I

(Risoluzioni, raccomandazioni e pareri)

RACCOMANDAZIONI

CONSIGLIO

RACCOMANDAZIONE DEL CONSIGLIO

del 8 dicembre 2022

su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche

(Testo rilevante ai fini del SEE)

(2023/C 20/01)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114 e l'articolo 292, prima e seconda frase,

vista la proposta della Commissione europea,

considerando quanto segue:

1) Allo scopo di garantire il funzionamento del mercato interno, è nell'interesse di tutti gli Stati membri e dell'Unione nel suo insieme individuare chiaramente e proteggere le pertinenti infrastrutture critiche che forniscono servizi essenziali in detto mercato, in particolare in settori chiave quali l'energia, le infrastrutture digitali, i trasporti e lo spazio, nonché le infrastrutture critiche di significativa rilevanza transfrontaliera ([1]), la cui perturbazione potrebbe avere un significativo impatto su altri Stati membri.

2) La presente raccomandazione, che è un atto non vincolante, mette in luce la volontà politica degli Stati membri di cooperare nonché l'impegno da essi assunto nei confronti delle misure raccomandate, come illustrato in un piano in cinque punti pubblicato dalla presidente della Commissione europea, nel pieno rispetto delle competenze degli Stati membri. La presente raccomandazione non pregiudica la tutela degli interessi essenziali della sicurezza nazionale, della sicurezza pubblica o della difesa degli Stati membri e non ci si dovrebbe aspettare da nessuno Stato membro che condivida informazioni contrarie a tali interessi.

3) Sebbene la responsabilità primaria di garantire la sicurezza e la fornitura dei servizi essenziali da parte delle infrastrutture critiche spetti agli Stati membri e ai rispettivi operatori delle infrastrutture critiche, un maggiore coordinamento a livello dell'Unione risulta opportuno in particolare alla luce delle minacce in evoluzione che possono ripercuotersi su diversi Stati membri contemporaneamente, come la guerra di aggressione della Russia nei confronti dell'Ucraina e le campagne ibride contro gli Stati membri, o incidere sulla resilienza e sul buon funzionamento dell'economia, del mercato interno e dell'intera società dell'Unione. È opportuno prestare particolare attenzione alle infrastrutture critiche al di fuori del territorio degli Stati membri, come le infrastrutture critiche sottomarine o le infrastrutture energetiche offshore.

([1]) Gli Stati membri dovrebbero valutare tale rilevanza in linea con le rispettive prassi nazionali e possono farlo sulla base, tra l'altro, di una valutazione del rischio nonché dell'impatto e della natura dell'evento.

4) Il Consiglio europeo, nelle sue conclusioni del 20 e 21 ottobre 2022, ha condannato fermamente gli atti di sabotaggio contro le infrastrutture critiche, come quelli a danno dei gasdotti Nord Stream, indicando la volontà dell'Unione di dare una risposta unitaria e risoluta a qualsiasi perturbazione deliberata delle infrastrutture critiche o ad altre azioni ibride.

5) In considerazione dello scenario di minacce in rapida evoluzione, dovrebbero essere adottate in via prioritaria misure di aumento della resilienza in settori chiave quali energia, infrastrutture digitali, trasporti e spazio, e in altri settori pertinenti individuati dagli Stati membri. Tali misure dovrebbero puntare a rafforzare la resilienza delle infrastrutture critiche, tenendo conto dei rischi del caso, in particolare gli effetti a cascata, le perturbazioni delle catene di approvvigionamento, la dipendenza, l'impatto dei cambiamenti climatici, i fornitori e i partner inaffidabili nonché le minacce e le campagne ibride, comprese la manipolazione delle informazioni e le ingerenze da parte di attori stranieri. Per quanto riguarda le infrastrutture critiche nazionali, in considerazione delle possibili conseguenze, dovrebbe essere data priorità alle infrastrutture critiche di significativa rilevanza transfrontaliera. Gli Stati membri sono incoraggiati ad adottare con urgenza le suddette misure di aumento della resilienza, se del caso, mantenendo nel contempo l'approccio di cui al quadro giuridico in evoluzione.

(6) La protezione delle infrastrutture critiche europee nei settori dell'energia e dei trasporti è attualmente disciplinata dalla direttiva 2008/114/CE del Consiglio ([2]), mentre la sicurezza delle reti e dei sistemi informativi nell'Unione, con particolare riguardo per le minacce di natura informatica, è assicurata dalla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio ([3]). Al fine di garantire un livello comune più elevato di resilienza e protezione delle infrastrutture critiche, della cibersicurezza e del mercato finanziario, il quadro giuridico esistente viene modificato e integrato tramite l'adozione di nuove norme applicabili ai soggetti critici («direttiva CER»), di norme rafforzate per un livello comune elevato di cibersicurezza nell'Unione («direttiva NIS 2») e di nuove norme applicabili alla resilienza operativa digitale per il settore finanziario («DORA»).

7) Gli Stati membri, conformemente al diritto dell'Unione e al diritto nazionale, dovrebbero avvalersi di tutti gli strumenti disponibili per proseguire in questa direzione e contribuire a rafforzare la resilienza fisica e informatica. A tale riguardo, fra le infrastrutture critiche dovrebbero rientrare le pertinenti infrastrutture critiche individuate da uno Stato membro a livello nazionale o designate come infrastrutture critiche europee a norma della direttiva 2008/114/CE, come pure i soggetti critici da individuare a norma della direttiva CER o, se del caso, i soggetti di cui alla direttiva NIS 2. Il concetto di resilienza dovrebbe essere inteso come riferito alla capacità di un'infrastruttura critica di prevenire, proteggere, rispondere, resistere, attenuare, assorbire, adattarsi o recuperare rispetto a eventi che perturbano in modo significativo o che possono perturbare in modo significativo la fornitura di servizi essenziali nel mercato interno, vale a dire servizi cruciali per mantenere le funzioni vitali della società e dell'economia, la pubblica sicurezza, l'incolumità pubblica, la salute della popolazione o l'ambiente.

8) È opportuno convocare esperti nazionali per coordinare i lavori volti a conseguire un livello comune più elevato di resilienza e protezione delle infrastrutture critiche che sarà introdotto dalle nuove norme applicabili ai soggetti critici. Tale lavoro coordinato consentirebbe la cooperazione tra gli Stati membri e la condivisione di informazioni relative ad attività quali l'elaborazione di metodologie per individuare i servizi essenziali forniti dalle infrastrutture critiche. La Commissione ha già iniziato a convocare tali esperti e a facilitarne il lavoro, e intende proseguire in questa direzione. Una volta entrata in vigore la direttiva CER e istituito un gruppo per la resilienza dei soggetti critici a norma di detta direttiva, tale lavoro di anticipazione dovrebbe essere portato avanti da questo gruppo conformemente ai compiti ad esso attribuiti.

9) Prendendo atto del mutato scenario delle minacce, è opportuno sviluppare ulteriormente le possibilità di effettuare prove di stress sulle infrastrutture critiche a livello nazionale, giacché tali prove potrebbero rivelarsi utili per rafforzare la resilienza delle infrastrutture critiche. Per quanto riguarda l'importanza specifica del settore dell'energia, così come le conseguenze a livello dell'Unione di una sua possibile perturbazione, tale settore potrebbe trarre massimo beneficio dall'effettuazione di prove di stress secondo principi concordati. Tali prove rientrano nelle competenze degli Stati membri, i quali dovrebbero incoraggiare e sostenere gli operatori delle infrastrutture critiche a effettuare dette prove, laddove ritenute vantaggiose e conformi ai rispettivi quadri giuridici nazionali.

([2]) Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione (GU L 345 del 23.12.2008, pag. 75).

([3]) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1).

10) Al fine di garantire una risposta coordinata ed efficace alle minacce attuali e previste, la Commissione è incoraggiata a fornire un sostegno supplementare agli Stati membri, in particolare fornendo informazioni pertinenti sotto forma di istruzioni, manuali e orientamenti non vincolanti. Il servizio europeo per l'azione esterna (SEAE), in particolare attraverso il Centro UE di situazione e di intelligence e la sua cellula per l'analisi delle minacce ibride, con il sostegno della direzione «Intelligence» dello Stato maggiore dell'Unione europea (EUMS) nel quadro della capacità unica di analisi dell'intelligence (SIAC), dovrebbe fornire valutazioni delle minacce. La Commissione è inoltre invitata, in cooperazione con gli Stati membri, a promuovere l'adozione di progetti di ricerca e innovazione finanziati dall'Unione.

11) Con la crescente interdipendenza delle infrastrutture fisiche e digitali, è possibile che le attività informatiche dolose rivolte a settori critici causino perturbazioni o danni alle infrastrutture fisiche o che il sabotaggio delle infrastrutture fisiche renda i servizi digitali inaccessibili. Gli Stati membri sono invitati ad accelerare i lavori preparatori per il recepimento e l'applicazione del nuovo quadro giuridico applicabile ai soggetti critici e del quadro giuridico rafforzato per la cibersicurezza, sulla scorta dell'esperienza acquisita in seno al gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 («gruppo di cooperazione NIS»), il più presto possibile, tenendo conto dei termini per il recepimento e del fatto che tali lavori preparatori dovrebbero progredire in parallelo e in modo coerente.

12) Oltre a migliorare la preparazione, è importante rafforzare la capacità di rispondere in modo rapido ed efficace a una perturbazione dei servizi essenziali forniti dalle infrastrutture critiche. La presente raccomandazione contiene pertanto misure a livello sia dell'Unione che nazionale, anche sottolineando il ruolo di sostegno e il valore aggiunto che si possono ottenere introducendo una cooperazione rafforzata e uno scambio di informazioni nel contesto del meccanismo unionale di protezione civile (UCPM) istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio ([4]) e utilizzando le risorse pertinenti del programma spaziale dell'Unione istituito a norma del regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio ([5]).

13) La Commissione, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza («alto rappresentante») e il gruppo di cooperazione NIS, in collaborazione con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), devono effettuare una valutazione dei rischi ed elaborare scenari di rischio. In aggiunta, sulla scorta dell'invito ministeriale congiunto di Nevers, una valutazione dei rischi è attualmente condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'Agenzia europea per la cibersicurezza (ENISA) e in cooperazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC). Questi due esercizi saranno coerenti e coordinati con l'elaborazione di scenari nel quadro dell'UCPM, compresi gli eventi di cibersicurezza e il loro impatto reale, attualmente condotta dalla Commissione e dagli Stati membri. Ai fini dell'efficienza, dell'efficacia e della coerenza, nonché per la corretta applicazione della presente raccomandazione, i risultati di tali esercizi dovrebbero essere rispecchiati a livello nazionale.

14) Per potenziare immediatamente la preparazione e la capacità di rispondere agli incidenti di cibersicurezza su vasta scala, la Commissione ha istituito un programma a breve termine volto a sostenere gli Stati membri attraverso finanziamenti aggiuntivi assegnati all'ENISA. Tra i servizi proposti figurano, tra l'altro, azioni di preparazione, quali test di penetrazione dei soggetti al fine di individuare le vulnerabilità. Il programma può inoltre rafforzare le possibilità di assistere gli Stati membri in caso di incidenti di cibersicurezza su vasta scala che colpiscano soggetti critici. Si tratta di un primo passo in linea con le conclusioni del Consiglio del 23 maggio 2022 sull'elaborazione di una posizione dell'Unione europea in materia di deterrenza informatica («conclusioni del Consiglio sulla posizione dell'UE in materia di deterrenza informatica»), in cui si invita la Commissione a presentare una proposta su un Fondo di risposta alle emergenze di cibersicurezza. Gli Stati membri dovrebbero sfruttare appieno tali opportunità, nel rispetto dei requisiti applicabili, e sono incoraggiati a proseguire i lavori nel settore della gestione delle crisi informatiche dell'Unione, in particolare monitorando e facendo il punto periodicamente dei progressi compiuti nell'attuazione della tabella di marcia per la gestione delle crisi informatiche, elaborata di recente in sede di Consiglio. Tale tabella di marcia è un documento in divenire che dovrebbe essere rivisto e aggiornato ove necessario.

([4]) 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).

([5]) Regolamento (UE) 2021/696 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e che abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE (GU L 170 del 12.5.2021, pag. 69).

15) I cavi di comunicazione sottomarini globali sono essenziali per la connettività a livello mondiale e all'interno dell'UE. Poiché i cavi sono molto lunghi e installati sul fondo marino, il monitoraggio visivo subacqueo della maggior parte delle loro sezioni è estremamente impegnativo. La competenza condivisa e altre questioni giurisdizionali relative a tali cavi rappresentano un argomento specifico a favore della cooperazione europea e internazionale in materia di protezione e recupero delle infrastrutture. È pertanto necessario integrare le valutazioni dei rischi, tanto in corso quanto pianificate, relative alle infrastrutture digitali e fisiche su cui si basano i servizi digitali con valutazioni dei rischi e possibili misure di attenuazione specifiche per i cavi di comunicazione sottomarini. Gli Stati membri invitano la Commissione a effettuare studi a tal fine e a trasmettere loro le sue conclusioni.

16) Sui settori dell'energia e dei trasporti possono incidere anche le minacce relative alle infrastrutture digitali, ad esempio in relazione alle tecnologie energetiche che comprendono componenti digitali. La sicurezza delle catene di approvvigionamento associate è importante per la continuità della fornitura di servizi essenziali e per il controllo strategico delle infrastrutture critiche nel settore energetico. È opportuno tenerne conto al momento di adottare misure volte a rafforzare la resilienza delle infrastrutture critiche conformemente alla presente raccomandazione.

17) Data la crescente importanza delle infrastrutture spaziali, delle risorse di terra relative allo spazio — compresi gli impianti di produzione — e dei servizi spaziali per le attività connesse alla sicurezza, è essenziale garantire la resilienza e la protezione dello spazio dell'Unione come pure delle sue risorse e dei suoi servizi di terra all'interno dell'Unione. Per le stesse ragioni, è essenziale anche, nel quadro della presente raccomandazione, utilizzare in modo più strutturato i dati e i servizi spaziali, che sono forniti dai sistemi e dai programmi spaziali per la sorveglianza e il tracciamento e per la protezione delle infrastrutture critiche in altri settori. La futura strategia spaziale dell'UE per la sicurezza e la difesa proporrà azioni adeguate al riguardo, di cui si dovrebbe tenere conto nell'attuazione della presente raccomandazione.

18) Occorre inoltre cooperare a livello internazionale così da affrontare efficacemente i rischi per le infrastrutture critiche, tra l'altro, nelle acque internazionali. Gli Stati membri sono pertanto invitati a cooperare con la Commissione e l'alto rappresentante per adottare misure al fine di realizzare tale cooperazione, ricordando che dovrebbero intervenire solo in conformità dei rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, in particolare delle disposizioni dei trattati in materia di relazioni esterne.

19) Come stabilito nella comunicazione del 15 febbraio 2022 dal titolo «Contributo della Commissione alla difesa europea», a sostegno della «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», entro il 2023 la Commissione valuterà, in cooperazione con l'alto rappresentante e gli Stati membri, i parametri di riferimento settoriali per la resilienza contro le minacce ibride al fine di individuare le lacune e i bisogni, così come le misure atte a colmare le prime e soddisfare i secondi. Tale iniziativa dovrebbe orientare i lavori previsti dalla presente raccomandazione, contribuendo a intensificare la condivisione delle informazioni e il coordinamento delle azioni per aumentare la resilienza, compresa quella delle infrastrutture critiche.

20) La strategia per la sicurezza marittima dell'Unione europea del 2014 e il relativo piano d'azione riveduto esortavano ad aumentare la protezione delle infrastrutture marittime critiche, incluse quelle subacquee, e in particolare delle infrastrutture marittime nel settore dei trasporti, dell'energia e della comunicazione, tra l'altro promuovendo la conoscenza della situazione marittima attraverso il miglioramento dell'interoperabilità e l'ottimizzazione dello scambio (obbligatorio e volontario) di informazioni. La strategia e il piano d'azione sono attualmente in fase di aggiornamento e comprenderanno azioni rafforzate volte a proteggere le infrastrutture marittime critiche. Tali azioni dovrebbero integrare la presente raccomandazione.

21) Il rafforzamento della resilienza delle infrastrutture critiche contribuisce a intensificare gli sforzi per contrastare le minacce e le campagne ibride contro l'Unione e i suoi Stati membri. La presente raccomandazione si basa sulla comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo «Quadro congiunto per contrastare le minacce ibride — La risposta dell'Unione europea». L'azione 1 del quadro congiunto, vale a dire lo studio sui rischi ibridi, svolge un ruolo fondamentale nell'individuare le vulnerabilità che possono interessare strutture e reti nazionali e paneuropee. Inoltre, l'attuazione delle conclusioni del Consiglio del 21 giugno 2022 su un quadro per una risposta coordinata dell'UE alle campagne ibride fornirà un'azione coordinata più forte attraverso l'applicazione del pacchetto di strumenti dell'UE contro le minacce ibride in tutti i settori interessati,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

CAPO I: OBIETTIVO, AMBITO DI APPLICAZIONE E DEFINIZIONE DELLE PRIORITÀ

1) La presente raccomandazione stabilisce una serie di azioni mirate a livello dell'Unione e nazionale per sostenere e rafforzare la resilienza delle infrastrutture critiche, su base volontaria, con particolare attenzione alle infrastrutture critiche di significativa rilevanza transfrontaliera e in determinati settori chiave, quali l'energia, le infrastrutture digitali, i trasporti e lo spazio. Tali azioni mirate riguardano una maggiore preparazione, una risposta rafforzata e la cooperazione internazionale.

2) Le informazioni condivise al fine di conseguire gli obiettivi della presente raccomandazione che sono riservate ai sensi della normativa dell'Unione e nazionale, nonché di quella sulla riservatezza commerciale dovrebbero essere scambiate con la Commissione e con altre autorità competenti solo nella misura in cui tale scambio sia necessario ai fini della corretta applicazione della presente raccomandazione. La presente raccomandazione non pregiudica la tutela degli interessi essenziali della sicurezza nazionale, della sicurezza pubblica o della difesa degli Stati membri e non ci si dovrebbe aspettare da nessuno Stato membro che condivida informazioni contrarie a tali interessi.

CAPO II: MIGLIORAMENTO DELLA PREPARAZIONE

Azioni a livello degli Stati membri

3) Gli Stati membri dovrebbero prendere in considerazione un approccio multirischio nell'aggiornare le loro valutazioni dei rischi o le loro analisi equivalenti esistenti, in linea con la natura evolutiva delle attuali minacce alle loro infrastrutture critiche, in particolare in determinati settori chiave e, ove possibile, in tutti i settori contemplati dal nuovo imminente quadro giuridico applicabile ai soggetti critici.

4) Gli Stati membri sono invitati ad accelerare i lavori preparatori e ad adottare misure di rafforzamento della resilienza, ove possibile, come previsto dall'imminente quadro giuridico applicabile ai soggetti critici, con particolare attenzione alla cooperazione e alla condivisione delle informazioni pertinenti tra gli Stati membri e con la Commissione, all'individuazione dei soggetti critici di significativa rilevanza transfrontaliera e al rafforzamento del sostegno ai soggetti critici individuati al fine di renderli più resilienti.

5) Gli Stati membri dovrebbero sostenere la formazione e le esercitazioni degli esperti nonché la condivisione tra esperti delle migliori pratiche e degli insegnamenti tratti. Gli Stati membri dovrebbero incoraggiare gli esperti a partecipare alle piattaforme di formazione esistenti, sia nazionali che internazionali, ad esempio nell'ambito dell'UCPM.

6) Gli Stati membri dovrebbero incoraggiare e sostenere gli operatori delle infrastrutture critiche almeno nel settore dell'energia affinché effettuino prove di stress, seguendo principi concordati a livello dell'Unione, ove ciò sia vantaggioso. Le prove di stress dovrebbero valutare la resilienza delle infrastrutture critiche alle minacce antagoniste di origine umana. Pertanto, gli Stati membri dovrebbero mirare a individuare le pertinenti infrastrutture critiche da sottoporre alle prove e a consultare i pertinenti operatori delle infrastrutture critiche quanto prima e comunque entro la fine del primo trimestre del 2023. Inoltre, gli Stati membri dovrebbero sostenere gli operatori delle infrastrutture critiche affinché effettuino tali prove il prima possibile e mirino a completarle entro la fine del 2023, conformemente al diritto nazionale. Il Consiglio intende valutare lo stato dei lavori sulle prove di stress entro la fine di aprile 2023.

7) A causa della rapida evoluzione delle minacce alle infrastrutture critiche, il mantenimento di un elevato livello di protezione è di vitale importanza. Gli Stati membri sono incoraggiati a stanziare risorse finanziarie sufficienti per rafforzare le capacità delle rispettive autorità nazionali competenti e a sostenerle, al fine di essere in grado di migliorare la resilienza delle infrastrutture critiche. Gli Stati membri sono inoltre incoraggiati a stanziare risorse finanziarie sufficienti per le autorità responsabili della gestione degli incidenti di cibersicurezza su vasta scala, a sostenerle e a garantire che i loro gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e le loro autorità competenti siano pienamente mobilitati rispettivamente nella rete CSIRT e nella rete EU-CyCLONe.

8) Gli Stati membri sono invitati a sfruttare, conformemente ai requisiti applicabili, le potenziali opportunità di finanziamento a livello dell'Unione e nazionale per rafforzare la resilienza delle infrastrutture critiche nell'Unione, nonché a incoraggiare gli operatori delle infrastrutture critiche a sfruttare tali opportunità di finanziamento, ivi comprese ad esempio le reti transeuropee, contro l'intera gamma di minacce significative, in particolare nell'ambito dei programmi finanziati dal Fondo Sicurezza interna istituito dal regolamento (UE) 2021/1149 del Parlamento europeo e del Consiglio ([6]), dal Fondo europeo di sviluppo regionale istituito dal regolamento (UE) n. 1301/2013 del Parlamento europeo e del Consiglio ([7]), dall'UCPM e dal piano REPowerEU della Commissione. Gli Stati membri sono inoltre incoraggiati a utilizzare al meglio i risultati dei progetti pertinenti nell'ambito dei programmi di ricerca, come Orizzonte Europa, istituito dal regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio ([8]).

9) Per quanto riguarda le infrastrutture di comunicazione e di rete nell'Unione, il gruppo di cooperazione NIS è invitato, in conformità dell'articolo 11 della direttiva (UE) 2016/1148, ad accelerare i lavori in corso sull'invito ministeriale congiunto di Nevers su una valutazione mirata dei rischi e dovrebbe presentare quanto prima le prime raccomandazioni. Tale valutazione dei rischi dovrebbe fornire informazioni per i lavori in corso relativi alla valutazione intersettoriale dei rischi di cibersicurezza e all'elaborazione di scenari, richieste dal Consiglio nelle conclusioni sulla posizione dell'UE in materia di deterrenza informatica. Tale lavoro dovrebbe inoltre essere svolto garantendo coerenza e complementarità con l'operato del gruppo di cooperazione NIS sulla sicurezza della catena di approvvigionamento delle tecnologie dell'informazione e della comunicazione e di altri gruppi pertinenti.

10) Il gruppo di cooperazione NIS è inoltre invitato, con il sostegno della Commissione e dell'ENISA, a proseguire i lavori sulla sicurezza delle infrastrutture digitali, anche in relazione alle infrastrutture sottomarine, in particolare ai cavi di comunicazione sottomarini, e ad avviare altresì i lavori sul settore spaziale, anche preparando, ove necessario, orientamenti strategici e metodologie di gestione dei rischi di cibersicurezza secondo un approccio multirischio e un approccio basato sul rischio per gli operatori del settore spaziale, al fine di aumentare la resilienza delle infrastrutture di terra da cui dipende la fornitura di servizi spaziali.

11) Gli Stati membri dovrebbero sfruttare appieno i servizi di preparazione in materia di cibersicurezza offerti dal programma di sostegno a breve termine attuato dalla Commissione con l'ENISA, ad esempio i test di penetrazione per individuare le vulnerabilità, e in tale contesto sono esortati a dare priorità ai soggetti che gestiscono infrastrutture critiche nei settori dell'energia, delle infrastrutture digitali e dei trasporti.

12) Gli Stati membri dovrebbero sfruttare appieno il Centro europeo di competenza per la cibersicurezza. Gli Stati membri dovrebbero incoraggiare i propri centri nazionali di coordinamento a dialogare in modo proattivo con i membri della comunità di cibersicurezza per sviluppare capacità a livello dell'Unione e nazionale al fine di sostenere meglio gli operatori di servizi essenziali.

13) È importante che gli Stati membri attuino le misure raccomandate nel pacchetto di strumenti dell'UE sulla cibersicurezza delle reti 5G e, in particolare, che introducano restrizioni nei confronti dei fornitori ad alto rischio, considerando che i ritardi possono aumentare la vulnerabilità delle reti nell'Unione, e inoltre che rafforzino la protezione fisica e non fisica delle parti critiche e sensibili delle reti 5G, anche tramite rigorosi controlli dell'accesso. Inoltre gli Stati membri, in cooperazione con la Commissione, dovrebbero valutare la necessità di un'azione complementare per garantire un livello coerente di sicurezza e resilienza delle reti 5G.

14) Gli Stati membri, insieme alla Commissione e all'ENISA, dovrebbero concentrarsi sull'attuazione delle conclusioni del Consiglio del 17 ottobre 2022 sulla sicurezza della catena di approvvigionamento delle TIC.

([6]) Regolamento (UE) 2021/1149 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che istituisce il Fondo Sicurezza interna (GU L 251 del 15.7.2021, pag. 94).

([7]) Regolamento (UE) n. 1301/2013 del Parlamento europeo e del Consiglio, del 17 dicembre 2013, relativo al Fondo europeo di sviluppo regionale e a disposizioni specifiche concernenti l'obiettivo «Investimenti a favore della crescita e dell'occupazione» e che abroga il regolamento (CE) n. 1080/2006 (GU L 347 del 20.12.2013, pag. 289).

([8]) Regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa e ne stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013 (GU L 170 del 12.5.2021, pag. 1).

15) Gli Stati membri dovrebbero tenere conto del prossimo codice di rete per gli aspetti di cibersicurezza dei flussi transfrontalieri di energia elettrica[...] sulla base dell'esperienza acquisita con l'attuazione della direttiva (UE) 2016/1148 e dei relativi orientamenti elaborati dal gruppo di cooperazione NIS, in particolare il documento di riferimento sulle misure di sicurezza per gli operatori di servizi essenziali.

16) Gli Stati membri dovrebbero sviluppare l'uso di Copernicus, di Galileo e del Servizio europeo di copertura per la navigazione geostazionaria (EGNOS) a fini di sorveglianza con l'obiettivo di condividere le informazioni pertinenti con gli esperti convocati conformemente al punto 15. È opportuno fare buon uso delle capacità offerte dalle comunicazioni satellitari governative dell'Unione (GOVSATCOM) del programma spaziale dell'Unione per monitorare le infrastrutture critiche e sostenere la previsione delle crisi e la risposta a esse.

Azioni a livello dell'Unione

17) È opportuno rafforzare il dialogo e la cooperazione tra gli esperti designati dagli Stati membri e con la Commissione, al fine di aumentare la resilienza fisica delle infrastrutture critiche, in particolare:

a) contribuendo alla preparazione, allo sviluppo e alla promozione di strumenti volontari comuni per sostenere gli Stati membri nel rafforzamento di tale resilienza, comprese metodologie e scenari di rischio;

b) sostenendo gli Stati membri nell'attuazione del nuovo quadro giuridico applicabile ai soggetti critici, anche incoraggiando la Commissione ad adottare l'atto delegato in modo tempestivo;

c) sostenendo la realizzazione delle prove di stress di cui al punto 6, sulla base di principi comuni, a cominciare dalle prove incentrate sulle minacce antagoniste di origine umana nel settore dell'energia e successivamente in altri settori chiave, e fornendo sostegno e consulenza in merito allo svolgimento di tali prove di stress, su richiesta di uno Stato membro;

d) facendo uso di qualsiasi piattaforma sicura — una volta istituita dalla Commissione — per raccogliere, valutare e condividere, su base volontaria, le migliori pratiche, gli insegnamenti tratti dalle esperienze nazionali e altre informazioni relative a tale resilienza.

Il lavoro di tali esperti designati dovrebbe prestare particolare attenzione alle dipendenze intersettoriali e alle infrastrutture critiche di significativa rilevanza transfrontaliera, e dovrebbe essere proseguito in sede di Consiglio e di Commissione, ove opportuno.

18) Gli Stati membri sono incoraggiati a sfruttare qualsiasi sostegno offerto dalla Commissione, ad esempio attraverso la preparazione di manuali e orientamenti come il manuale sulla protezione delle infrastrutture critiche e degli spazi pubblici contro i sistemi di aeromobili senza equipaggio, e strumenti per la valutazione dei rischi. Il SEAE, in particolare attraverso il Centro UE di situazione e di intelligence e la sua cellula per l'analisi delle minacce ibride, con il sostegno della direzione «Intelligence» dell'EUMS nel quadro del SIAC, è invitato a elaborare note sulle minacce alle infrastrutture critiche nell'Unione al fine di migliorare la conoscenza situazionale.

19) Gli Stati membri dovrebbero favorire le azioni intraprese dalla Commissione per sfruttare i risultati dei progetti sulla resilienza delle infrastrutture critiche finanziati nell'ambito dei programmi di ricerca e innovazione dell'Unione. Il Consiglio prende atto dell'intenzione della Commissione di aumentare i finanziamenti a favore della resilienza, nell'ambito del bilancio assegnato a Orizzonte Europa nel quadro finanziario pluriennale 2021-2027, senza pregiudicare gli altri progetti per la ricerca e l'innovazione in materia di sicurezza civile nell'ambito di Orizzonte Europa.

20) In ragione dei compiti previsti nelle conclusioni del Consiglio sulla posizione dell'UE in materia di deterrenza informatica, la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS sono invitati a intensificare, conformemente ai rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, la collaborazione con le reti e gli organismi e le agenzie civili e militari competenti per valutare i rischi ed elaborare scenari di rischio in relazione alla cibersicurezza, tenendo conto in particolare dell'importanza delle infrastrutture dell'energia, digitali, dei trasporti e dello spazio e delle interdipendenze tra i diversi settori e tra gli Stati membri. Tale esercizio dovrebbe tenere conto dei relativi rischi per le infrastrutture su cui si basano questi settori. Ove vantaggioso, la valutazione e gli scenari di rischio potrebbero svolgersi su base regolare e dovrebbero integrare le valutazioni dei rischi già esistenti o previste in questi settori, basarsi su di esse ed evitare duplicazioni, nonché orientare le discussioni su come rafforzare la resilienza complessiva dei soggetti che gestiscono infrastrutture critiche e affrontare le vulnerabilità.

21) Conformemente ai suoi compiti nell'ambito della gestione delle crisi informatiche, la Commissione è invitata ad accelerare le sue attività volte a sostenere la preparazione e la risposta degli Stati membri agli incidenti di cibersicurezza su vasta scala, e in particolare:

a) effettuare, a complemento delle pertinenti valutazioni dei rischi nel contesto della sicurezza delle reti e dell'informazione, uno studio completo ([9]) che faccia il punto sulle infrastrutture sottomarine, in particolare sui cavi di comunicazione sottomarini che collegano gli Stati membri e l'Europa nel suo insieme al resto del mondo, i cui risultati dovrebbero essere condivisi con gli Stati membri;

b) sostenere la preparazione e la risposta degli Stati membri e delle istituzioni, degli organi e degli organismi dell'Unione agli incidenti di cibersicurezza su vasta scala o agli incidenti gravi, conformemente al quadro giuridico rafforzato per la cibersicurezza e ad altre norme pertinenti applicabili ([10]);

c) accelerare lo sviluppo del concetto principale del Fondo di risposta alle emergenze di cibersicurezza con un'adeguata discussione con gli Stati membri.

22) La Commissione è incoraggiata a intensificare i lavori su azioni preventive lungimiranti, anche in collaborazione con gli Stati membri a norma degli articoli 6 e 10 della decisione n. 1313/2013/UE, e sotto forma di pianificazione di emergenza a sostegno della preparazione operativa e della risposta del Centro di coordinamento della risposta alle emergenze (ERCC) alle perturbazioni delle infrastrutture critiche; ad aumentare gli investimenti negli approcci preventivi e nella preparazione della popolazione; aumentare il sostegno relativo allo sviluppo di capacità nell'ambito della rete unionale della conoscenza in materia di protezione civile.

23) La Commissione dovrebbe promuovere l'uso delle risorse di sorveglianza dell'Unione (Copernicus, Galileo ed EGNOS) per aiutare gli Stati membri a monitorare le infrastrutture critiche e, se del caso, le loro immediate vicinanze, e per sostenere altre opzioni di sorveglianza previste dal programma spaziale dell'Unione, come il quadro in materia di conoscenza dell'ambiente spaziale e il quadro UE in materia di sorveglianza dello spazio e tracciamento.

24) Se del caso, le agenzie e gli altri organismi competenti dell'Unione sono invitati a fornire sostegno, conformemente ai rispettivi mandati, su questioni relative alla resilienza delle infrastrutture critiche, in particolare:

a) l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) per quanto riguarda la raccolta di informazioni, l'analisi dei fenomeni criminali e il sostegno investigativo nelle azioni di contrasto transfrontaliere e, ove pertinente e opportuno, la condivisione dei risultati con gli Stati membri;

b) l'Agenzia europea per la sicurezza marittima (EMSA) su questioni relative alla sicurezza e protezione del settore marittimo nell'Unione, compresi i servizi di sorveglianza marittima a tal fine;

c) l'Agenzia dell'Unione europea per il programma spaziale (EUSPA) e il Centro satellitare dell'UE (Satcen) possono essere in grado di fornire assistenza attraverso operazioni nell'ambito del programma spaziale dell'Unione;

d) il Centro europeo di competenza per la cibersicurezza per quanto riguarda le attività connesse alla cibersicurezza, anche in cooperazione con l'ENISA, potrebbe sostenere l'innovazione e la politica industriale in materia di cibersicurezza.

([9]) Tale studio dovrebbe comprendere la mappatura delle capacità e delle ridondanze, vulnerabilità e minacce, nonché dei rischi per la disponibilità dei servizi, come pure dell'impatto dei tempi di inattività dei cavi sottomarini (transatlantici) per gli Stati membri e l'Unione nel complesso e l'attenuazione dei rischi, tenendo conto nel contempo della sensibilità di tali informazioni e dell'esigenza di proteggerle.

([10]) È inoltre opportuno riservare particolare attenzione a tutte le attività che preparano una risposta efficace e coordinata a livello dell'Unione nel caso di un grave incidente di cibersicurezza transfrontaliero o di una minaccia connessa che potrebbe avere un impatto sistemico sul settore finanziario dell'Unione, come previsto dal nuovo quadro giuridico sulla resilienza operativa digitale.

CAPO III: UNA RISPOSTA RAFFORZATA

Azioni a livello degli Stati membri

25) Gli Stati membri sono invitati a:

a) proseguire il coordinamento della loro risposta e, se del caso, mantenere una visione d'insieme della risposta intersettoriale alle gravi perturbazioni dei servizi essenziali forniti dalle infrastrutture critiche. Ciò potrebbe essere fatto nel quadro di un futuro programma per una risposta coordinata alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera, degli esistenti dispositivi integrati per la risposta politica alle crisi (IPCR) per il coordinamento della risposta politica in materia di infrastrutture critiche di rilevanza transfrontaliera, del programma per gli incidenti e le crisi di cibersicurezza su vasta scala di cui alla raccomandazione (UE) 2017/1584 della Commissione ([11]), di EU-CyCLONe, nel quadro di una risposta coordinata dell'UE alle campagne ibride e del pacchetto di strumenti dell'UE contro le minacce ibride in caso di minacce e campagne ibride e del sistema di allarme rapido in caso di disinformazione;

b) intensificare lo scambio di informazioni a livello operativo con l'ERCC nel quadro dell'UCPM al fine di migliorare l'allarme rapido e coordinare la loro risposta nell'ambito dell'UCPM in caso di perturbazioni di infrastrutture critiche di significativa rilevanza transfrontaliera, così da garantire, ove necessario, una reazione più rapida con il sostegno dell'Unione;

c) aumentare la capacità di reagire prontamente, se del caso, mediante strumenti esistenti o da sviluppare, a tali gravi perturbazioni di cui alla lettera a);

d) collaborare per sviluppare ulteriormente i pertinenti mezzi di risposta nell'ambito del pool europeo di protezione civile e di rescEU;

e) incoraggiare gli operatori delle infrastrutture critiche e le autorità nazionali competenti a rafforzare le loro capacità per poter ripristinare rapidamente le prestazioni di base dei servizi essenziali forniti da tali operatori delle infrastrutture critiche;

f) incoraggiare gli operatori delle infrastrutture critiche, in sede di ricostruzione delle infrastrutture critiche, a costruirle in modo che siano il più resilienti possibile, tenendo conto della proporzionalità delle misure in relazione alle valutazioni dei rischi e ai costi, rispetto all'intera gamma di rischi significativi a cui possono essere esposte, anche in scenari climatici avversi.

26) Gli Stati membri sono invitati ad accelerare i lavori preparatori, ove possibile, come prescritto dal quadro giuridico rafforzato in materia di cibersicurezza, mirando al rafforzamento delle capacità dei CSIRT nazionali in considerazione dei nuovi compiti dei CSIRT e del maggior numero di soggetti di nuovi settori, riesaminando e aggiornando le loro strategie di cibersicurezza in maniera tempestiva e adottando quanto prima piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza, se non ancora esistenti.

27) Gli Stati membri sono invitati a prendere in considerazione, a livello nazionale, i mezzi più pertinenti per garantire che i portatori di interessi siano consapevoli della necessità di promuovere la resilienza delle infrastrutture critiche cooperando con fornitori e partner affidabili. È importante investire in capacità supplementari, in particolare nei settori in cui le infrastrutture attuali si trovano al termine del loro ciclo di vita (ad esempio, infrastrutture per le comunicazioni sottomarine via cavo), al fine di poter garantire la continuità della fornitura dei servizi essenziali in caso di perturbazioni e ridurre dipendenze indesiderate.

28) Gli Stati membri sono incoraggiati a prestare attenzione a una comunicazione strategica proattiva a livello nazionale nel contesto del contrasto delle minacce e campagne ibride, anche considerando la possibilità che gli avversari cerchino di partecipare alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri, contribuendo alle narrazioni relative agli incidenti a carico di infrastrutture critiche.

Azioni a livello dell'Unione

29) La Commissione è invitata a collaborare strettamente con gli Stati membri per sviluppare ulteriormente gli organismi, gli strumenti e le capacità di risposta del caso, al fine di migliorare la preparazione operativa per affrontare gli effetti immediati e indiretti di perturbazioni significative dei servizi essenziali forniti dalle infrastrutture critiche, in particolare esperti e risorse disponibili tramite il pool europeo di protezione civile e rescEU nell'ambito dell'UCPM o futuri gruppi di risposta rapida alle minacce ibride.

([11]) 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).

30) Tenendo conto dell'evoluzione del panorama delle minacce e in cooperazione con gli Stati membri, nel contesto dell'UCPM la Commissione è invitata a:

a) analizzare e testare costantemente l'adeguatezza e la prontezza operativa delle capacità di risposta esistenti;

b) monitorare e individuare periodicamente le carenze potenzialmente significative nelle capacità di risposta del pool europeo di protezione civile e di rescEU;

c) intensificare ulteriormente la collaborazione intersettoriale per garantire una risposta adeguata a livello dell'Unione e organizzare formazioni o esercitazioni periodiche per testare tale collaborazione in cooperazione con uno o più Stati membri;

d) sviluppare ulteriormente l'ERCC quale polo di emergenza intersettoriale a livello dell'Unione per il coordinamento del sostegno agli Stati membri colpiti.

31) Il Consiglio si impegna ad avviare i lavori al fine di approvare un programma su una risposta coordinata a perturbazioni delle infrastrutture critiche di significativa rilevanza transfrontaliera, che descriva e definisca gli obiettivi e le modalità di cooperazione tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione nel rispondere agli incidenti a carico di tali infrastrutture critiche. Il Consiglio attende con interesse che la Commissione elabori tale programma, basandosi sul sostegno e sui contributi delle pertinenti agenzie dell'Unione. Il programma è pienamente coerente e interoperabile con il protocollo operativo riveduto dell'Unione relativo al contrasto delle minacce ibride («Manuale tattico dell'UE») e tiene conto del programma relativo alla risposta coordinata agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala ([12]) e del mandato per la rete UE delle organizzazioni di collegamento per le crisi informatiche (CyCLONe) stabilito nella direttiva NIS 2, ed evita la duplicazione di strutture e attività. Tale programma dovrebbe rispettare pienamente gli esistenti IPCR per il coordinamento della risposta.

32) La Commissione è invitata a consultare i pertinenti portatori di interessi ed esperti in merito a misure appropriate in relazione a possibili incidenti significativi riguardanti le infrastrutture sottomarine, da presentare congiuntamente allo studio di valutazione di cui al punto 20, lettera a), nonché a elaborare ulteriormente gli obiettivi definiti nella decisione sull'UCPM per quanto riguarda la pianificazione di emergenza, gli scenari di rischio e la resilienza dell'Unione alle catastrofi di cui alla decisione n. 1313/2013/UE.

CAPO IV: COOPERAZIONE INTERNAZIONALE

Azioni a livello degli Stati membri

33) Gli Stati membri dovrebbero cooperare, laddove opportuno e in conformità del diritto dell'Unione, con i paesi terzi interessati per quanto attiene alla resilienza delle infrastrutture critiche di significativa rilevanza transfrontaliera.

34) Gli Stati membri sono incoraggiati a cooperare con la Commissione e l'alto rappresentante al fine di affrontare efficacemente i rischi per le infrastrutture critiche nelle acque internazionali.

35) Gli Stati membri sono invitati a contribuire, in cooperazione con la Commissione e l'alto rappresentante, ad accelerare lo sviluppo e l'attuazione del pacchetto di strumenti dell'UE contro le minacce ibride e degli orientamenti di attuazione di cui alle conclusioni del Consiglio del 21 giugno 2022 su un quadro per una risposta coordinata dell'UE alle campagne ibride e in seguito a utilizzarle, per attuare pienamente tale quadro, in particolare al momento di esaminare e preparare risposte globali e coordinate dell'Unione alle campagne ibride e alle minacce ibride, comprese quelle nei confronti degli operatori delle infrastrutture critiche.

([12]) Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

Azioni a livello dell'Unione

36) La Commissione e l'alto rappresentante sono invitati a sostenere, se del caso e conformemente ai rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, i paesi terzi interessati per rafforzare la resilienza delle infrastrutture critiche nel loro territorio, in particolare delle infrastrutture critiche fisicamente collegate al loro territorio e a quello di uno Stato membro.

37) La Commissione e l'alto rappresentante, in linea con i rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, rafforzeranno il coordinamento con la NATO sulla resilienza delle infrastrutture critiche di interesse comune attraverso il dialogo strutturato UE-NATO sulla resilienza, nel pieno rispetto delle competenze dell'Unione e degli Stati membri conformemente ai trattati e ai principi guida fondamentali della cooperazione UE-NATO concordati dal Consiglio europeo, in particolare la reciprocità, l'inclusività e l'autonomia decisionale. In tale contesto, tale cooperazione sarà portata avanti nell'ambito del dialogo strutturato UE-NATO sulla resilienza, integrato nell'esistente meccanismo a livello di personale per l'attuazione delle dichiarazioni congiunte, garantendo nel contempo la piena trasparenza e il pieno coinvolgimento di tutti gli Stati membri.

38) La Commissione è invitata a prendere in considerazione la partecipazione di rappresentanti dei paesi terzi interessati, ove necessario e opportuno, nel quadro della cooperazione e dello scambio di informazioni tra gli Stati membri nel settore della resilienza delle infrastrutture critiche fisicamente collegate al territorio di uno Stato membro e a quello di un paese terzo.

Fatto a Bruxelles, il 8 dicembre 2022

Per il Consiglio
Il presidente
V. RAKUŠAN