COMMISSIONE
EUROPEA

Strasburgo, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Proposta di

RACCOMANDAZIONE DEL CONSIGLIO

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

(Testo rilevante ai fini del SEE)

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

La sicurezza è un obiettivo fondamentale dell'Unione europea. Sebbene la responsabilità primaria della protezione dei cittadini sia in capo agli Stati membri, l'azione collettiva a livello dell'Unione contribuisce in modo significativo alla sicurezza dell'UE nel suo insieme. Il coordinamento contribuisce a potenziare la resilienza, a migliorare la vigilanza e a rafforzare la nostra risposta collettiva. Nel contesto dell'Unione della sicurezza sono state adottate misure importanti per sviluppare mezzi e capacità di prevenzione, individuazione e risposta rapida a numerose minacce alla sicurezza, e per associare gli operatori del settore pubblico e privato in uno sforzo comune.

Dotare l'UE degli strumenti necessari per far fronte a uno scenario di minacce in continuo mutamento richiede una vigilanza e un adattamento costanti. La guerra di aggressione della Russia nei confronti dell'Ucraina ha portato nuovi rischi, spesso combinati come una minaccia ibrida. Uno di questi è il rischio di perturbazione nella fornitura di servizi essenziali da parte di soggetti che gestiscono infrastrutture critiche in Europa. Ciò è diventato tanto più evidente con l'apparente sabotaggio dei gasdotti Nord Stream e altri recenti incidenti. La società dipende fortemente dalle infrastrutture sia fisiche che digitali, e l'interruzione dei servizi essenziali, attraverso attacchi fisici tradizionali o attacchi informatici, o una combinazione di entrambi, può avere gravi conseguenze per il benessere dei cittadini, le nostre economie e la fiducia nei nostri sistemi democratici.

Garantire il regolare funzionamento del mercato interno è un altro obiettivo fondamentale dell'UE, anche quando ciò riguarda i servizi essenziali forniti dai soggetti che gestiscono le infrastrutture critiche. L'UE ha pertanto già adottato una serie di misure per ridurre le vulnerabilità e aumentare la resilienza dei soggetti critici, sia per quanto riguarda i rischi informatici che quelli non informatici.

Occorre intervenire con urgenza per rafforzare la capacità dell'Unione di far fronte ai potenziali attacchi contro le infrastrutture critiche, principalmente nella stessa UE ma, se del caso, anche nell'immediato vicinato.

La proposta di raccomandazione del Consiglio intende intensificare il sostegno dell'UE per il rafforzamento della resilienza delle infrastrutture critiche, e garantire un coordinamento a livello dell'UE in termini di preparazione e risposta. Mira a massimizzare e ad accelerare i lavori volti a proteggere le risorse, le strutture e i sistemi necessari per il funzionamento dell'economia e per la fornitura di servizi essenziali nel mercato interno, su cui i cittadini fanno affidamento, come pure ad attenuare l'impatto di qualsiasi attacco garantendo un recupero più rapido possibile. Tutte queste infrastrutture dovrebbero essere protette, ma la priorità principale è attualmente rappresentata dai settori dell'energia, delle infrastrutture digitali, dei trasporti e dello spazio in virtù del loro carattere specificamente orizzontale per la società e l'economia e delle attuali valutazioni dei rischi.

L'UE ha un ruolo particolare da svolgere nel garantire la resilienza delle infrastrutture a cavallo di frontiere terrestri o marittime, che incidono sugli interessi di diversi Stati membri, o che sono utilizzate per fornire servizi essenziali transfrontalieri. Le infrastrutture critiche rilevanti per più Stati membri possono tuttavia essere situate in un solo Stato membro o addirittura al di fuori del territorio di uno Stato membro, ad esempio nel caso di cavi o condotte sottomarini. Una chiara individuazione delle infrastrutture critiche e dei soggetti che

le gestiscono, nonché dei rischi che le minacciano, e un impegno collettivo a proteggerle, sono nell'interesse di tutti gli Stati membri e dell'UE nel suo insieme.

Il Parlamento europeo e il Consiglio hanno già raggiunto un accordo politico per approfondire il quadro legislativo dell'UE allo scopo di contribuire a rafforzare la resilienza dei soggetti che gestiscono infrastrutture critiche. Nell'estate del 2022 sono stati raggiunti accordi sulla direttiva sulla resilienza delle infrastrutture critiche ("direttiva CER")[1] e sulla direttiva riveduta sulla sicurezza dei sistemi informatici e di rete ("direttiva NIS2")[2]. Ciò rappresenterà una notevole intensificazione delle capacità rispetto al quadro legislativo in vigore, la direttiva 2008/114/CE, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione ("direttiva ECI")[3], e la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("direttiva NIS")[4]. La nuova legislazione dovrebbe entrare in vigore alla fine del 2022 o all'inizio del 2023 e il recepimento e l'applicazione dovrebbero essere considerati prioritari dagli Stati membri, conformemente al diritto dell'Unione.

Ciò premesso, e data la potenziale urgenza di affrontare le minacce derivanti dalla guerra di aggressione della Russia nei confronti dell'Ucraina, alle misure delineate nella nuova legislazione dovrebbe essere accordata, ove possibile e opportuno, e fin da oggi, la più grande attenzione. Intensificando già adesso la cooperazione reciproca si contribuirebbe inoltre a dare slancio a un'attuazione efficace quando la nuova legislazione sarà pienamente in vigore.

Il risultato sarebbe quello di andare già oltre i quadri attuali, sia in termini di profondità dell'azione che di ampiezza dei settori interessati. La nuova direttiva CER propone un nuovo quadro di cooperazione come pure obblighi, per gli Stati membri e i soggetti critici, per rafforzare la resilienza fisica non informatica, contro le minacce naturali e di origine umana, dei soggetti che forniscono servizi essenziali nel mercato interno, specificando undici settori[5]. La direttiva NIS2 predisporrà un'ampia copertura settoriale per gli obblighi in materia di cibersicurezza. Ciò comporterà il nuovo obbligo per gli Stati membri di includere, se del caso, i cavi sottomarini nelle loro strategie di cibersicurezza.

La legislazione impone alla Commissione di assumere un ruolo di coordinamento sostanziale. La direttiva CER prevede che la Commissione abbia un ruolo di sostegno e facilitazione, da svolgere con l'aiuto e il coinvolgimento del gruppo per la resilienza dei soggetti critici (CERG) istituito da tale direttiva, e che dovrebbe integrare le attività degli Stati membri sviluppando migliori prassi, metodologie e materiali di orientamento. Per quanto riguarda la cibersicurezza, il Consiglio, nelle sue conclusioni sulla posizione dell'UE in materia di sicurezza informatica dell'estate 2022, ha già invitato la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS a lavorare sulle valutazioni dei rischi e sugli scenari dal punto di vista della cibersicurezza. Tale coordinamento può ispirare un approccio analogo per altre infrastrutture critiche fondamentali.

Il 5 ottobre 2022 la presidente von der Leyen ha presentato un piano in cinque punti che definisce un approccio coordinato per i necessari lavori futuri. Gli elementi chiave sono i seguenti: rafforzare la preparazione; lavorare con gli Stati membri per sottoporre a prove di

---

1 COM(2020) 829 final
2 COM(2020) 823 final
3 GU L 345 del 23.12.2008
4 GU L 194 del 19.7.2016
5 Energia, trasporti, infrastrutture digitali, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, amministrazione pubblica, spazio e approvvigionamento alimentare.

stress le loro infrastrutture critiche, iniziando con il settore dell'energia e poi continuando con altri settori ad alto rischio; aumentare la capacità di risposta, in particolare attraverso il meccanismo di protezione civile dell'Unione; mettere a frutto la capacità satellitare per individuare potenziali minacce; e rafforzare la cooperazione con la NATO e i partner principali in materia di resilienza delle infrastrutture critiche. Il piano in cinque punti sottolinea l'importanza di anticipare la legislazione che già gode di un accordo politico.

La proposta di raccomandazione del Consiglio accoglie con favore tale approccio, volto a strutturare il sostegno agli Stati membri e a coordinare i loro sforzi in materia di sensibilizzazione ai rischi, preparazione e risposta alle minacce attuali. A tale riguardo, sono convocate riunioni di esperti per discutere della resilienza dei soggetti che gestiscono infrastrutture critiche in previsione dell'entrata in vigore della direttiva CER e del CERG istituito da tale direttiva.

Sarà essenziale rafforzare la cooperazione con i partner principali, i paesi vicini e altri paesi terzi rilevanti in materia di resilienza dei soggetti che gestiscono infrastrutture critiche, in particolare attraverso il dialogo strutturato UE-NATO sulla resilienza.

Il fulcro della presente raccomandazione è il rafforzamento della capacità dell'Unione di anticipare, prevenire e rispondere alle nuove minacce derivanti dalla guerra di aggressione della Russia nei confronti dell'Ucraina. Le raccomandazioni proposte si concentrano pertanto sui rischi correlati alla sicurezza e sulle minacce alle infrastrutture critiche. Andrebbe tuttavia osservato che i recenti avvenimenti hanno anche sottolineato l'incalzante necessità di prestare maggiore attenzione alle conseguenze dei cambiamenti climatici sulle infrastrutture e sui servizi critici in termini, ad esempio, di disponibilità idriche stagionali compromesse e non prevedibili per il raffreddamento delle centrali nucleari, le centrali idroelettriche e la navigazione interna, o rischio di danni materiali alle infrastrutture di trasporto, che possono causare gravi perturbazioni dei servizi essenziali. Tali preoccupazioni continueranno ad essere affrontate attraverso la legislazione e il coordinamento pertinenti.

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

La presente proposta di raccomandazione del Consiglio è pienamente in linea con il quadro giuridico attuale e futuro sulla resilienza dei soggetti che gestiscono infrastrutture critiche, rispettivamente la direttiva ECI e la direttiva CER, in quanto è volta, tra l'altro, a facilitare la cooperazione tra gli Stati membri in questo settore e a sostenere misure concrete per rafforzare la resilienza alle attuali minacce imminenti nei confronti dei soggetti che gestiscono infrastrutture critiche nell'UE.

Essa integra e anticipa inoltre la direttiva CER, invitando già gli Stati membri a dare priorità al recepimento tempestivo di tale direttiva, cooperando attraverso le riunioni di esperti convocate nell'ambito del piano in cinque punti annunciato dalla Commissione, e mirando a coordinare il percorso verso un approccio comune allo svolgimento di prove di stress sulle infrastrutture critiche nell'UE.

La proposta è inoltre in linea con la direttiva NIS e la futura direttiva NIS2, che abrogherà la direttiva NIS, chiedendo un rapido avvio dei lavori di attuazione e recepimento. Rispecchia inoltre l'invito congiunto di Nevers del marzo 2022 e le conclusioni del Consiglio sulla posizione dell'UE in materia di sicurezza informatica del maggio 2022 per quanto riguarda la richiesta degli Stati membri alla Commissione di elaborare valutazioni dei rischi e scenari di rischio.

La proposta è altresì in linea con la politica dell'UE in materia di protezione civile, poiché si prevede che, in caso di pesante perturbazione delle attività delle infrastrutture/dei soggetti critici, gli Stati membri e i paesi terzi possano chiedere assistenza tramite il centro di

coordinamento della risposta alle emergenze (ERCC) nell'ambito del meccanismo unionale di protezione civile (UCPM). Qualora venga attivato l'UCPM, l'ERCC è in grado di coordinare e cofinanziare l'invio al paese colpito di attrezzature, materiali e competenze essenziali disponibili negli Stati membri (in parte nel contesto del pool europeo di protezione civile) e nell'ambito di rescEU. L'assistenza che può essere messa a disposizione su richiesta comprende, ad esempio, combustibile, generatori, infrastrutture elettriche, capacità di riparo, capacità di depurazione dell'acqua e capacità mediche di emergenza.

La proposta è inoltre in linea con l'*acquis* dell'UE in materia di sicurezza dell'approvvigionamento energetico.

Il settore dell'energia nucleare non è specificamente incluso nella proposta di raccomandazione del Consiglio, eccezion fatta ad esempio per infrastrutture correlate (come le linee di trasmissione connesse alle centrali nucleari) che possono incidere sulla sicurezza dell'approvvigionamento. Gli elementi nucleari specifici sono disciplinati dalla pertinente normativa in materia nucleare ai sensi del trattato Euratom e/o dalla legislazione nazionale[6]. Sulla base degli insegnamenti tratti dall'incidente di Fukushima la legislazione europea in materia di sicurezza nucleare è stata rafforzata, e le autorità nazionali devono di conseguenza effettuare revisioni periodiche della sicurezza di ciascun impianto al fine di garantirne la costante conformità ai requisiti più elevati di sicurezza e di individuare ulteriori miglioramenti in materia, e devono inoltre essere svolte revisioni tematiche annuali tra pari a livello dell'UE.

La strategia per la sicurezza marittima dell'UE[7] e il relativo piano d'azione[8] evidenziano la natura mutevole delle minacce nel settore marittimo e chiedono un impegno rinnovato a favore della protezione delle infrastrutture marittime critiche, incluse quelle subacquee, e in particolare delle infrastrutture marittime nel settore dei trasporti, dell'energia e della comunicazione, fra l'altro promuovendo la conoscenza della situazione marittima attraverso il miglioramento dell'interoperabilità e l'ottimizzazione dello scambio delle informazioni.

La proposta è in linea anche con altre normative settoriali pertinenti. L'attuazione della presente raccomandazione dovrebbe pertanto essere coerente con le misure specifiche che disciplinano o potranno disciplinare in futuro taluni aspetti della resilienza dei soggetti che operano nei settori interessati, come i trasporti. Questo comprende altre iniziative pertinenti quali il piano di emergenza per i trasporti[9], o il piano di emergenza per l'approvvigionamento alimentare e la sicurezza di tale approvvigionamento in tempi di crisi[10] e il collegato meccanismo europeo di preparazione e risposta alla sicurezza dell'approvvigionamento alimentare. Più in generale, la raccomandazione dovrebbe naturalmente essere attuata nel pieno rispetto di tutte le norme applicabili del diritto dell'UE, comprese quelle stabilite nelle direttive ECI e NIS.

La proposta è inoltre in linea con la bussola strategica per la sicurezza e la difesa, che ha sottolineato la necessità di rafforzare in modo sostanziale la resilienza e la capacità di contrastare le minacce ibride e gli attacchi informatici, come pure la necessità di potenziare la resilienza dei paesi partner e di cooperare con la NATO. È infine in linea con il quadro per una risposta coordinata dell'UE alle minacce e alle campagne ibride che interessano l'UE, gli Stati membri e i partner[11].

---

6 Considerando 9 della direttiva 2008/114/CE del Consiglio (direttiva ECI).
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.
11 Consiglio dell'Unione europea, documento 10016/22, 21 giugno 2022.

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La proposta si basa sull'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), che prevede il ravvicinamento delle legislazioni per il miglioramento del mercato interno, in combinato disposto con l'articolo 292 TFUE. Ciò è giustificato dal fatto che la proposta di raccomandazione del Consiglio mira principalmente ad anticipare le misure stabilite nelle nuove direttive CER e NIS2, entrambe basate sull'articolo 114 TFUE. In linea con la logica che giustifica il ricorso a tale articolo come base giuridica di tali direttive, è necessaria un'azione dell'UE per garantire il corretto funzionamento del mercato interno, in particolare in considerazione della natura e dell'ambito di applicazione transfrontalieri dei servizi interessati e delle potenziali conseguenze in caso di perturbazione, nonché delle misure nazionali attuali ed emergenti volte a rafforzare la resilienza dei soggetti che gestiscono infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

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

Un percorso a livello europeo nel settore della resilienza dei soggetti che gestiscono infrastrutture critiche è giustificato dal carattere interdipendente e transfrontaliero delle relazioni tra le attività delle infrastrutture critiche e i servizi essenziali forniti e dalla necessità di un approccio europeo più comune e coordinato, al fine di garantire che i soggetti interessati siano abbastanza resilienti nell'attuale contesto geopolitico. Se molte delle sfide comuni, come l'apparente sabotaggio dei gasdotti North Stream, sono affrontate in primo luogo mediante misure nazionali o dai soggetti che gestiscono le infrastrutture critiche, per potenziare la resilienza, migliorare la vigilanza e rafforzare la risposta collettiva dell'UE è necessario il sostegno dell'Unione, compreso se del caso quello delle agenzie competenti.

- **Proporzionalità**

La presente proposta è conforme al principio di proporzionalità di cui all'articolo 5, paragrafo 4, del trattato sull'Unione europea (TUE).

Né il contenuto né la forma della presente proposta di raccomandazione del Consiglio vanno al di là di quanto è necessario per conseguire gli obiettivi fissati. Le azioni proposte sono proporzionate agli obiettivi perseguiti, in quanto rispettano le prerogative e gli obblighi degli Stati membri ai sensi del diritto nazionale.

Infine, la proposta accoglie un potenziale approccio differenziato che rispecchia le diverse realtà interne degli Stati membri per quanto riguarda la preparazione e la risposta alle minacce fisiche alle infrastrutture critiche.

- **Scelta dell'atto giuridico**

Per conseguire gli obiettivi di cui sopra il TFUE, nello specifico all'articolo 292, prevede l'adozione da parte del Consiglio di raccomandazioni sulla base di una proposta della Commissione. Una raccomandazione del Consiglio è uno strumento appropriato in questo caso, anche alla luce dell'attuale contesto legislativo, come spiegato in precedenza. Come atto giuridico, sebbene di natura non vincolante, una raccomandazione del Consiglio indica l'impegno degli Stati membri nei confronti delle misure ivi incluse e fornisce una solida base politica per la cooperazione in questi settori, nel pieno rispetto della competenza degli Stati membri.

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

- **Consultazioni dei portatori di interessi**

Nell'elaborare la presente proposta si è tenuto conto dei pareri espressi dagli esperti degli Stati membri nella riunione del 12 ottobre 2022. Si è registrato un ampio consenso sull'utilità di un maggiore coordinamento a livello dell'Unione per quanto riguarda la preparazione e la risposta nell'attuale contesto delle minacce e di anticipare alcuni elementi della direttiva CER prima della sua adozione formale. Gli Stati membri si sono dichiarati disposti a condividere esperienze e migliori pratiche sulle misure e sulle metodologie per aumentare la resilienza dei soggetti che gestiscono infrastrutture critiche. Si sono inoltre dichiarati aperti a un approccio coordinato alle prove di stress sui soggetti che gestiscono infrastrutture critiche, su base volontaria e secondo principi comuni. Gli Stati membri hanno indicato che i soggetti che gestiscono infrastrutture critiche nei settori dell'energia, delle infrastrutture digitali e dei trasporti, in particolare quelli rilevanti per più Stati membri, dovrebbero essere considerati prioritari ai fini della presente raccomandazione. Hanno inoltre accolto con favore l'intenzione della Commissione di convocare ulteriori riunioni di esperti degli Stati membri nelle prossime settimane.

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

La proposta di raccomandazione del Consiglio prevede quanto segue:

– Il capo I definisce lo scopo della proposta e il suo ambito di applicazione e definisce le priorità delle misure raccomandate.

– Il capo II si concentra sulle misure che dovrebbero essere adottate per rafforzare la preparazione, sia a livello dell'Unione che degli Stati membri.

– Il capo III riguarda il rafforzamento della risposta, sia a livello dell'UE che degli Stati membri.

– Il capo IV tratta della cooperazione internazionale e delle azioni che dovrebbero essere adottate per aumentare la resilienza dei soggetti che gestiscono infrastrutture critiche.

2022/0338 (NLE)

Proposta di

RACCOMANDAZIONE DEL CONSIGLIO

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

(Testo rilevante ai fini del SEE)

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) L'Unione ha un ruolo particolare da svolgere in relazione alle infrastrutture a cavallo delle frontiere, che incidono sugli interessi di diversi Stati membri, o che sono altrimenti utilizzate dai soggetti che forniscono servizi essenziali su base transfrontaliera. Tale fornitura di servizi e tali infrastrutture critiche rilevanti per più Stati membri possono tuttavia essere situate in un solo Stato membro o al di fuori del territorio degli Stati membri, ad esempio nel caso di cavi o condotte sottomarini. Una chiara individuazione di tali infrastrutture e soggetti e delle minacce con cui si confrontano, come pure un impegno collettivo a proteggerle, sono nell'interesse di tutti gli Stati membri e dell'Unione nel suo insieme.

(2) La protezione delle infrastrutture critiche in due settori è attualmente disciplinata dalla direttiva 2008/114/CE del Consiglio[12]. Tale direttiva stabilisce una procedura di individuazione e designazione delle infrastrutture critiche europee e un approccio comune per la valutazione della necessità di migliorarne la protezione al fine di contribuire alla tutela delle persone. La direttiva riguarda i settori dell'energia e dei trasporti. Al fine di migliorare la resilienza dei soggetti critici, dei servizi essenziali da essi forniti e delle infrastrutture critiche da cui dipendono, è in fase di adozione da parte del legislatore dell'Unione una nuova direttiva sulla resilienza dei soggetti critici[13] ("direttiva CER"), che sostituirà la direttiva 2008/114/CE e riguarderà un maggior numero di settori, comprese le infrastrutture digitali.

(3) La 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[14], si concentra inoltre sulle minacce di natura informatica. Tale direttiva sarà sostituita da una nuova direttiva relativa a misure per un livello comune

---

12 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).

13 COM(2020) 829.

14 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).

elevato di cibersicurezza nell'Unione[15] ("direttiva NIS2"), anch'essa in fase di adozione da parte del legislatore dell'Unione.

(4) In considerazione di uno scenario di minacce in rapida evoluzione, in particolare nel contesto dell'apparente sabotaggio dei gasdotti Nord Stream 1 e 2, i soggetti che gestiscono infrastrutture critiche si trovano ad affrontare sfide particolari per quanto riguarda la loro resilienza nei confronti di atti ostili e altre minacce di origine umana, mentre le sfide derivanti da fattori naturali e cambiamenti climatici sono in aumento e possono interagire con atti ostili. I soggetti in questione devono pertanto adottare, con il sostegno degli Stati membri, adeguate misure di aumento della resilienza. Tali misure dovrebbero essere adottate, e il sostegno dovrebbe essere fornito, al di là delle disposizioni previste dalla direttiva 2008/114/CE e dalla direttiva (UE) 2016/1148, e ancor prima dell'adozione, dell'entrata in vigore e del recepimento delle nuove direttive CER e NIS2.

(5) In attesa dell'adozione, dell'entrata in vigore e del recepimento di tali nuove direttive, l'Unione e gli Stati membri sono incoraggiati, conformemente al diritto dell'Unione, ad avvalersi di tutti gli strumenti disponibili per proseguire in questa direzione e contribuire a rafforzare la resilienza fisica e informatica dei soggetti interessati e delle infrastrutture critiche da essi gestite per fornire servizi essenziali nel mercato interno, vale a dire servizi cruciali per il mantenimento di funzioni vitali della società, delle attività economiche, della sicurezza e della salute pubblica o dell'ambiente. A tale riguardo, il concetto di resilienza dovrebbe essere inteso come riferito alla capacità di un soggetto di prevenzione, protezione, risposta, resistenza, attenuazione, assorbimento, adattamento e recupero rispetto ad eventi che possono perturbare in modo significativo, o che perturbano, la fornitura dei servizi essenziali in questione.

(6) Al fine di garantire un approccio efficace e il più coerente possibile con la nuova direttiva CER, le misure contenute nella presente raccomandazione dovrebbero riguardare le infrastrutture designate da uno Stato membro come infrastrutture critiche, che comprendono sia infrastrutture critiche nazionali che infrastrutture critiche europee, indipendentemente dal fatto che il soggetto che gestisce l'infrastruttura critica sia già stato designato come soggetto critico ai sensi di tale nuova direttiva. Ai fini della presente raccomandazione, il termine "infrastrutture critiche" dovrebbe essere inteso di conseguenza.

(7) Alla luce delle minacce esistenti, dovrebbero essere adottate in via prioritaria misure di aumento della resilienza nei settori chiave dell'energia, delle infrastrutture digitali, dei trasporti e dello spazio, e tali misure dovrebbero incentrarsi sull'aumento della resilienza dei soggetti che gestiscono infrastrutture critiche rispetto ai rischi di origine umana. Per quanto riguarda le infrastrutture critiche nazionali, in considerazione delle possibili conseguenze in caso di concretizzazione dei rischi, dovrebbe essere data priorità alle infrastrutture di rilevanza transfrontaliera.

(8) Di conseguenza, le misure stabilite nella presente raccomandazione sono volte principalmente a integrare le nuove direttive CER e NIS2, basate sull'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE), anticipando e completando le misure previste da tali nuove direttive. Pertanto, e in considerazione della natura e della rilevanza transfrontaliere dei servizi essenziali e delle infrastrutture critiche in questione e delle attuali ed emergenti disparità delle legislazioni nazionali che

[15] COM(2020) 823.

distorcono il mercato interno, è opportuno basare anche la presente raccomandazione sull'articolo 114 TFUE, in combinato disposto con l'articolo 292 TFUE.

(9) L'attuazione della presente raccomandazione non dovrebbe essere intesa come un intervento che incida sugli obblighi derivanti dal diritto dell'Unione e riguardanti taluni aspetti della resilienza dei soggetti interessati, e dovrebbe essere coerente con essi. Tali obblighi sono stabiliti in strumenti generali quali la direttiva 2008/114/CE, la direttiva (UE) 2016/1148 e le nuove direttive CER e NIS2 che le sostituiscono, ma anche in alcuni strumenti settoriali, ad esempio nel settore dei trasporti, per il quale, fra gli altri, la Commissione ha intrapreso un'iniziativa in merito a un piano di emergenza[16]. Conformemente al principio di leale cooperazione, la presente raccomandazione dovrebbe essere attuata nel pieno rispetto reciproco e con il massimo sostegno reciproco.

(10) Il 5 ottobre 2022 la Commissione ha annunciato un piano in cinque punti che definisce un approccio coordinato per affrontare le sfide future, e che contempla sia un lavoro sulla preparazione, che si basa sulla nuova direttiva CER e ne anticipa l'adozione e l'entrata in vigore, sia la collaborazione con gli Stati membri al fine di effettuare prove di stress su soggetti che gestiscono infrastrutture critiche, secondo principi comuni, iniziando dal settore dell'energia. La presente raccomandazione, che contribuirà a tale piano, accoglie con favore l'approccio proposto e definisce come esso possa essere tradotto in azione.

(11) Sullo sfondo di uno scenario di minacce in rapida evoluzione e dell'attuale contesto di rischio caratterizzato da rischi di origine umana, in particolare per quanto riguarda le infrastrutture critiche di rilevanza transfrontaliera, è essenziale disporre di un quadro preciso, aggiornato e completo dei rischi più importanti con cui si confrontano i soggetti che gestiscono infrastrutture critiche. Gli Stati membri dovrebbero pertanto adottare le misure necessarie per effettuare o aggiornare le loro valutazioni di tali rischi. Anche se la presente raccomandazione si concentra sui rischi correlati alla sicurezza, si dovrebbe continuare a investire negli sforzi per affrontare i cambiamenti climatici e i rischi per l'ambiente, in particolare quando gli eventi naturali possono aggravare ulteriormente i rischi causati dall'uomo.

(12) Tenuto conto di tale scenario di minacce, gli Stati membri dovrebbero essere invitati ad adottare quanto prima misure adeguate per aumentare la resilienza delle infrastrutture critiche, anche al di là delle suddette valutazioni dei rischi, che saranno successivamente richieste ai sensi della nuova direttiva CER.

(13) Nell'ambito dell'attuazione del piano in cinque punti annunciato dalla Commissione, è necessario coordinare i lavori convocando riunioni di esperti nazionali in previsione dell'istituzione, mediante la nuova direttiva CER, del gruppo per la resilienza dei soggetti critici, al fine di consentire la cooperazione tra gli Stati membri e lo scambio di informazioni relative alla resilienza dei soggetti che gestiscono infrastrutture critiche. Ciò dovrebbe includere la cooperazione e lo scambio di informazioni riguardanti attività quali l'individuazione dei soggetti e delle infrastrutture critici, la preparazione dello sviluppo e della promozione di una serie comune di principi per effettuare prove di stress e la raccolta di insegnamenti comuni da tali prove, individuando le vulnerabilità e le possibili capacità. Tali processi dovrebbero anche apportare vantaggi per la resilienza dei soggetti che gestiscono infrastrutture critiche rispetto ai rischi climatici e ambientali. Questo lavoro consentirebbe inoltre di definire

[16] COM(2022) 211.

priorità comuni per le prove di stress, con particolare attenzione ai settori dell'energia, delle infrastrutture digitali, dei trasporti e dello spazio. 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 nuova direttiva CER e istituito il gruppo per la resilienza dei soggetti critici, tale lavoro di anticipazione dovrebbe essere portato avanti da questo gruppo conformemente ai compiti ad esso attribuiti dalla direttiva CER.

(14) L'esercizio delle prove di stress dovrebbe essere integrato dall'elaborazione di un programma per gli incidenti e le crisi delle infrastrutture critiche, che descriva e definisca gli obiettivi e le modalità di cooperazione tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE nel rispondere agli incidenti che colpiscono le infrastrutture critiche, in particolare laddove questi comportino perturbazioni significative della fornitura di servizi essenziali per il mercato interno. Tale programma dovrebbe avvalersi degli esistenti dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR) per il coordinamento della risposta, dovrebbe funzionare in coerenza e complementarità con il piano relativo agli incidenti di cibersicurezza su vasta scala, e dovrebbe inoltre prevedere un accordo sui principali messaggi di comunicazione pubblica, dato che le comunicazioni di crisi svolgono un ruolo importante nell'attenuare gli effetti negativi degli incidenti e delle crisi delle infrastrutture critiche.

(15) Al fine di garantire una risposta coordinata ed efficace alle minacce attuali e previste, la Commissione dovrebbe fornire un sostegno supplementare agli Stati membri allo scopo di aumentare la resilienza tenuto conto di tali minacce, in particolare fornendo informazioni pertinenti sotto forma di istruzioni, manuali e orientamenti, promuovendo l'adozione di progetti di ricerca e innovazione finanziati dall'Unione, adottando le necessarie azioni di anticipazione e ottimizzando l'uso dei mezzi di sorveglianza dell'Unione. Il SEAE, in particolare attraverso il Centro UE di situazione e di intelligence, dovrebbe fornire valutazioni delle minacce.

(16) Le agenzie settoriali dell'Unione e altri organismi rilevanti dovrebbero fornire sostegno per le questioni connesse alla resilienza, nella misura in cui i rispettivi mandati stabiliti nei pertinenti strumenti del diritto dell'Unione lo consentano. In particolare, l'Agenzia europea per la cibersicurezza (ENISA) potrebbe fornire assistenza in materia di cibersicurezza, l'Agenzia europea per la sicurezza marittima (EMSA) potrebbe, grazie alle sue competenze, contribuire ad aiutare gli Stati membri attraverso il suo servizio di sorveglianza marittima per le questioni relative alla sicurezza e alla protezione marittima, l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) potrebbe fornire sostegno in relazione alla raccolta di informazioni e alle indagini nelle azioni di contrasto transfrontaliere, mentre l'Agenzia dell'Unione europea per il programma spaziale (EUSPA) e il Centro satellitare dell'UE (SatCen) potrebbero essere in grado di fornire assistenza attraverso operazioni nell'ambito del programma spaziale dell'Unione.

(17) Sebbene la responsabilità primaria di garantire la sicurezza delle infrastrutture critiche e dei soggetti interessati spetti agli Stati membri, un maggiore coordinamento a livello dell'Unione risulta opportuno, in particolare alla luce delle minacce che possono ripercuotersi su diversi Stati membri contemporaneamente, come la guerra di aggressione della Russia nei confronti dell'Ucraina, o incidere sulla resilienza e sul buon funzionamento dell'economia, del mercato unico e delle società dell'Unione.

(18) La presente raccomandazione non comporta la comunicazione di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

(19) Con la crescente interdipendenza delle infrastrutture fisiche e digitali, le attività informatiche dolose rivolte a settori critici possono causare perturbazioni o danni alle infrastrutture fisiche, mentre il sabotaggio delle infrastrutture fisiche può rendere i servizi digitali inaccessibili. Tenuto conto della maggiore minaccia rappresentata dagli attacchi ibridi sofisticati, gli Stati membri dovrebbero includere anche tali considerazioni nei loro lavori di attuazione della presente raccomandazione. In considerazione delle interconnessioni tra la cibersicurezza e la sicurezza fisica degli operatori, è importante che i lavori preparatori per il recepimento e l'applicazione della nuova direttiva NIS2 inizino quanto prima e che tali lavori progrediscano in parallelo anche per la nuova direttiva CER.

(20) Oltre a migliorare la preparazione è importante rafforzare la capacità di rispondere in modo pronto ed efficace qualora si concretizzino dei rischi che incidono sulla fornitura di servizi essenziali da parte di soggetti che gestiscono infrastrutture critiche. La presente raccomandazione dovrebbe pertanto contenere le misure che dovrebbero essere adottate a livello sia degli Stati membri che dell'Unione, compresi la cooperazione rafforzata e lo scambio di informazioni nel contesto del meccanismo unionale di protezione civile e l'uso delle risorse pertinenti del programma spaziale dell'Unione.

(21) A seguito dell'invito rivolto dal Consiglio nelle sue conclusioni sulla posizione dell'UE in materia di sicurezza informatica[17], la Commissione, l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza ("alto rappresentante") e il gruppo di cooperazione istituito dalla direttiva (UE) 2016/1148 ("gruppo di cooperazione NIS") stanno effettuando, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe, una valutazione dei rischi ed elaborando scenari di rischio in relazione alla cibersicurezza in una situazione di minaccia o di possibile attacco nei confronti di Stati membri o paesi partner. Tale esercizio è incentrato su settori critici quali l'energia, le infrastrutture digitali, i trasporti e lo spazio.

(22) L'invito ministeriale congiunto di Nevers[18] e le conclusioni del Consiglio sulla posizione dell'UE in materia di sicurezza informatica hanno inoltre esortato a rafforzare la resilienza delle infrastrutture e delle reti di comunicazione nell'Unione sulla base di una valutazione dei rischi, indirizzando raccomandazioni agli Stati membri e alla Commissione. Tale valutazione dei rischi è attualmente condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA e in cooperazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC). La valutazione dei rischi e l'analisi delle carenze esaminano i rischi di attacchi informatici nei vari sottosettori delle infrastrutture di comunicazione, comprese le infrastrutture fisse e mobili, i satelliti, i cavi sottomarini, l'instradamento in internet, ecc., costituendo così una base per i lavori previsti dalla presente raccomandazione. Tale valutazione dei rischi fornirà informazioni utili per l'attività in

[17] Posizione in materia di sicurezza informatica: il Consiglio approva le conclusioni — Consilium (europa.eu)

[18] https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

corso di valutazione intersettoriale dei rischi di cibersicurezza ed elaborazione di scenari, richiesta dal Consiglio nelle conclusioni del 23 maggio 2022.

(23) Questi due esercizi saranno coerenti e coordinati con l'elaborazione di scenari incentrati sulla protezione civile nel contesto di un'ampia gamma di catastrofi naturali e di origine umana, compresi gli eventi di cibersicurezza e il loro impatto reale, attualmente condotta dalla Commissione e dagli Stati membri conformemente alla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio[19]. Ai fini dell'efficienza, dell'efficacia e della coerenza, la presente raccomandazione dovrebbe essere attuata tenendo conto dei risultati di tali esercizi.

(24) Il pacchetto di strumenti dell'UE per la cibersicurezza delle reti 5G[20] stabilisce misure e piani di mitigazione pertinenti per rafforzare la sicurezza delle reti 5G. Data la dipendenza di molti servizi essenziali dalle reti 5G e la natura interconnessa degli ecosistemi digitali, è essenziale che tutti gli Stati membri attuino urgentemente le misure raccomandate nel pacchetto di strumenti e, in particolare, applichino le pertinenti restrizioni ai fornitori ad alto rischio per le risorse essenziali definite critiche e sensibili nella valutazione dei rischi coordinata a livello dell'UE.

(25) Per potenziare immediatamente la preparazione e le capacità di risposta ai gravi incidenti di cibersicurezza, la Commissione ha istituito un programma a breve termine volto a sostenere gli Stati membri attraverso finanziamenti aggiuntivi assegnati all'ENISA. Tra i servizi forniti figurano azioni di preparazione, quali test di penetrazione dei soggetti critici al fine di individuare le vulnerabilità. Il programma rafforzerà inoltre le possibilità di assistere gli Stati membri in caso di incidenti gravi che colpiscano soggetti critici. Si tratta di un primo passo in linea con le conclusioni del Consiglio sulla posizione in materia di sicurezza 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.

(26) La rete globale di cavi sottomarini per la trasmissione di dati e le comunicazioni elettroniche è essenziale 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 rendono particolarmente utile la 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 ed eventuali misure di attenuazione specifiche per i cavi sottomarini. La Commissione effettuerà studi sull'argomento e trasmetterà le sue conclusioni agli Stati membri.

(27) I rischi relativi alle infrastrutture digitali possono incidere anche sui settori prioritari dell'energia e dei trasporti individuati nella presente raccomandazione. Possono riguardare, ad esempio, le 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 gestite da soggetti che operano nel settore energetico.

---

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

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

È opportuno tenerne conto al momento di adottare misure volte a rafforzare la resilienza dei soggetti che gestiscono infrastrutture critiche conformemente alla presente raccomandazione.

(28) Data la crescente importanza delle infrastrutture spaziali e dei servizi spaziali per le attività connesse alla sicurezza, è essenziale garantire la resilienza e la protezione delle risorse e dei servizi spaziali dell'Unione al suo interno, ma anche, nel quadro della presente raccomandazione, utilizzare in modo più strutturato i dati e i servizi spaziali forniti dai sistemi spaziali e dai programmi per la sorveglianza e 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.

(29) Occorre inoltre cooperare a livello internazionale così da affrontare efficacemente i rischi per la resilienza dei soggetti che gestiscono infrastrutture critiche, nell'Unione, nei paesi terzi interessati o nelle acque internazionali. Gli Stati membri dovrebbero pertanto essere invitati a cooperare con la Commissione e l'alto rappresentante per adottare misure a tal fine, fermo restando che dovrebbero intervenire solo in conformità dei rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, in particolare delle disposizioni dei trattati dell'UE in materia di relazioni esterne.

(30) Come stabilito nella comunicazione "Contributo della Commissione alla difesa europea"[21], 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"[22], 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. L'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.

(31) La strategia per la sicurezza marittima dell'Unione europea del 2014 e il relativo piano d'azione 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, anche 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. La presente raccomandazione dovrebbe attingere a tali azioni e integrarle.

(32) Gli Stati membri dovrebbero utilizzare pienamente il potenziale del programma di ricerca dell'Unione in materia di sicurezza, in particolare sfruttando la priorità dedicata alle infrastrutture critiche, specialmente nell'ambito dei programmi finanziati dal Fondo Sicurezza interna, e altre potenziali opportunità di finanziamento a livello dell'Unione quale il Fondo europeo di sviluppo regionale, purché le misure specifiche soddisfino i requisiti di ammissibilità. Anche REPowerEU può offrire possibilità di finanziamento ai fini della resilienza. Le opportunità offerte dai finanziamenti

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

22 Consiglio dell'Unione europea, documento 7371/22 del 21 marzo 2022.

dell'Unione devono essere comunque utilizzate nel rispetto dei requisiti giuridici applicabili,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

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

(1) La presente raccomandazione invita gli Stati membri ad adottare urgentemente misure efficaci e a cooperare in modo leale, efficace, solidale e coordinato tra loro, con la Commissione e con le altre autorità pubbliche competenti, nonché con i soggetti interessati, per aumentare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

(2) Le misure di cui alla presente raccomandazione riguardano le infrastrutture designate da uno Stato membro come infrastrutture critiche, comprese le infrastrutture critiche europee.

(3) Nell'attuare la presente raccomandazione è opportuno dare la priorità all'aumento della resilienza dei soggetti che operano nei settori dell'energia, delle infrastrutture digitali, dei trasporti e dello spazio, e delle infrastrutture critiche con rilevanza transfrontaliera gestite da tali soggetti, rispetto ai rischi di origine umana.

CAPO II: MIGLIORAMENTO DELLA PREPARAZIONE

Azioni a livello degli Stati membri

(4) Gli Stati membri sono invitati a svolgere o aggiornare le valutazioni dei rischi relative alla resilienza dei soggetti che gestiscono infrastrutture critiche europee nei settori dei trasporti e dell'energia designate a norma della direttiva 2008/114/CE e a cooperare reciprocamente in merito a tali valutazioni dei rischi e alle eventuali misure di aumento della resilienza che ne derivano conformemente a tale direttiva.

(5) Inoltre, affinché i soggetti che gestiscono infrastrutture critiche conseguano un livello elevato di resilienza, gli Stati membri dovrebbero accelerare i lavori preparatori per recepire e applicare quanto prima la nuova direttiva CER, nel seguente modo:

(a) accelerando l'adozione o l'aggiornamento delle strategie nazionali volte ad aumentare la resilienza dei soggetti che gestiscono infrastrutture critiche per rispondere alla minaccia attuale. Le parti pertinenti di tale strategia dovrebbero essere comunicate alla Commissione;

(b) svolgendo o aggiornando le valutazioni dei rischi in linea con la natura evolutiva delle attuali minacce per quanto riguarda la resilienza dei soggetti che gestiscono infrastrutture critiche in settori pertinenti diversi da quelli dell'energia, delle infrastrutture digitali, dei trasporti e dello spazio e, se possibile, nei settori cui si applica la nuova direttiva CER, vale a dire banche, infrastrutture dei mercati finanziari, infrastrutture digitali, sanità, acqua potabile, acque reflue, pubblica amministrazione, spazio e produzione, trasformazione e distribuzione di alimenti, tenendo conto della potenziale natura ibrida delle minacce, compresi gli effetti a cascata e gli effetti dei cambiamenti climatici;

(c) informando la Commissione dei tipi di rischi individuati per ciascun settore e sottosettore e dei risultati delle valutazioni dei rischi, eventualmente mediante un modello comune per la presentazione di relazioni elaborato dalla Commissione in cooperazione con gli Stati membri;

(d) accelerando il processo di individuazione e designazione dei soggetti critici, dando priorità ai soggetti critici che:

(a) utilizzano infrastrutture critiche fisicamente collegate tra due o più Stati membri;

(b) fanno parte di strutture societarie collegate o associate a soggetti critici in altri Stati membri;

(c) sono stati individuati come tali in uno Stato membro e forniscono servizi essenziali in sei o più Stati membri, o a sei o più Stati membri, e hanno pertanto una particolare rilevanza europea, e informandone la Commissione;

(d) cooperando tra loro, specialmente per quanto riguarda i soggetti critici, i servizi essenziali e le infrastrutture critiche di rilevanza transfrontaliera, in particolare avviando consultazioni reciproche ai fini del punto 5, lettera d), e informandosi reciprocamente in caso di incidenti che causino perturbazioni significative o potenzialmente significative a livello transfrontaliero, e tenendo debitamente informata la Commissione;

(e) rafforzando il sostegno ai soggetti critici designati per renderli più resilienti, eventualmente fornendo materiali e metodologie di orientamento, organizzando esercitazioni per testare la loro resilienza e offrendo consulenza e formazione al loro personale, e permettendo di effettuare controlli dei precedenti personali di coloro che rivestono ruoli sensibili, conformemente alla legislazione dell'Unione e nazionale, nel quadro delle misure di gestione della sicurezza del personale adottate dai soggetti critici;

(f) accelerando la designazione o l'istituzione di un punto di contatto unico presso l'autorità competente, che svolga una funzione di collegamento con i punti di contatto unici di altri Stati membri per garantire la cooperazione transfrontaliera relativa alla resilienza dei soggetti che gestiscono infrastrutture critiche.

(6) Gli Stati membri sono incoraggiati a sottoporre a prove di stress i soggetti che gestiscono infrastrutture critiche. In particolare, gli Stati membri sono invitati ad accelerare la loro preparazione e quella dei soggetti interessati nel settore dell'energia e a effettuare prove di stress in tale settore, ove possibile seguendo principi concordati a livello dell'Unione, provvedendo nel contempo a un'efficace comunicazione con i soggetti interessati. In una fase successiva potrebbe essere valutata, se necessario, l'opportunità di introdurre prove di stress in altri settori prioritari, in particolare le infrastrutture digitali, i trasporti e lo spazio, tenendo debitamente conto delle ispezioni svolte nei sottosettori aereo e marittimo a norma del diritto dell'Unione e delle pertinenti disposizioni della legislazione settoriale.

(7) Gli Stati membri sono invitati a cooperare, laddove opportuno e in conformità del diritto dell'Unione, con i paesi terzi interessati per quanto attiene alla resilienza dei soggetti che gestiscono infrastrutture critiche di rilevanza transfrontaliera.

(8) Gli Stati membri sono invitati a sfruttare, conformemente ai requisiti applicabili, le potenziali opportunità di finanziamento a livello dell'Unione e nazionale per rendere i soggetti che gestiscono infrastrutture critiche nell'Unione, ad esempio lungo le reti transeuropee, più resilienti nei confronti dell'intera gamma delle minacce significative, in particolare nell'ambito dei programmi finanziati dal Fondo Sicurezza interna e dal Fondo europeo di sviluppo regionale, a condizione che siano soddisfatti i rispettivi criteri di ammissibilità, e del meccanismo per collegare l'Europa, comprese le disposizioni sulla resilienza ai cambiamenti climatici. A tale scopo possono essere utilizzati anche i finanziamenti del meccanismo unionale di

protezione civile, nel rispetto dei requisiti applicabili, in particolare per progetti relativi a valutazioni dei rischi, piani di investimento o studi, sviluppo delle capacità o miglioramento delle conoscenze di base. Anche REPowerEU può offrire possibilità di finanziamento ai fini della resilienza.

(9) Per quanto riguarda le infrastrutture di comunicazione e di rete nell'Unione, il gruppo di cooperazione NIS dovrebbe, in conformità dell'articolo 11 della direttiva (UE) 2016/1148 e successivamente dell'articolo 14 della direttiva NIS2, accelerare i lavori in corso su una valutazione mirata dei rischi e presentare le prime raccomandazioni all'inizio del 2023. Tale lavoro dovrebbe 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, quali il gruppo per la resilienza dei soggetti critici da istituire a norma della nuova direttiva CER e il forum di sorveglianza da istituire a norma del nuovo atto sulla resilienza operativa digitale (DORA)[23].

(10) Il gruppo di cooperazione NIS, che svolgerà i suoi compiti conformemente all'articolo 11 della direttiva (UE) 2016/1148 e successivamente dell'articolo 14 della direttiva NIS2, è invitato, con il sostegno della Commissione e dell'ENISA, a dare priorità ai lavori sulla sicurezza delle infrastrutture digitali e del settore spaziale, preparando orientamenti strategici e metodologie e misure di gestione dei rischi di cibersicurezza secondo un approccio multirischio in relazione ai cavi di comunicazione sottomarini, in previsione dell'entrata in vigore della direttiva NIS2, nonché orientamenti sulle misure di gestione dei rischi di cibersicurezza destinate agli operatori del settore spaziale, al fine di aumentare la resilienza delle infrastrutture terrestri 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, in particolare 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 attuare con urgenza le misure raccomandate nel pacchetto di strumenti dell'UE sulla cibersicurezza delle reti 5G[24]. Gli Stati membri che non hanno ancora introdotto restrizioni nei confronti dei fornitori ad alto rischio dovrebbero farlo senza ulteriori indugi, considerando che i ritardi possono aumentare la vulnerabilità delle reti nell'Unione. Dovrebbero inoltre rafforzare 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, compresi requisiti giuridicamente vincolanti a livello dell'Unione, per garantire un livello coerente di sicurezza e resilienza delle reti 5G.

(13) Gli Stati membri dovrebbero attuare quanto prima il 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 NIS e dei relativi

---

23 COM(2020) 595 final.

24 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

orientamenti elaborati dal gruppo di cooperazione NIS, in particolare il documento di riferimento sulle misure di sicurezza per gli operatori di servizi essenziali.

(14) Gli Stati membri dovrebbero sviluppare l'uso di Galileo e/o Copernicus a fini di sorveglianza e condividere le informazioni pertinenti all'interno dei gruppi di 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 risposta alle crisi.

Azioni a livello dell'Unione

(15) La Commissione intende rafforzare la cooperazione tra gli esperti degli Stati membri per contribuire ad aumentare la resilienza fisica non informatica dei soggetti che gestiscono infrastrutture critiche, e in particolare:

(a) preparare lo sviluppo e la promozione di strumenti comuni per sostenere gli Stati membri nel rafforzamento di tale resilienza, comprese metodologie e scenari di rischio;

(b) sostenere la definizione di principi comuni per la realizzazione delle prove di stress di cui al punto 6 da parte degli Stati membri, a cominciare da prove incentrate sui rischi di origine umana nel settore dell'energia e successivamente in altri settori chiave quali le infrastrutture digitali, i trasporti e lo spazio; affrontare altri rischi e pericoli significativi; se del caso, fornire sostegno e consulenza in merito allo svolgimento di tali prove di stress;

(c) fornire una piattaforma sicura per raccogliere, valutare e condividere le migliori pratiche, gli insegnamenti tratti dalle esperienze nazionali e altre informazioni relative a tale resilienza, anche per quanto riguarda lo svolgimento delle prove di stress e la traduzione dei risultati in protocolli e piani di emergenza.

Il lavoro di tali esperti dovrebbe prestare particolare attenzione alle dipendenze intersettoriali e ai soggetti che gestiscono infrastrutture critiche con rilevanza transfrontaliera, e dovrebbe essere proseguito dal gruppo per la resilienza dei soggetti critici una volta istituito.

(16) Gli Stati membri dovrebbero partecipare pienamente alla cooperazione rafforzata di cui al punto 15, fra l'altro designando punti di contatto dotati delle adeguate competenze e condividendo le esperienze sulle metodologie utilizzate per le prove di stress e i protocolli e i piani di emergenza elaborati su tale base. Lo scambio di informazioni dovrebbe tutelare la riservatezza di dette informazioni e la sicurezza e gli interessi commerciali dei soggetti critici, nel rispetto della sicurezza degli Stati membri. Tale scambio non comporta la comunicazione di informazioni la cui divulgazione sia contraria agli interessi essenziali degli Stati membri in materia di sicurezza nazionale, pubblica sicurezza o difesa.

(17) La Commissione sosterrà gli Stati membri fornendo manuali e orientamenti, quali un 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, è invitato a elaborare note sulle minacce alle infrastrutture critiche nell'UE al fine di migliorare la conoscenza situazionale.

(18) La Commissione favorirà la diffusione dei risultati dei progetti sulla resilienza dei soggetti che gestiscono infrastrutture critiche finanziati nell'ambito dei programmi

di ricerca e innovazione dell'Unione. La Commissione intende aumentare i finanziamenti a favore della resilienza, nell'ambito del bilancio assegnato a Orizzonte Europa nel quadro finanziario pluriennale 2021-2027. Ciò dovrebbe consentire di affrontare le sfide attuali e future in questo settore, come la capacità delle infrastrutture critiche di reagire ai cambiamenti climatici, senza pregiudicare gli altri finanziamenti per la ricerca e l'innovazione in materia di sicurezza civile nell'ambito di Orizzonte Europa. La Commissione intensificherà inoltre l'impegno per diffondere i risultati dei progetti di ricerca finanziati dall'Unione in questo settore.

(19) Il gruppo di cooperazione NIS, in collaborazione con la Commissione e l'alto rappresentante, è invitato a intensificare, conformemente ai rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, la collaborazione con le reti e gli organismi civili e militari competenti per valutare i rischi ed elaborare scenari di rischio in relazione alla cibersicurezza, concentrandosi inizialmente sulle infrastrutture dell'energia, delle comunicazioni, dei trasporti e dello spazio e sulle interdipendenze tra i diversi settori e tra gli Stati membri. Tale esercizio dovrebbe tenere conto dei relativi rischi per le infrastrutture fisiche su cui si basano questi settori. Le valutazioni dei rischi e gli scenari dovrebbero 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, e orientare le discussioni su come rafforzare la resilienza complessiva dei soggetti che gestiscono infrastrutture critiche e affrontare le vulnerabilità.

(20) La Commissione intende accelerare le sue attività volte a sostenere la preparazione degli Stati membri e la risposta agli incidenti di cibersicurezza su vasta scala, e in particolare:

(a) effettuerà, a complemento delle valutazioni dei rischi nel contesto della sicurezza delle reti e dell'informazione, uno studio completo che faccia il punto sull'infrastruttura dei cavi sottomarini che collegano gli Stati membri tra loro e l'Europa al resto del mondo, con una mappatura di tale infrastruttura e l'indicazione delle sue capacità e ridondanze, le vulnerabilità, i rischi in termini di disponibilità dei servizi e le possibilità di attenuazione dei rischi; i risultati dovrebbero essere condivisi con gli Stati membri;

(b) sosterrà la preparazione della risposta degli Stati membri e delle istituzioni, degli organi e degli organismi dell'Unione europea (EUIBA) agli incidenti di cibersicurezza su vasta scala.

(21) La Commissione intensificherà i lavori su azioni preventive lungimiranti, anche nell'ambito dell'UCPM, 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 del Centro di coordinamento della risposta alle emergenze.

In particolare, la Commissione si impegnerà sui seguenti punti:

(a) proseguimento dei lavori intrapresi nell'ambito del Centro di coordinamento della risposta alle emergenze per la previsione e prevenzione intersettoriale, la preparazione e la pianificazione della risposta, così da poter anticipare e prepararsi a possibili perturbazioni della fornitura di servizi essenziali da parte dei soggetti che gestiscono infrastrutture critiche;

(b) aumento degli investimenti negli approcci preventivi e nella preparazione della popolazione a perturbazioni di questo tipo, con particolare attenzione agli agenti

chimici, biologici, radiologici e nucleari-esplosivi o altre minacce emergenti di origine umana;

(c) rafforzamento dello scambio di conoscenze e migliori pratiche e miglioramento della progettazione e dello svolgimento delle attività di sviluppo delle capacità, quali corsi di formazione ed esercitazioni con i soggetti che gestiscono infrastrutture critiche, utilizzando le strutture e le competenze esistenti, come la rete unionale della conoscenza in materia di protezione civile.

(22) La Commissione promuoverà l'uso delle risorse di sorveglianza dell'UE (Copernicus e Galileo) 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.

(23) Se opportuno le agenzie dell'Unione e altri organismi competenti sono invitati a fornire sostegno, conformemente ai rispettivi mandati, su questioni relative alla resilienza dei soggetti che gestiscono infrastrutture critiche, ad esempio:

(a) Europol per quanto riguarda la raccolta di informazioni, l'analisi dei fenomeni criminali e il sostegno investigativo nelle azioni di contrasto transfrontaliere;

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

(c) l'EUSPA per quanto riguarda le attività nell'ambito del programma spaziale dell'Unione;

(d) l'ENISA per quanto riguarda le attività connesse alla cibersicurezza.

CAPO III: UNA RISPOSTA RAFFORZATA

Azioni a livello degli Stati membri

(24) Gli Stati membri dovrebbero:

(a) coordinare la loro risposta e mantenere una visione d'insieme della risposta intersettoriale alle perturbazioni significative della fornitura di servizi essenziali da parte dei soggetti che gestiscono infrastrutture critiche, nel quadro del meccanismo di crisi (IPCR) del Consiglio per quanto riguarda le infrastrutture critiche di rilevanza transfrontaliera, del programma per gli incidenti e le crisi di cibersicurezza su vasta scala o del quadro per una risposta coordinata alle campagne ibride ove pertinente;

(b) intensificare lo scambio di informazioni nell'ambito del meccanismo unionale di protezione civile al fine di rendere più efficace l'allarme rapido e coordinare la loro risposta nell'ambito del meccanismo in caso di perturbazioni significative, così da reagire più rapidamente, se necessario con il sostegno dell'Unione;

(c) aumentare la capacità di reagire prontamente, attraverso il meccanismo unionale di protezione civile, a tali perturbazioni significative, in particolare laddove possano avere implicazioni significative a livello transfrontaliero o addirittura paneuropeo, nonché intersettoriale;

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

(e) invitare i soggetti che gestiscono infrastrutture critiche e le autorità nazionali competenti a rafforzare la capacità di tali soggetti di ripristinare rapidamente le prestazioni di base di servizi essenziali;

(f) garantire che, quando è necessario ricostruire le infrastrutture critiche, le nuove infrastrutture siano resilienti nei confronti dell'intera gamma di rischi significativi a cui sono esposte, anche in scenari climatici avversi.

(25) Gli Stati membri sono invitati ad accelerare i lavori preparatori per il recepimento e l'applicazione della direttiva NIS2, iniziando immediatamente a rafforzare le capacità dei gruppi nazionali di intervento per la sicurezza informatica in caso di incidente (CSIRT) in considerazione dei nuovi compiti dei CSIRT e del maggior numero di soggetti di nuovi settori, aggiornando rapidamente le loro strategie di cibersicurezza e adottando quanto prima piani nazionali di risposta agli incidenti e alle crisi di cibersicurezza.

Azioni a livello dell'Unione

(26) Gli esperti degli Stati membri dovrebbero coordinare tra loro la reazione alle perturbazioni significative nella fornitura di servizi essenziali da parte dei soggetti che gestiscono infrastrutture critiche per quanto riguarda la resilienza di tali soggetti e le risposte a tali perturbazioni; tali competenze possono contribuire al funzionamento del meccanismo di crisi (IPCR) del Consiglio.

(27) La Commissione collaborerà strettamente con gli Stati membri per sviluppare ulteriori capacità utilizzabili di risposta alle emergenze, compresi gli esperti e le scorte di rescEU nell'ambito dell'UCPM, al fine di migliorare la preparazione operativa ad affrontare gli effetti immediati e indiretti di perturbazioni significative della fornitura di servizi essenziali da parte di soggetti che gestiscono infrastrutture critiche.

(28) Tenendo conto dell'evoluzione del panorama dei rischi e in cooperazione con gli Stati membri, nel contesto dell'UCPM la Commissione intende:

(a) analizzare e testare costantemente l'adeguatezza e la prontezza operativa della capacità di risposta esistente;

(b) riesaminare periodicamente la potenziale necessità di sviluppare nuovi mezzi di risposta a livello dell'UE attraverso rescEU;

(c) intensificare ulteriormente la collaborazione intersettoriale per garantire una risposta adeguata a livello dell'UE e organizzare esercitazioni periodiche per testare tale collaborazione;

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

(29) La Commissione, in cooperazione con l'alto rappresentante, in stretta consultazione con gli Stati membri e con il sostegno delle pertinenti agenzie dell'Unione, elaborerà un programma per gli incidenti e le crisi delle infrastrutture critiche che descriva e definisca gli obiettivi e le modalità di cooperazione tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE nel rispondere agli incidenti che colpiscono le infrastrutture critiche, in particolare laddove questi comportino perturbazioni significative della fornitura di servizi essenziali per il mercato interno. Tale programma dovrebbe avvalersi degli esistenti dispositivi integrati per la risposta politica alle crisi (IPCR) per il coordinamento della risposta.

(30) La Commissione collaborerà con i portatori di interessi e gli esperti in merito a possibili misure di recupero dopo gli incidenti riguardanti le infrastrutture dei cavi sottomarini, da presentare congiuntamente allo studio di valutazione di cui al punto 20, lettera a), ed elaborerà ulteriormente la pianificazione di emergenza, gli scenari di

rischio e i lavori sulla resilienza dell'Unione nei confronti delle catastrofi nell'ambito del meccanismo unionale di protezione civile.

CAPO IV: COOPERAZIONE INTERNAZIONALE

(31) La Commissione e l'alto rappresentante aiuteranno, se del caso e conformemente ai rispettivi compiti e responsabilità ai sensi del diritto dell'Unione, i paesi partner a rafforzare la resilienza dei soggetti che gestiscono infrastrutture critiche nel loro territorio.

(32) 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 attraverso il dialogo strutturato UE-NATO sulla resilienza e istituiranno a tal fine una task force.

(33) 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 gli orientamenti di attuazione di cui alle conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride[25] e in seguito a utilizzarle, per attuare pienamente tale quadro, in particolare al momento di esaminare e preparare risposte globali e coordinate dell'UE alle campagne ibride e alle minacce ibride, comprese quelle nei confronti di soggetti che gestiscono infrastrutture critiche.

(34) La Commissione prenderà in considerazione la partecipazione di rappresentanti di paesi terzi, ove pertinente e opportuno, nel quadro della cooperazione e dello scambio di informazioni tra gli esperti degli Stati membri nel settore della resilienza dei soggetti che gestiscono infrastrutture critiche.

[…]

Fatto a Strasburgo, il

Per il Consiglio
Il presidente

[25] Conclusioni del Consiglio su un quadro per una risposta coordinata dell'UE alle campagne ibride — Consilium (europa.eu)