivisione delle informazioni con la NATO in modo inclusivo, reciproco e non discriminatorio, in particolare garantendo strumenti per una comunicazione sicura tenendo conto, nel contempo, delle norme in materia di condivisione delle informazioni dei diversi Stati membri.

66) Nell'ambito del programma continuo di esercitazioni informatiche dell'Unione di cui al precedente capo V, i servizi della Commissione e il SEAE dovrebbero prendere in considerazione la possibilità di organizzare un'esercitazione a livello di personale con la NATO, al fine di sperimentare la cooperazione tra soggetti civili e militari in caso di incidente di cibersicurezza su vasta scala o crisi informatica in cui gli Stati membri o gli alleati della NATO cerchino risposte a un attacco informatico che incida sulla loro sicurezza. L'esercitazione dovrebbe essere condotta in modo inclusivo e non discriminatorio e nel pieno rispetto dei principi concordati dei parametri della cooperazione UE-NATO. Dovrebbe inoltre essere condotta nel quadro dell'esercitazione "Integrated Resolve" dell'UE (esercitazione parallela e coordinata, "PACE"). È opportuno adottare tutte le misure necessarie per garantire la partecipazione di tutti gli attori di cui al programma per la cibersicurezza.

67) Dovrebbero essere prese in considerazione anche esercitazioni informatiche congiunte a livello dell'Unione con i paesi dei Balcani occidentali, la Repubblica di Moldova, l'Ucraina e altri partner strategici e paesi terzi che condividono gli stessi principi, in consultazione con il Consiglio, la Commissione e l'alto rappresentante.

X: coordinamento della gestione delle crisi informatiche con gli attori militari a livello dell'UE

68) Gli Stati membri dovrebbero continuare a rafforzare la cooperazione tra gli attori informatici civili e militari a livello nazionale.

69) EU-CyCLONe e la rete di CSIRT dovrebbero individuare possibili modalità e procedure per cooperare con i pertinenti attori militari dell'UE, come la conferenza dei comandanti per la sicurezza informatica dell'UE e la rete operativa delle squadre militari di pronto intervento informatico ("MICNET"), al fine di trarre beneficio da una prospettiva militare e civile congiunta, in particolare attraverso riunioni congiunte. EU-CyCLONe e la rete di CSIRT dovrebbero informare il Consiglio in merito ai progressi compiuti in relazione a tale cooperazione.

70) Lo Stato membro interessato è invitato a informare EU-CyCLONe, nonché il SEAE, se le pertinenti capacità di risposta militare nazionali o multinazionali sono utilizzate nel contesto di un incidente di cibersicurezza su vasta scala o di una crisi informatica; la trasmissione di tali informazioni è reciprocamente concordata tra l'utente e il soggetto che fornisce tale capacità di risposta.

71) Nell'ambito del programma continuo di esercitazioni informatiche dell'Unione di cui al precedente capo V, la Commissione e l'alto rappresentante dovrebbero prendere in considerazione la possibilità di organizzare un'esercitazione congiunta al fine di sperimentare la cooperazione tra attori informatici sia civili che militari nel caso in cui si verifichi un incidente di cibersicurezza su vasta scala che interessi gli Stati membri.

XI: ripresa da una crisi informatica e insegnamenti tratti

72) Gli Stati membri, le entità e le reti pertinenti dell'Unione dovrebbero collaborare durante la fase di ripresa successiva a una crisi informatica per garantire il rapido ripristino delle funzionalità di base. Anche le comunità di contrasto dovrebbero, se del caso, essere coinvolte in tale cooperazione. In questa fase, la cooperazione con il settore privato è fondamentale, in particolare per facilitare il recupero dei dati e il ripristino dei sistemi. Un coordinamento efficace tra i portatori di interessi dovrebbe in via prioritaria ridurre al minimo le perturbazioni e assicurare la continuità operativa.

73) Gli Stati membri, le entità e le reti pertinenti dell'Unione dovrebbero collaborare nella fase di ripresa sulla base degli insegnamenti tratti dalle crisi informatiche o dagli incidenti di cibersicurezza gestiti in passato, nonché sulla base delle segnalazioni di incidenti, in particolare nel contesto del meccanismo europeo di riesame degli incidenti di cibersicurezza istituito dal regolamento (UE) 2025/38.

74) EU-CyCLONe dovrebbe fornire alla rete di CSIRT, al gruppo di cooperazione NIS e al Consiglio un elenco completo degli insegnamenti tratti dalle crisi informatiche o dagli incidenti di cibersicurezza gestiti in passato e delle migliori pratiche. L'ENISA dovrebbe garantire che si tenga debitamente conto di tali insegnamenti nelle future attività di preparazione e nel valutare la pianificazione di esercitazioni future.

XII: comunicazione sicura

75) Sulla base della mappatura degli strumenti di comunicazione sicura esistenti[15], la Commissione dovrebbe proporre entro la fine del 2026 una serie interoperabile di soluzioni di comunicazione sicura. Il Consiglio, la Commissione, l'alto rappresentante, EU-CyCLONe e la rete di CSIRT dovrebbero raggiungere un accordo al riguardo entro la fine del 2027. Tali soluzioni dovrebbero beneficiare delle azioni nel settore delle comunicazioni sicure che le istituzioni dell'UE potrebbero intraprendere nell'ambito della strategia dell'UE in materia di preparazione e dovrebbero riguardare l'intera gamma di modi di comunicazione richiesti (voce, dati, videoconferenza, messaggistica, collaborazione e condivisione e consultazione di documenti). Le soluzioni dovrebbero soddisfare requisiti definiti di comune accordo per la protezione delle informazioni sensibili non classificate. Dovrebbero essere utilizzate soluzioni basate su un protocollo aperto con implementazioni open source adatte alla comunicazione in tempo reale, gestite da un soggetto residente nell'UE.

76) Ai fini dello scambio di informazioni classificate come RESTREINT UE/EU RESTRICTED, EU-CyCLONe e la rete di CSIRT, se necessario, dovrebbero poter utilizzare canali di comunicazione sicuri concepiti per le istituzioni, gli organi e gli organismi dell'UE, affinché possano scambiare informazioni classificate tra di loro e con gli Stati membri.

---

15 Doc. WK 862/2023.

77) Il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca istituito a norma del regolamento (UE) 2021/887[16], fatto salvo il futuro quadro finanziario pluriennale, dovrebbe prendere in considerazione la possibilità di erogare finanziamenti attraverso il programma Europa digitale per assistere gli Stati membri nell'utilizzo di strumenti di comunicazione sicura. Dovrebbe essere evitata qualsiasi duplicazione degli investimenti in sistemi sicuri interoperabili.

78) In particolare, i soggetti e gli Stati membri dell'UE dovrebbero sviluppare piani di emergenza in caso di crisi gravi in cui i normali canali di comunicazione basati su internet o su reti di telecomunicazione non siano disponibili o siano oggetto di perturbazioni.

79) Dovrebbero essere istituiti meccanismi di comunicazione e condivisione delle informazioni tra le autorità di contrasto e le reti di cibersicurezza, in particolare a livello tecnico, al fine di rispondere efficacemente alle crisi informatiche. Tali meccanismi dovrebbero rispettare il ruolo di ciascuna parte, nonché evitare di interferire con le operazioni in corso e garantire la ridondanza delle comunicazioni. Il sistema di comunicazione critica dell'UE attualmente in fase di sviluppo può apportare benefici alla risposta congiunta con le pertinenti comunità informatiche.

XIII: disposizioni finali

80) EU-CyCLONe, in cooperazione con la rete di CSIRT e altri attori principali nell'ecosistema dell'UE di gestione delle crisi informatiche e con il sostegno dell'ENISA, dovrebbe sviluppare, entro un anno dalla pubblicazione della raccomandazione, diagrammi di flusso di processo dettagliati che illustrino i flussi di informazioni tra gli attori pertinenti, i processi decisionali e le relazioni elaborate durante la gestione degli incidenti di cibersicurezza su vasta scala o delle crisi informatiche di cui alla presente raccomandazione. I diagrammi di flusso dovrebbero riguardare modalità e livelli di cooperazione differenti. Dovrebbero essere aggiornati ove necessario.

---

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

81) Per sostenere l'efficace applicazione del programma per la cibersicurezza riveduto e sulla base dell'esperienza acquisita attraverso le esercitazioni informatiche congiunte condotte nell'ambito dello stesso, il Consiglio può elaborare, se necessario, una serie di orientamenti di attuazione. Tali orientamenti potrebbero affrontare le sfide pratiche individuate nel corso delle esercitazioni e porre rimedio alle lacune e ai collegamenti mancanti individuati nel coordinamento, nella comunicazione e nell'interazione operativa.

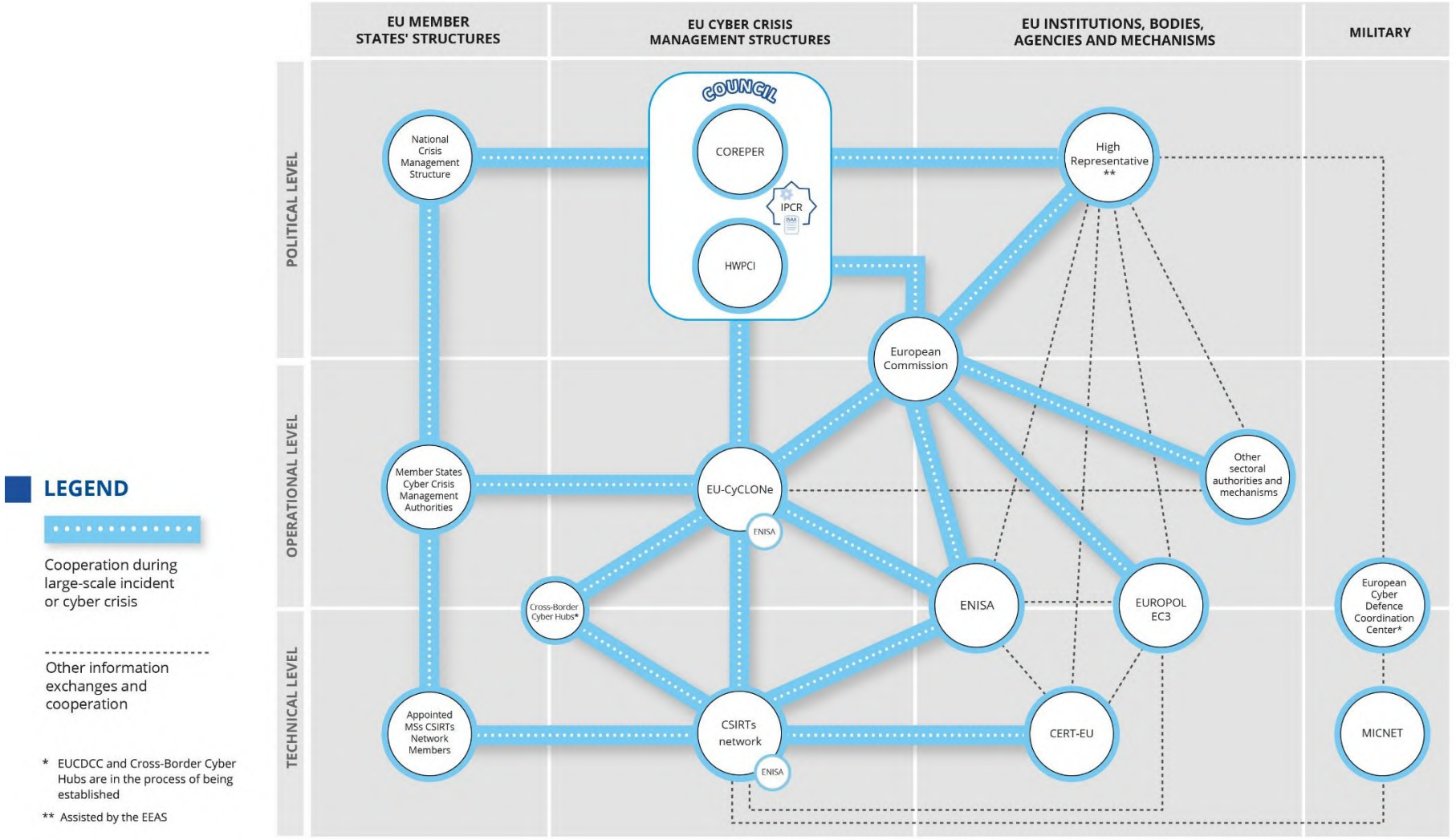
82) La presente raccomandazione dovrebbe essere riesaminata dalla Commissione in cooperazione con gli Stati membri, almeno ogni quattro anni dopo la sua pubblicazione. A seguito di ciascun riesame, la Commissione dovrebbe pubblicare una relazione e presentarla al Consiglio. La Commissione e gli Stati membri dovrebbero tenere conto, in particolare, dell'impatto del panorama delle minacce in evoluzione, dei risultati delle esercitazioni congiunte e delle modifiche legislative, in particolare le eventuali modifiche derivanti dalla revisione del regolamento (UE) 2019/881.

Fatto a Bruxelles, ...

Per il Consiglio

Il presidente

ALLEGATO I – Programma dell'Unione per rispondere a una crisi di cibersicurezza



ALLEGATO II – ATTORI (ENTITÀ E RETI) E MECCANISMI DI GESTIONE DELLE CRISI PERTINENTI A LIVELLO DELL'UNIONE

(1) Coinvolgimento dei principali attori durante tutto il ciclo di gestione delle crisi informatiche (incidenti di cibersicurezza su vasta scala e crisi informatiche)

	Preparazione	Individuazione	Risposta a un incidente di cibersicurezza su vasta scala o a una crisi informatica			Comunicazione pubblica	Ripresa e insegnamenti tratti
			a livello tecnico	a livello operativo	a livello politico		
Stati membri	X	X	X	X	X	X	X
Commissione	X			X	X	X	
Alto rappresentante con l'assistenza del SEAE	X			X	X	X	
Consiglio	X				X	X	X
ENISA	X		X	X			
CERT-UE	X	X	X	X		X	X
Rete di CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Ruoli e competenze degli attori e dei meccanismi pertinenti a livello dell'Unione (in ordine alfabetico nella versione inglese del testo) in relazione alla gestione delle crisi informatiche

Attore	Livello	Ruolo e competenza	Riferimento
CERT-UE	Tecnico/operativo	Coordina la risposta alle crisi a livello tecnico e la gestione degli incidenti gravi che interessano i soggetti dell'Unione. Tiene un inventario delle competenze tecniche disponibili che risulterebbero necessarie per la risposta agli incidenti in caso di incidenti gravi e assiste l'IICB nel coordinare i piani di gestione delle crisi informatiche dei soggetti dell'Unione per gli incidenti gravi. È membro della rete di CSIRT. Sostiene la Commissione nell'ambito di EU-CyCLONe per quanto riguarda la gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala. Funge da piattaforma per lo scambio di informazioni sulla cibersicurezza e il coordinamento della risposta in caso di incidenti, facilitando la circolazione delle informazioni riguardo agli incidenti, alle minacce informatiche,	Regolamento (UE, Euratom) 2023/2841 Regolamento (UE) 2025/38

Attore	Livello	Ruolo e competenza	Riferimento
		alle vulnerabilità e ai quasi incidenti tra i soggetti dell'Unione e gli omologhi. Richiede la mobilitazione della riserva dell'UE per la cibersicurezza per conto dei soggetti dell'Unione. Coopera con il centro per la cibersicurezza della NATO sulla base del loro accordo tecnico.	
Consiglio dell'Unione europea	Politico	Ha funzioni di definizione delle politiche e di coordinamento. È incaricato degli IPCR, che riguardano il coordinamento e la risposta a livello politico dell'Unione.	Articolo 16 del trattato sull'Unione europea
Presidenza del Consiglio dell'Unione europea	Politico	Decide (fatta eccezione per i casi in cui è invocata la clausola di solidarietà a norma dell'articolo 222 del trattato sul funzionamento dell'Unione europea) se attivare gli IPCR, in consultazione con gli Stati membri interessati, se del caso, nonché con la Commissione e l'alto rappresentante.	Articolo 16 del trattato sull'Unione europea Decisione di esecuzione (UE) 2018/1993 del Consiglio
Poli informatici transfrontalieri	Tecnico	Il polo informatico transfrontaliero è una piattaforma multinazionale, istituita mediante un accordo di consorzio scritto, che riunisce in una	Regolamento (UE) 2025/38

Attore	Livello	Ruolo e competenza	Riferimento
		struttura di rete coordinata i poli informatici nazionali di almeno tre Stati membri e che è concepita per migliorare il monitoraggio, il rilevamento e l'analisi delle minacce informatiche, per impedire gli incidenti informatici e per favorire l'elaborazione di analisi delle minacce informatiche, in particolare mediante lo scambio di dati e informazioni pertinenti, se del caso anonimizzati, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia. Cooperano strettamente con la rete di CSIRT per condividere informazioni. Forniscono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, alle autorità degli Stati membri e alla Commissione attraverso EU-CyCLONe e la rete di CSIRT.	

Attore	Livello	Ruolo e competenza	Riferimento
Rete di CSIRT	Tecnico	Contribuisce allo sviluppo della fiducia e promuove una cooperazione operativa rapida fra gli Stati membri. È la rete principale per lo scambio di informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità. Su richiesta di un membro potenzialmente interessato da un incidente, la rete scambia e discute informazioni relative a tale incidente e alle minacce informatiche associate. La rete può anche agevolare una risposta coordinata a un incidente identificato nella giurisdizione di un membro richiedente. Fornisce assistenza agli Stati membri nella gestione degli incidenti transfrontalieri e prende in esame ulteriori forme di cooperazione, compresa l'assistenza reciproca. Riceve informazioni dagli Stati membri in merito alle richieste da loro presentate alla riserva dell'UE per la cibersicurezza.	Direttiva (UE) 2022/2555 Regolamento (UE) 2025/38

Attore	Livello	Ruolo e competenza	Riferimento
Conferenza dei comandanti per la sicurezza informatica		Si tratta di un forum per i comandanti per la sicurezza informatica a livello nazionale all'interno degli Stati membri per collaborare e scambiare informazioni essenziali sulle operazioni e sulle strategie in corso nel ciberspazio volte a mitigare gli incidenti di cibersicurezza su vasta scala. È organizzato dalla presidenza di turno del Consiglio dell'Unione europea con il sostegno dell'Agenzia europea per la difesa (AED) e del servizio europeo per l'azione esterna (SEAE), compreso lo Stato maggiore dell'UE (EUMS).	Comunicazione congiunta sulla politica di ciberdifesa dell'UE (2022)
Commissione	Operativo/politico	È l'organo esecutivo dell'Unione europea. Garantisce il corretto funzionamento del mercato interno. Facilita la coerenza delle azioni di risposta alle crisi a livello dell'Unione collegate e il loro coordinamento. Si occupa di determinate azioni di preparazione generali a livello dell'Unione nel quadro della decisione UCPM, compresa la gestione del Centro di coordinamento della risposta	Articolo 17 del trattato sull'Unione europea Decisione di esecuzione (UE) 2018/1993 Decisione n. 1313/2013/UE Direttiva (UE) 2022/2555

Attore	Livello	Ruolo e competenza	Riferimento
		alle emergenze e del sistema comune di comunicazione e informazione in caso di emergenza. È osservatore presso EU-CyCLONe e membro in caso di incidente su vasta scala, potenziale o in corso, che abbia o abbia probabilità di avere un impatto significativo sui servizi e sulle attività che rientrano nell'ambito di applicazione della direttiva (UE) 2022/2555. È osservatore presso la rete di CSIRT. Ha la responsabilità generale per l'attuazione della riserva dell'UE per la cibersicurezza. È il punto di contatto presso il comitato interistituzionale per la cibersicurezza ai fini della condivisione, con EU-CyCLONe, delle informazioni pertinenti in relazione agli incidenti gravi. Viene consultata dalla presidenza del Consiglio in merito alle decisioni di attivare o disattivare gli IPCR (fatta eccezione per i casi in cui è invocata la	Regolamento (UE) 2025/38 Regolamento (UE, Euratom) 2023/2841

Attore	Livello	Ruolo e competenza	Riferimento
		clausola di solidarietà a norma dell'articolo 222 TFUE). I servizi della Commissione elaborano, insieme al SEAE, le relazioni ISAA.	
Agenzia dell'Unione europea per la cibersicurezza (ENISA)	Tecnico/operativo	Svolge compiti al fine di conseguire un livello elevato di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri e le istituzioni dell'Unione. Svolge le funzioni di segretariato della rete di CSIRT e di EU-CyCLONe. Elabora periodicamente una relazione sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce informatiche (con l'EC3 e il CERT-UE e in stretta cooperazione con gli Stati membri). Contribuisce a sviluppare una risposta comune agli incidenti o alle crisi su vasta scala di carattere transfrontaliero, soprattutto: - aggregando e analizzando le relazioni delle fonti nazionali; - assicurando il flusso di informazioni tra i livelli tecnico, operativo e politico;	Direttiva (UE) 2022/2555 Regolamento (UE) 2019/881 Regolamento (UE) 2025/38 Regolamento (UE) 2024/2847

Attore	Livello	Ruolo e competenza	Riferimento
		- agevolando, su richiesta, la gestione degli incidenti; - sostenendo i soggetti dell'Unione per quanto riguarda la comunicazione pubblica; - sostenendo, su richiesta, gli Stati membri per quanto riguarda la comunicazione pubblica; - testando le capacità di risposta agli incidenti e organizzando periodicamente esercitazioni di cibersicurezza. Agisce in qualità di amministrazione aggiudicatrice quando è stata incaricata dell'amministrazione e del funzionamento, in tutto o in parte, della riserva dell'UE per la cibersicurezza. Organizza ogni due anni un'esercitazione globale di cibersicurezza su vasta scala a livello dell'Unione con elementi tecnici, operativi o strategici. Prepara una relazione di riesame dell'incidente in collaborazione con lo Stato membro interessato e altri portatori di interessi pertinenti, al fine di valutare le cause, l'impatto e la mitigazione di un incidente (su richiesta della Commissione o di EU-	

Attore	Livello	Ruolo e competenza	Riferimento
		CyCLONe e con l'approvazione dello Stato membro interessato). Informa EU-CyCLONe se le informazioni fornite a norma degli obblighi di segnalazione previsti dal regolamento sulla ciberresilienza sono pertinenti per la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala.	
Rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe)	Operativo	Sostiene la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala. Garantisce il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. Coordina la gestione degli incidenti e delle crisi di cibersicurezza su vasta scala e sostiene il processo decisionale a livello politico in merito a tali incidenti e crisi. Valuta le conseguenze e l'impatto dei pertinenti incidenti e delle pertinenti crisi di cibersicurezza su vasta scala e propone possibili misure di mitigazione.	Direttiva (UE) 2022/2555 Regolamento (UE) 2025/38

Attore	Livello	Ruolo e competenza	Riferimento
		Discute, su richiesta di uno Stato membro interessato, i piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala. Elabora, insieme all'ENISA e alla Commissione, il modello per facilitare la presentazione di richieste di sostegno della riserva dell'UE per la cibersicurezza. Riceve informazioni dagli Stati membri in merito alle richieste da loro presentate alla riserva dell'UE per la cibersicurezza. Riceve informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, dai poli informatici transfrontalieri o dalla rete di CSIRT.	
Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza con l'assistenza del servizio	Politico	Guida e coordina gli sforzi dell'Unione per affrontare le minacce esterne per la sicurezza di natura ibrida e informatica. È responsabile della diplomazia informatica e degli strumenti di ciberdifesa dell'Unione ai fini della deterrenza e della risposta alle	Decisione 2010/427/UE del Consiglio

Attore	Livello	Ruolo e competenza	Riferimento
europeo per l'azione esterna		minacce esterne, anche utilizzando i pacchetti di strumenti dell'Unione contro le minacce ibride e della diplomazia informatica. Interagisce con i partner esterni, anche attraverso la PSDC. Contribuisce alla preparazione dell'Unione e degli Stati membri per quanto riguarda la conoscenza situazionale in merito alle minacce ibride e informatiche e la capacità di reagire alle stesse, ad esempio attraverso esercitazioni pratiche, formazioni e reti. Gestisce le implicazioni in materia di sicurezza e difesa delle risorse spaziali dell'Unione, in particolare nell'ambito della politica di sicurezza e di difesa comune (PSDC) dell'Unione. Fornisce sostegno alla conferenza dei comandanti per la sicurezza informatica dell'UE. Fornisce sostegno alla rete operativa delle squadre militari di pronto intervento informatico (MICNET).	

Attore	Livello	Ruolo e competenza	Riferimento
		Viene consultato dalla presidenza del Consiglio in merito alle decisioni di attivare o disattivare gli IPCR (fatta eccezione per i casi in cui è invocata la clausola di solidarietà a norma dell'articolo 222 TFUE). Il SEAE elabora, insieme ai servizi della Commissione, le relazioni ISAA.	
Centro di coordinamento della ciberdifesa dell'UE	Orizzontale	Il suo obiettivo iniziale è principalmente migliorare la conoscenza situazionale condivisa dell'Unione e dei suoi Stati membri sulle attività dolose nel ciberspazio, in particolare per quanto riguarda le missioni e operazioni militari nell'ambito della PSDC.	Comunicazione congiunta sulla politica di ciberdifesa dell'UE (2022)
Europol	Operativo	Fornisce sostegno operativo e tecnico alle autorità competenti degli Stati membri ai fini della prevenzione e della deterrenza della criminalità informatica. Assiste le autorità competenti degli Stati membri, su loro richiesta, nel rispondere agli attacchi informatici di sospetta origine criminale.	Regolamento (UE) 2016/794, comprese tutte le modifiche

Attore	Livello	Ruolo e competenza	Riferimento
Comitato interistituzionale per la cibersicurezza		Istituisce un piano di gestione delle crisi informatiche al fine di sostenere, a livello operativo, la gestione coordinata degli incidenti gravi che colpiscono i soggetti dell'Unione e al fine di contribuire allo scambio regolare di informazioni pertinenti. Coordina l'adozione dei piani individuali di gestione delle crisi informatiche dei soggetti dell'Unione. Adotta, sulla base di una proposta del CERT-UE, indirizzi o raccomandazioni sulla cooperazione in materia di risposta agli incidenti in caso di incidenti significativi che riguardano soggetti dell'Unione.	Regolamento (UE, Euratom) 2023/2841
Rete operativa delle squadre militari di pronto intervento informatico (MICNET)	Tecnico	Promuove una risposta più solida e coordinata alle minacce informatiche che colpiscono sistemi di difesa nell'Unione, compresi quelli impiegati nelle missioni e operazioni militari nell'ambito della PSDC. È sostenuta dall'Agenzia europea per la difesa.	Comunicazione congiunta sulla ciberdifesa (2022)
Capacità unica di analisi		È composta 1) dal Centro UE di situazione e di intelligence (EU INTCEN) e 2) dalla direzione	Articolo 38 e articoli da 42 a 46 del

Attore	Livello	Ruolo e competenza	Riferimento
dell'intelligence (SIAC)		"Intelligence" dello Stato maggiore dell'UE (EUMS INT). Fornisce intelligence strategica in materia di politica estera, terrorismo e minacce informatiche e ibride. Inoltre, gestisce l'intelligence militare per le missioni nell'ambito della PSDC e sostiene le operazioni di difesa e di gestione delle crisi dell'Unione. Opera sotto l'autorità dell'alto rappresentante.	trattato sull'Unione europea

(3) Pertinenti meccanismi e piattaforme di gestione delle crisi a livello dell'Unione

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
ARGUS	Orizzontale	È il processo di coordinamento e il sistema generale di allarme della Commissione volto a fornire una risposta coerente in caso di grave crisi transfrontaliera che richieda un'azione a livello dell'UE. Riunisce tutti i servizi e i gabinetti competenti per decidere e coordinare le misure. Consente alla Commissione di scambiare informazioni pertinenti sulle crisi multisettoriali emergenti oppure sulle minacce prevedibili o imminenti che richiedono un'azione a livello dell'Unione.	Comunicazione della Commissione COM(2005)662
Centro di risposta alle crisi (CRC) del SEAE	Orizzontale	È il punto di accesso unico per tutte le questioni connesse alle crisi in seno al SEAE e la capacità permanente di risposta alle crisi, disponibile 24 ore su 24 e 7 giorni su 7, per le emergenze che mettono a repentaglio la sicurezza del personale nelle delegazioni dell'UE, e/o in risposta a crisi che interessano cittadini dell'Unione all'estero. Riunisce esperti in materia consolare, di sicurezza e di conoscenza situazionale, avvalendosi nel contempo di professionisti impegnati sul campo presso le delegazioni dell'Unione.	Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
			internazionali (21 marzo 2022)
Programma per le infrastrutture critiche	Orizzontale	Coordina una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera.	Raccomandazione C/2024/4371 del Consiglio
Sistema di allerta per la cibersicurezza	Specifico per il ciberspazio	Garantisce capacità avanzate dell'Unione per migliorare le capacità di rilevamento, analisi e trattamento dei dati in relazione alle minacce informatiche e la prevenzione degli incidenti nell'Unione.	Regolamento (UE) 2025/38
Pacchetto di strumenti della diplomazia informatica (quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose)	Specifico per il ciberspazio	Consente di fornire una risposta diplomatica comune dell'Unione alle attività informatiche dolose, contribuendo a prevenire i conflitti, ridurre le minacce alla cibersicurezza e incrementare la stabilità nelle relazioni internazionali.	Conclusioni del Consiglio del 19 giugno 2017 Orientamenti di attuazione rivisti (doc. 10289/23 dell'8 giugno 2023)

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
Riserva dell'UE per la cibersicurezza	Specifico per il ciberspazio	Mobilita esperti e risorse in materia di cibersicurezza durante le crisi per sostenere gli sforzi di risposta negli Stati membri e presso le istituzioni, gli organi o gli organismi dell'Unione.	Regolamento (UE) 2025/38
Codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica	Settoriale	Definisce un processo ricorrente di valutazioni dei rischi per la cibersicurezza nel settore dell'energia elettrica a livello di Unione, di Stati membri, di regioni e di soggetti. Include disposizioni specifiche per la gestione delle crisi e la cooperazione con i CSIRT e EU-CyCLONe nei casi in cui un incidente di cibersicurezza su vasta scala abbia ripercussioni su altri settori dipendenti dalla sicurezza dell'approvvigionamento di energia elettrica.	Regolamento delegato (UE) 2024/1366 della Commissione
Pacchetto di strumenti contro le minacce ibride	Orizzontale	Comprende una serie di disposizioni per garantire una panoramica degli strumenti disponibili a livello dell'UE in risposta a tutti i tipi di minacce ibride e al loro uso coordinato, assicurando la coerenza delle azioni in tutti i settori. Il pacchetto di strumenti contro le minacce ibride contribuisce a garantire che il processo decisionale si basi su una conoscenza	Conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride (22 giugno 2022) Orientamenti di attuazione del

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
		situazionale completa e sugli insegnamenti tratti.	quadro per una risposta coordinata dell'UE alle campagne ibride (14 dicembre 2022)
Gruppi di risposta rapida alle minacce ibride	Orizzontale	Nell'ambito del pacchetto di strumenti dell'UE contro le minacce ibride, i gruppi di risposta rapida dell'UE alle minacce ibride attingono alle pertinenti competenze civili e militari settoriali a livello nazionale e dell'UE per fornire un'assistenza mirata e su misura a breve termine agli Stati membri, alle missioni e operazioni nell'ambito della politica di sicurezza e di difesa comune e ai paesi partner per contrastare le minacce e le campagne ibride.	Quadro di riferimento per l'istituzione pratica dei gruppi di risposta rapida dell'UE alle minacce ibride (21 maggio 2024) Orientamenti operativi per il dispiegamento di gruppi di risposta rapida alle minacce ibride, approvati dal Coreper il 4 dicembre 2024
IPCR	Orizzontale	Sostengono un processo decisionale rapido e coordinato a livello politico dell'Unione in caso di crisi gravi e complesse. La decisione di attivazione e disattivazione è adottata dalla presidenza del Consiglio, che	Decisione di esecuzione (UE) 2018/1993 del Consiglio

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
		consulta (fatta eccezione per i casi in cui è stata invocata la clausola di solidarietà) gli Stati membri interessati, la Commissione e l'alto rappresentante. Il segretariato generale del Consiglio, i servizi della Commissione e il SEAE possono inoltre convenire, in consultazione con la presidenza, di attivare gli IPCR in modalità scambio di informazioni. Le attività degli IPCR muovono dalle relazioni ISAA elaborate dai servizi della Commissione e dal SEAE. Tali relazioni si basano su informazioni e analisi pertinenti fornite dagli Stati membri (per esempio dalle pertinenti unità nazionali di crisi) e dagli organismi e agenzie dell'Unione competenti.	
Protocollo di risposta alle emergenze delle autorità di contrasto dell'UE	Orizzontale	È uno strumento per aiutare le autorità di contrasto dell'Unione a fornire una risposta immediata in caso di gravi attacchi informatici transfrontalieri attraverso una valutazione rapida, la condivisione sicura e tempestiva di informazioni critiche e un coordinamento efficace degli aspetti internazionali delle loro indagini.	Conclusioni del Consiglio relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala (26 giugno 2018)

Meccanismo	Orizzontale/settoriale/specifico per il ciberspazio	Descrizione	Riferimento
Gruppi di risposta rapida agli incidenti informatici (CRRT) della PESCO	Specifico per il ciberspazio	I CRRT della PESCO sono una capacità di ciberdifesa civile-militare sviluppata congiuntamente dagli Stati membri dell'UE per rispondere rapidamente agli incidenti informatici e alle crisi informatiche e svolgere azioni preventive, quali valutazioni delle vulnerabilità e monitoraggio elettorale. La missione dei CRRT della PESCO consiste nel fornire sostegno in materia di cibersicurezza, su richiesta, agli Stati membri dell'UE, alle istituzioni, agli organi e agli organismi dell'UE, alle missioni e operazioni militari nell'ambito della PSDC dell'UE nonché ai paesi partner.	Articolo 42, paragrafo 6, articolo 46 e protocollo n. 10 del trattato sull'Unione europea

Architettura di risposta alle minacce spaziali (STRA)	Settoriale (Minacce spaziali, comprese quelle informatiche)	Riguarda le responsabilità che devono essere esercitate dal Consiglio e dall'alto rappresentante per prevenire una minaccia derivante dal dispiegamento, dal funzionamento o dall'uso dei sistemi istituiti e dei servizi forniti nell'ambito del programma spaziale dell'Unione.	Decisione (PESC) 2021/698 del Consiglio
Quadro di coordinamento sistemico degli incidenti informatici (EU-SCICF)	Settoriale	Si tratta di un quadro, in fase di elaborazione, per la comunicazione e il coordinamento che affronta e gestisce potenziali eventi informatici sistemici nel settore finanziario. Si baserà su uno dei ruoli previsti delle autorità europee di vigilanza (AEV) a norma del regolamento (UE) 2022/2554, ossia consentire gradualmente una risposta efficace coordinata a livello dell'Unione in caso di un grave incidente transfrontaliero connesso alle tecnologie dell'informazione e della comunicazione (TIC) o di una minaccia connessa aventi un impatto sistemico sul settore finanziario dell'Unione nel suo complesso.	Raccomandazione del Comitato europeo per il rischio sistemico, del 2 dicembre 2021, su un quadro paneuropeo di coordinamento sistemico degli incidenti informatici per le autorità competenti (CERS/2021/17)
Meccanismo unionale di protezione civile (UCPM)	Orizzontale	Garantisce la cooperazione in materia di protezione civile per migliorare la prevenzione, la preparazione e la risposta alle catastrofi.	Decisione n. 1313/2013/UE

Ambiente comune per la condivisione delle informazioni (CISE)	Specifico per il settore marittimo, riguardante sette ambiti	È una rete che collega i sistemi delle autorità dell'UE/del SEE con responsabilità in materia di sorveglianza marittima. Consente lo scambio di informazioni pertinenti a livello transfrontaliero e in diversi settori in modo continuo e automatizzato.	Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali (21 marzo 2022)

(4) Settori ad alta criticità e altri settori critici a norma della direttiva (UE) 2022/2555 e meccanismi settoriali di gestione delle crisi a livello dell'Unione (se del caso)		
Settore	**Sottosettore**	**Meccanismi settoriali di gestione delle crisi applicabili**
Energia	Energia elettrica	Gruppo di coordinamento per l'energia elettrica
	Teleriscaldamento e teleraffrescamento	n.a.
	Petrolio	Gruppo di coordinamento del petrolio Gruppo di autorità dell'Unione europea per le attività in mare nel settore degli idrocarburi (EUOAG)
	Gas	Gruppo di coordinamento del gas
	Idrogeno	n.a.
Trasporti	Trasporto aereo	Cellula europea di coordinamento dell'aviazione in caso di crisi (EACCC)
	Trasporto ferroviario	n.a.
	Trasporto per vie d'acqua	Agenzia europea di controllo della pesca (EFCA) SafeSeaNet Servizi marittimi integrati (IMS) Centro di raccolta dati del sistema di identificazione e tracciamento delle navi a lungo raggio (LRIT) Servizi di supporto marittimo dell'EMSA

	Trasporto su strada	n.a.
	Orizzontale	Rete dei punti di contatto per i trasporti, istituita dal piano di emergenza per i trasporti (COM(2022) 211)
Settore bancario		EU-SCICF
Infrastrutture dei mercati finanziari		EU-SCICF Meccanismo europeo di stabilizzazione finanziaria

Settore sanitario		Sistema di allarme rapido e di reazione (SARR) Centro operativo per le emergenze sanitarie (*Health Emergency Operations Facility* – HEOF) - Sistema di allarme rapido per tessuti, cellule e componenti del sangue (*Rapid alert system for tissue and cell and blood Components* – RATC/RAB) Quadro per le emergenze di sanità pubblica Sistema di allarme rapido per incidenti chimici (*Rapid Alerting System for Chemical incidents* – RASCHEM) Portale europeo di sorveglianza delle malattie infettive Autorità per la preparazione e la risposta alle emergenze sanitarie (HERA) Sistema di informazione sanitaria medica (*Medical health intelligence System* – MediSys) Gruppo direttivo esecutivo per le carenze dei dispositivi medici (MDSSG) Allarme rapido di farmacovigilanza Task force sanitaria dell'UE (EUHTF) Comitato per la sicurezza sanitaria
Acqua potabile		n.a.

Acque reflue		n.a.
Infrastrutture digitali		n.a.
Gestione dei servizi TIC		n.a.
Pubblica amministrazione		n.a.
Spazio		Architettura di risposta alle minacce spaziali (STRA)
Servizi postali e di corriere		n.a.
Gestione dei rifiuti		n.a.
Fabbricazione, produzione e distribuzione di sostanze chimiche		Sistema di allarme rapido per incidenti chimici (RASCHEM)

Produzione, trasformazione e distribuzione di alimenti		Sistema europeo di monitoraggio delle colture Rilevamento di anomalie nella produzione agricola a livello mondiale (*Global agricultural production anomaly hotspot detection* – ASAP) - Rete europea dei sistemi d'informazione fitosanitaria (*European Network of Plant Health Information Systems* – EUROPHYT) - Squadra veterinaria di emergenza dell'UE (*EU Veterinary Emergency Team* – EUVET) Sistema di allarme rapido per gli alimenti e i mangimi (RASFF) Meccanismo europeo di preparazione e risposta alle crisi della sicurezza dell'approvvigionamento alimentare (EFSCM) Regolamento sulle emergenze e la resilienza nel mercato interno (IMERA)
Fabbricazione	Dispositivi medici	n.a.
	Computer e prodotti di elettronica e ottica	n.a.
	Macchinari e apparecchiature	n.a.
	Fabbricazione di autoveicoli, rimorchi e semirimorchi	n.a.
	Fabbricazione di altri mezzi di trasporto	n.a.

Fornitori di servizi digitali		n.a.
Ricerca		n.a.

Allegato III – Quadro di risposta alle crisi di cibersicurezza dell'UE e strumenti correlati

Dal 2017 l'Unione ha sviluppato il proprio quadro in materia di cibersicurezza attraverso diversi strumenti che contengono disposizioni rilevanti per la gestione delle crisi di cibersicurezza:

- regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[1],
- direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[2],
- regolamento di esecuzione (UE) 2024/2690 della Commissione[3], regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio[4],
- regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio[5],
- regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio[6] e
- regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio ("regolamento sulla cibersolidarietà")[7].

Tra le misure settoriali specifiche per le crisi di cibersicurezza figurano il regolamento delegato (UE) 2024/1366 della Commissione[8] e il futuro quadro di coordinamento sistemico degli incidenti informatici (EU-SCICF) nel contesto del regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio[9].

La direttiva 2013/40/UE[10] fornisce il riferimento per la definizione di attività criminali connesse agli attacchi informatici e le norme dell'Unione sull'accesso transfrontaliero alle prove elettroniche, in particolare il regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio[11], una volta attuate, agevoleranno in modo significativo l'azione di contrasto in questo settore.

La politica di ciberdifesa dell'UE[12] delinea i ruoli di una rete operativa delle squadre militari di pronto intervento informatico (MICNET) dell'UE e della conferenza dei comandanti per la sicurezza informatica dell'UE e prevede l'istituzione di un centro di coordinamento della ciberdifesa dell'UE (EUCDCC).

Altri meccanismi di conoscenza situazionale e risposta alle crisi, di natura non informatica, sono presenti in alcuni dei settori critici elencati negli allegati I e II della direttiva (UE) 2022/2555.

La raccomandazione del Consiglio relativa a un programma per coordinare una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera[13] prevede la cooperazione tra gli attori rilevanti qualora un incidente interessi sia aspetti fisici sia la cibersicurezza dell'infrastruttura critica.

[1] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

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

[3] Regolamento di esecuzione (UE) 2024/2690 della Commissione, del 17 ottobre 2024, recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari (GU L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (GU L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

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

[6] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti

informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (GU L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Regolamento delegato (UE) 2024/1366 della Commissione, dell'11 marzo 2024, che integra il regolamento (UE) 2019/943 del Parlamento europeo e del Consiglio istituendo un codice di rete relativo a disposizioni settoriali per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica (GU L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Regolamento (UE) 2023/1543 del Parlamento europeo e del Consiglio, del 12 luglio 2023, relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali e direttiva (UE) 2023/1544 del Parlamento europeo e del Consiglio, del 12 luglio 2023, recante norme armonizzate sulla designazione di stabilimenti designati e sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove elettroniche nei procedimenti penali (GU L 191 del 28.7.2023, pag. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022JC0049

[13] *GU C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=OJ:C_202404371