Consiglio dell'Unione europea

Bruxelles, 7 settembre 2023
(OR. en)

12485/23
ADD 1

Fascicolo interistituzionale: 2023/0318(NLE)

PROCIV 57	ATO 48
ENV 925	CSC 408
JAI 1084	ECOFIN 839
SAN 494	CSCI 149
COSI 140	DATAPROTECT 216
CHIMIE 85	MI 698
ENFOPOL 356	CODEC 1500
RECH 380	COPS 418
CT 133	JAIEX 46
DENLEG 38	COPEN 292
COTER 153	IND 441
RELEX 987	POLMIL 221
ENER 467	IPCR 55
HYBRID 53	DIGIT 160
TRANS 329	DISINFO 62
CYBER 203	CSDP/PSDC 608
TELECOM 251	MARE 18
ESPACE 45	POLMAR 47

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	6 settembre 2023
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2023) 526 final ANNEX
Oggetto:	ALLEGATO della proposta di RACCOMANDAZIONE DEL CONSIGLIO relativa a un programma per coordinare una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera

Si trasmette in allegato, per le delegazioni, il documento COM(2023) 526 final ANNEX.

All.: COM(2023) 526 final ANNEX

COMMISSIONE
EUROPEA

Bruxelles, 6.9.2023
COM(2023) 526 final

ANNEX

ALLEGATO

della

proposta di RACCOMANDAZIONE DEL CONSIGLIO

relativa a un programma per coordinare una risposta a livello dell'Unione alle perturbazioni delle infrastrutture critiche con significativa rilevanza transfrontaliera

ALLEGATO

Il presente allegato descrive i principi, gli obiettivi, i principali attori, l'interazione con i meccanismi di risposta alle crisi esistenti e il funzionamento di un programma per coordinare la risposta agli incidenti significativi delle infrastrutture critiche ("programma per le infrastrutture critiche") e migliorare la cooperazione tra gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie competenti dell'Unione in relazione a tali incidenti, conformemente alle norme e alle procedure applicabili. Il presente programma non incide in alcun modo sul ruolo e sul funzionamento di altri accordi.

PARTE I: OBIETTIVI, PRINCIPI, ATTORI E ALTRI STRUMENTI

1. Obiettivi

Il presente programma mira a conseguire i seguenti tre obiettivi principali in risposta a un incidente significativo delle infrastrutture critiche:

(a) **una conoscenza situazionale condivisa**, poiché una buona comprensione degli incidenti significativi delle infrastrutture critiche negli Stati membri, della loro origine e delle loro potenziali conseguenze per tutte le parti interessate a livello operativo e strategico/politico è essenziale per una risposta coordinata adeguata;

(b) **una comunicazione pubblica coordinata**, che contribuisce ad attenuare gli effetti negativi di un incidente significativo delle infrastrutture critiche e a ridurre al minimo le discrepanze nei messaggi rivolti ai cittadini negli e fra gli Stati membri. Una comunicazione pubblica chiara è importante anche per attenuare le conseguenze della disinformazione;

(c) **una risposta efficace**, poiché rafforzando la reazione degli Stati membri e la cooperazione tra questi e con le istituzioni, gli organi, gli uffici e le agenzie competenti dell'Unione si contribuisce ad attenuare gli effetti degli incidenti significativi delle infrastrutture critiche e a consentire il rapido ripristino dei servizi essenziali in modo da ridurre al minimo la vulnerabilità a ulteriori incidenti significativi.

2. Principi

Proporzionalità

Gli eventi che disturbano il funzionamento delle infrastrutture critiche e/o la fornitura di servizi essenziali spesso si collocano al di sotto della soglia di incidente significativo delle infrastrutture critiche come specificato al punto 2 della presente raccomandazione.. In tal caso essi possono, in linea di principio, essere affrontati in modo efficace a livello nazionale. L'applicazione del programma per le infrastrutture critiche è limitata pertanto agli incidenti delle infrastrutture critiche di carattere significativo.

Sussidiarietà

Conformemente al diritto dell'Unione, gli Stati membri sono i principali responsabili della risposta al disfunzionamento di un'infrastruttura critica o dei servizi essenziali forniti dai soggetti critici, Le istituzioni, gli organi, gli uffici e le agenzie competenti dell'Unione, e il Servizio europeo per l'azione esterna ("SEAE"), rivestono tuttavia un importante ruolo complementare in caso di incidente significativo delle infrastrutture critiche di grande rilevanza transfrontaliera, in quanto tale incidente può avere ripercussioni su più settori o

persino su tutti i settori dell'attività economica nel mercato interno, sulla vita dei cittadini nell'Unione, sulla sicurezza e sulle relazioni internazionali dell'UE.

Complementarità

Il programma per le infrastrutture critiche tiene in considerazione e rispecchia il funzionamento dei meccanismi di gestione delle crisi esistenti a livello dell'Unione, segnatamente i dispositivi integrati del Consiglio per la risposta politica alle crisi ("IPCR"), il processo interno di coordinamento della Commissione in caso di crisi, ARGUS, il meccanismo di protezione civile dell'Unione ("UCPM"), coadiuvato dal Centro di coordinamento della risposta alle emergenze ("ERCC"), e il meccanismo di risposta alle crisi del SEAE. Si basa inoltre su accordi settoriali, tra cui le disposizioni per la gestione coordinata degli incidenti di cibersicurezza su vasta scala di cui alla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[1] e il quadro stabilito nel programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala ("programma per la cibersicurezza")[2], la rete dei punti di contatto per i trasporti[3] e la cellula europea di coordinamento dell'aviazione in caso di crisi[4].

Il programma per le infrastrutture critiche si basa inoltre sulle strutture e sui meccanismi istituiti dalla direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio[5], in particolare per quanto riguarda la cooperazione tra le autorità competenti e con la Commissione e nel quadro del gruppo per la resilienza dei soggetti critici, e deve essere applicato conformemente a tali strutture e meccanismi. Il programma tiene inoltre conto delle responsabilità delle istituzioni, degli organi, degli uffici e delle agenzie competenti dell'Unione nell'ambito del quadro giuridico ad essi applicabile. Le attività di risposta alle crisi delle infrastrutture critiche sono complementari agli altri meccanismi di gestione delle crisi a livello dell'Unione, nazionale e settoriale, che sostengono il coordinamento multisettoriale.

Riservatezza delle informazioni

Il programma per le infrastrutture critiche tiene conto dell'importanza di salvaguardare la riservatezza delle informazioni classificate e delle informazioni sensibili non classificate relative alle infrastrutture critiche e ai soggetti critici.

3. Attori rilevanti

Ciascuno Stato membro e le istituzioni, gli organi, gli uffici e le agenzie competenti dell'Unione di cui alle lettere da a) a e) in appresso decidono, conformemente alle norme e alle procedure ad essi applicabili, quali siano gli attori rilevanti per ogni incidente significativo delle infrastrutture critiche, a seconda dei settori interessati e del tipo di incidente.

---

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

[2] 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)

[3] Comunicazione della Commissione - "Un piano di emergenza per i trasporti", COM(2022) 211 final.

[4] Istituita a norma dell'articolo 19 del regolamento di esecuzione (UE) 2019/123 della Commissione, del 24 gennaio 2019, che stabilisce norme dettagliate per l'attuazione delle funzioni della rete di gestione del traffico aereo (ATM).

[5] Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (GU L 333 del 27.12.2022, pag. 164).

a) Stati membri:

- autorità competenti (ad esempio autorità responsabili delle infrastrutture critiche, autorità settoriali rilevanti, punti di contatto unici designati o istituiti a norma dell'articolo 9, paragrafo 2, della direttiva (UE) 2022/2557, autorità designate o istituite a norma dell'articolo 9, paragrafo 1, della direttiva (UE) 2022/2557);

- se del caso, la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe") di cui all'articolo 16 della direttiva (UE) 2022/2555;

- il gruppo di cooperazione di cui all'articolo 14 della direttiva (UE) 2022/2555;

- se del caso, altri portatori di interessi, compresi soggetti o persone del settore privato quali gli operatori di infrastrutture critiche, comprese quelle identificate come soggetti critici;

- i ministri responsabili della resilienza delle infrastrutture critiche e/o i ministri responsabili dei settori più colpiti dall'incidente significativo delle infrastrutture critiche in questione.

b) Consiglio:

- la Presidenza di turno;

- i gruppi di lavoro rilevanti, quali il gruppo "Protezione civile", compreso il sottogruppo sulla resilienza dei soggetti critici PROCIV-CER, e i presidenti dei gruppi di lavoro rilevanti a seconda dei settori interessati e della natura dell'incidente, quali il gruppo orizzontale "Questioni riguardanti il ciberspazio" e il gruppo orizzontale "Rafforzare la resilienza e contrastare le minacce ibride";

- il Coreper, il Comitato politico e di sicurezza e gli IPCR, tutti sostenuti dal Segretariato generale del Consiglio.

c) Commissione, compresi i suoi gruppi di esperti:

- il servizio capofila designato (a seconda del settore interessato) con il sostegno dell'ERCC quale polo operativo 24/7 per la gestione delle risposte alle crisi e la Direzione generale della Migrazione e degli affari interni quale servizio responsabile del settore e, in caso di incidente intersettoriale, la Direzione generale della Migrazione e degli affari interni e altri servizi competenti della Commissione;

- la Direzione generale della Comunicazione e il servizio del portavoce;

- la Direzione generale HERA (Autorità europea per la preparazione e la risposta alle emergenze sanitarie);

- il gruppo per la resilienza dei soggetti critici, presieduto da un rappresentante della Commissione (Direzione generale della Migrazione e degli affari interni), istituito dalla direttiva (UE) 2022/2557, e, se del caso, altri gruppi di esperti e comitati rilevanti;

- l'ERCC istituito nell'ambito dell'UCPM con decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio[6] (polo operativo di gestione delle emergenze 24/7 nell'ambito dell'UCPM, ubicato presso la Direzione generale per la Protezione civile e le operazioni di aiuto umanitario europee);

[6] 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).

- il gruppo di cooperazione di cui all'articolo 14 della direttiva (UE) 2022/2555;

- il Centro di conoscenza e analisi della situazione informatica;

- il Comitato per la sicurezza sanitaria, di cui all'articolo 4 del regolamento (UE) 2022/2371[7];

- il Segretariato generale della Commissione (segretariato ARGUS) e il Segretario generale (aggiunto) (procedura ARGUS), Direzione generale Risorse umane (Direzione Sicurezza);

- altri gruppi rilevanti di esperti della Commissione che la coadiuvano nel coordinamento delle misure in una situazione di emergenza o di crisi;

- altre reti di gestione delle crisi, anche settoriali (ad esempio la rete dei punti di contatto per i trasporti gestita dalla Direzione generale della Mobilità e dei trasporti, la task force interistituzionale per le crisi informatiche[8], la cellula europea di coordinamento dell'aviazione in caso di crisi);

- il Presidente e/o il Vicepresidente/Commissario responsabile.

d) SEAE

- la capacità unica di analisi dell'intelligence ("SIAC") composta dal Centro di criticità e di intelligence ("IntCen") e dalla Direzione dell'intelligence dello Stato maggiore dell'UE ("EUMS Int");

- il Centro di risposta alle crisi ("CRC");

- l'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e Vicepresidente della Commissione.

e) Organi e uffici competenti dell'Unione e agenzie competenti dell'Unione, come Europol, a seconda dei settori interessati[9].

4. Interazione con altri meccanismi e strumenti rilevanti di gestione delle crisi

Il programma per le infrastrutture critiche è uno strumento flessibile che delinea varie azioni che potrebbero essere intraprese in parte o *in toto* avvalendosi dei diversi dispositivi esistenti, in funzione della gravità dell'incidente significativo delle infrastrutture critiche e della necessità di un coordinamento operativo e strategico/politico.

---

[7] Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio, del 23 novembre 2022, relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE (GU L 314 del 6.12.2022, pag. 26).

[8] Un gruppo informale che comprende servizi competenti della Commissione, il SEAE, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), il CERT-UE ed Europol, copresieduto dalla Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie e dal SEAE.

[9] Come Europol; per i trasporti: l'Agenzia dell'Unione europea per la sicurezza aerea (AESA), l'Agenzia europea per la sicurezza marittima (EMSA) e l'Agenzia ferroviaria europea (ERA); per la sanità: il Centro europeo per la prevenzione e il controllo delle malattie (ECDC) e l'Agenzia europea per i medicinali (EMA); per l'energia: l'Agenzia per la cooperazione fra i regolatori nazionali dell'energia (ACER); per lo spazio: l'Agenzia dell'Unione europea per il programma spaziale (EUSPA); per il settore alimentare: l'Autorità europea per la sicurezza alimentare (EFSA); per il settore marittimo: l'Agenzia europea di controllo della pesca (EFCA); per gli incidenti informatici: l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), e la squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'UE (CERT-UE).

a) Protocollo dell'UE per contrastare le minacce ibride[10] ("protocollo dell'UE")

Il protocollo dell'UE si applica in caso di minacce ibride[11] fornendo una descrizione dei processi e degli strumenti applicabili in caso di minacce o campagne di minacce di questo tipo.

In caso di incidente significativo delle infrastrutture critiche con una dimensione ibrida, il protocollo dell'UE si applica in complementarità con il programma per le infrastrutture critiche, se del caso, ad esempio per informazioni, analisi o comunicazioni specifiche sugli aspetti ibridi dell'incidente e per quanto riguarda la cooperazione con i partner esterni.

b) Programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza transfrontalieri su vasta scala

Il programma per la cibersicurezza si applica agli incidenti transfrontalieri su vasta scala che causano perturbazioni talmente ampie da non poter essere gestite autonomamente dallo Stato membro interessato o che interessano due o più Stati membri o istituzioni dell'UE e hanno un impatto di rilevanza tecnica o politica di così vasta portata da richiedere un coordinamento politico e una risposta tempestivi a livello di Unione.

Nel caso di un incidente significativo delle infrastrutture critiche che coincida, o risulti essere collegato, con un incidente di cibersicurezza su vasta scala, i gruppi di lavoro del Consiglio rilevanti predispongono un coordinamento appropriato a livello operativo, anche con EU-CyCLONe, o attraverso una riunione congiunta fra il gruppo per la resilienza dei soggetti critici e il gruppo di cooperazione. Lo scopo del coordinamento è determinare quali attori, strumenti o meccanismi potrebbero contribuire nel modo più efficace alla risposta a tale incidente, evitando doppioni negli interventi e filoni di lavoro paralleli.

c) Meccanismo di protezione civile dell'Unione e Centro di coordinamento della risposta alle emergenze

In linea con la decisione n. 1313/2013/UE su un meccanismo unionale di protezione civile, le risposte operative tramite l'UCPM alle catastrofi naturali e provocate dall'uomo, attuali o imminenti (comprese quelle che provocano perturbazioni delle infrastrutture critiche), all'interno e all'esterno dell'Unione, sono condotte dall'ERCC, il polo operativo unico della Commissione, attivo 24/7, per la gestione delle risposte alle crisi. In tali casi, l'ERCC può emanare un'allerta rapida, fornire notifiche e analisi e sostenere la condivisione delle informazioni e, in caso di attivazione dell'UCPM da parte di uno Stato membro, può inviare assistenza operativa ed esperti nelle zone colpite. L'ERCC può inoltre agevolare il coordinamento settoriale e intersettoriale sia a livello dell'Unione che tra l'Unione e le autorità nazionali competenti, comprese quelle responsabili della protezione civile e della resilienza delle infrastrutture critiche.

d) Altri meccanismi e strumenti settoriali o intersettoriali

Il programma per le infrastrutture critiche non costituisce un doppione di altri strumenti di gestione delle crisi o meccanismi di coordinamento settoriali o intersettoriali. Qualora tali strumenti o meccanismi già esistano nel settore interessato, il programma per le infrastrutture critiche, nel suo ambito di applicazione, può essere utilizzato come strumento complementare

---

[10] Documento di lavoro congiunto dei servizi - Protocollo dell'UE per contrastare le minacce ibride SWD(2023) 116 final.

[11] Le minacce ibride possono essere definite come una combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali, che possono essere usati in modo coordinato da soggetti statali o non statali per raggiungere determinati obiettivi, pur rimanendo sempre al di sotto della soglia di una guerra ufficialmente dichiarata. Si veda il protocollo dell'UE relativo alle minacce ibride.

agli strumenti o meccanismi settoriali o intersettoriali, senza tuttavia sostituirli. Dovrebbe essere garantito il necessario coordinamento tra i vari attori in modo da evitare tali duplicazioni. Ciò potrebbe essere realizzato, ad esempio, nel quadro del processo interno di coordinamento della Commissione in caso di crisi, ARGUS, coadiuvato dall'ERCC, e/o nelle riunioni di coordinamento IPCR.

PARTE II: SCAMBIO DI INFORMAZIONI E RISPOSTA COORDINATA

Le azioni descritte di seguito consistono in modalità di cooperazione, vale a dire scambio di informazioni, comunicazione coordinata e risposta. Questa struttura corrisponde alle modalità del meccanismo di coordinamento del Consiglio in caso di crisi (IPCR) e tiene conto, più in generale, del potenziale utilizzo dei meccanismi di coordinamento in caso di crisi già esistenti a livello dell'UE. La struttura mostra in che modo tali modalità di cooperazione si integrerebbero, se utilizzate. La maggior parte di queste azioni possono tuttavia anche essere intraprese autonomamente: non dipendono dall'utilizzo di tale meccanismo, ma piuttosto lo completano. Le azioni sono presentate in ordine cronologico, tenendo conto del fatto che, in caso di una crisi su vasta scala che costituisca un incidente significativo delle infrastrutture critiche, possono essere intraprese simultaneamente e continuativamente più azioni.

1. SCAMBIO DI INFORMAZIONI

(a) A livello operativo

Gli Stati membri interessati dall'incidente significativo delle infrastrutture critiche applicano le proprie misure di emergenza e garantiscono il coordinamento con i pertinenti meccanismi nazionali di gestione delle crisi e il coinvolgimento di tutti i rilevanti attori nazionali, regionali e locali, a seconda dei casi.

Se del caso, per quanto riguarda l'assistenza della protezione civile, il coordinamento tra gli Stati membri e con la Commissione è assicurato tramite l'ERCC nell'ambito dell'UCPM.

i) Condivisione delle informazioni e notifica da parte delle autorità nazionali competenti

Oltre agli obblighi di notifica e informazione di cui all'articolo 15 della direttiva (UE) 2022/2557, le autorità nazionali competenti per le infrastrutture critiche degli Stati membri interessati dall'incidente significativo condividono con la Presidenza di turno del Consiglio e la Commissione, attraverso i loro punti di contatto unici e senza indebito ritardo, le informazioni rilevanti ricevute dagli operatori delle infrastrutture critiche, dai soggetti critici o da altre fonti, nonché le informazioni relative ai meccanismi di gestione delle crisi attivati. Per la Commissione, l'ERCC garantisce su base 24/7 contatto operativo e capacità, e coordina, monitora e supporta in tempo reale la risposta alle emergenze a livello dell'Unione, fungendo per gli Stati membri e per la Commissione da polo operativo per la risposta alle crisi promuovendo un approccio intersettoriale alla gestione delle catastrofi.

Tale condivisione di informazioni riguarda la natura dell'incidente significativo dell'infrastruttura critica, la sua causa, l'impatto osservato o stimato della perturbazione sull'infrastruttura critica e sulla fornitura di servizi essenziali, le conseguenze dell'incidente a livello intersettoriale e transfrontaliero e le misure di attenuazione, già adottate o previste, a livello nazionale o con altri Stati membri interessati e la Commissione, sulla base delle disposizioni esistenti, ad esempio quelle riguardanti la condivisione delle informazioni di cui agli articoli 9 e 15 della direttiva (UE) 2022/2557. Tale notifica è fornita senza sottrarre le

risorse dell'infrastruttura critica o, in alcuni casi, del soggetto critico o dello Stato membro, dalle attività relative alla gestione degli incidenti, che devono essere considerate prioritarie.

Al fine di garantire un seguito, l'ERCC o i servizi della Commissione responsabili del settore o dei settori in cui si è verificato l'incidente significativo delle infrastrutture critiche, e ai quali tale incidente è stato notificato, informano il punto di contatto presso la Direzione generale della Migrazione e degli affari interni e il Segretariato generale della Commissione. Nel frattempo, se non lo ha ancora fatto, l'ERCC inizia a monitorare gli eventi, in particolare in caso di attivazione dell'UCPM da parte di uno o più degli Stati membri interessati.

Qualora le informazioni possano essere rilevanti per affrontare una dimensione di cibersicurezza o possano essere collegate a un incidente di cibersicurezza, la Commissione condivide tali informazioni pertinenti con EU-CyCLONe.

Le autorità nazionali competenti a norma della direttiva (UE) 2022/2557 sono tenute a cooperare e a scambiare informazioni con le autorità competenti a norma della direttiva (UE) 2022/2555, senza indebito ritardo, in relazione agli incidenti informatici e agli incidenti che interessano i soggetti critici, anche per quanto riguarda le misure di cibersicurezza e fisiche da questi adottate.

Per quanto riguarda il settore marittimo, le autorità nazionali valutano la possibilità di utilizzare l'ambiente comune per la condivisione delle informazioni ("CISE") per il loro scambio tempestivo.

ii) Organizzazione di riunioni di esperti

La Commissione convoca quanto prima il gruppo per la resilienza dei soggetti critici per agevolare lo scambio delle informazioni rilevanti tra le autorità nazionali competenti responsabili delle infrastrutture critiche e le istituzioni, gli organi, gli uffici e le agenzie competenti dell'Unione sull'incidente (natura, causa, impatto e conseguenze a livello intersettoriale e transfrontaliero) e sulle azioni di risposta, comprese le misure di attenuazione e il supporto tecnico agli Stati membri interessati. A seconda del centro di gravità dell'incidente, i servizi competenti della Commissione saranno strettamente associati alla riunione del gruppo per la resilienza dei soggetti critici al fine di condividere le informazioni raccolte attraverso gli strumenti settoriali esistenti. In caso di incidenti con una combinazione di aspetti di cibersicurezza e di aspetti fisici non informatici, i servizi competenti della Commissione, il CERT-UE e il SEAE, ove opportuno, comunicano e si consultano quanto prima nel quadro della task force per le crisi informatiche, nonché con i rispettivi presidenti del gruppo di cooperazione di cui all'articolo 14 della direttiva (UE) 2022/2555 e, se del caso, EU-CyCLONe, in merito alla necessità di attività di coordinamento. D'intesa con i rispettivi presidenti, la Commissione (Direzione generale della Migrazione e degli affari interni e Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie) può proporre una riunione congiunta fra il gruppo per la resilienza dei soggetti critici e il gruppo di cooperazione ai fini della condivisione della conoscenza situazionale e di coordinamento delle rispettive risposte.

In caso di incidente significativo delle infrastrutture critiche intersettoriale che richieda o possa richiedere una gestione delle conseguenze a livello dell'Unione, la Commissione può convocare riunioni di coordinamento intersettoriale con la partecipazione di tutte le parti interessate.

Nel caso in cui un incidente significativo delle infrastrutture critiche interessi anche un paese terzo, la Commissione consulta le autorità competenti del paese terzo colpito e può invitarle a una riunione del gruppo per la resilienza dei soggetti critici.

iii) Sostegno da parte della Commissione e delle agenzie dell'Unione

Se del caso e agendo conformemente al suo mandato, Europol presenta una relazione sulla situazione dell'incidente a livello dell'Unione. Le altre agenzie dell'Unione, se del caso e agendo conformemente ai rispettivi mandati, comunicano informazioni rilevanti che contribuiscono alla conoscenza situazionale o alla risposta coordinata all'incidente significativo delle infrastrutture critiche alle rispettive direzioni generali "di riferimento" che, a loro volta, riferiscono alla Commissione (alla Direzione generale della Migrazione e degli affari interni, in qualità di presidente del gruppo per la resilienza dei soggetti critici).

La Commissione può fornire un contributo alla conoscenza situazionale utilizzando le risorse del programma spaziale dell'Unione[12], quali Copernicus, Galileo ed EGNOS, se del caso e conformemente al quadro giuridico applicabile.

(b) A livello strategico

i) Elaborazione di relazioni sulla conoscenza situazionale

Sulla base delle informazioni condivise dalle autorità nazionali competenti in sede di riunione del gruppo per la resilienza dei soggetti critici o in riunioni congiunte con i servizi, i gruppi di esperti o le reti rilevanti, la Commissione elabora una relazione sulla conoscenza situazionale fondata su tali contributi delle autorità nazionali competenti e su altre informazioni disponibili.

Tale relazione, se del caso, terrà conto dei risultati delle rilevanti valutazioni dei rischi, analisi e scenari a livello dell'UE dal punto di vista della cibersicurezza, compresi quelli effettuati dalla Commissione, dall'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e dal gruppo di cooperazione.

In caso di attivazione degli IPCR, tale relazione può contribuire alla relazione sulla conoscenza e l'analisi integrate della situazione ("ISAA") preparata dai servizi della Commissione e dal SEAE.

La SIAC presenta se del caso una valutazione dell'incidente aggiornata e basata sull'intelligence.

ii) Attivazione dei meccanismi di coordinamento dell'Unione in caso di crisi e uso degli strumenti dell'Unione

L'ERCC inizia se del caso a fornire sostegno per la conoscenza situazionale relativa all'incidente, in particolare qualora l'evento determini l'attivazione dell'UCPM[13]. Gli Stati membri interessati possono inoltre richiedere immagini satellitari del loro territorio tramite il servizio di gestione delle emergenze di Copernicus.

Qualora si ritenga appropriato condividere informazioni fra la Commissione e il SEAE e le agenzie competenti dell'Unione, la Direzione generale capofila o la Direzione generale della Migrazione e degli affari interni, in coordinamento con il Segretariato generale, attiva il processo interno di coordinamento della Commissione in caso di crisi, ARGUS, Fase I, aprendo un evento tramite lo strumento informatico ARGUS.

---

[12] 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).

[13] Come la pubblicazione di prodotti di monitoraggio dei media, messaggi di protezione civile, resoconti analitici, mappe giornaliere di ECHO, flash giornalieri di ECHO, e altri prodotti su misura.

La Presidenza di turno del Consiglio dell'Unione può attivare i dispositivi IPCR in modalità "scambio di informazioni", il che comporta l'elaborazione di relazioni ISAA da parte della Commissione e del SEAE con contributi delle autorità nazionali competenti e di altre fonti, se del caso. Anche senza attivare gli IPCR, la Presidenza di turno del Consiglio o la Commissione, a determinate condizioni, possono creare una pagina di monitoraggio sulla piattaforma web IPCR.

Possono essere se del caso attivati altri meccanismi e strumenti (settoriali) di gestione delle crisi a livello dell'Unione seguendo le rispettive procedure. La Commissione garantirà il coordinamento tra tali meccanismi e strumenti.

Se l'incidente fisico coincide o sembra essere connesso a un incidente di cibersicurezza su vasta scala, quale definito all'articolo 6, punto 7, della direttiva (UE) 2022/2555, la Presidenza di turno del Consiglio può ricorrere al programma per la cibersicurezza per stabilire un coordinamento adeguato a livello operativo che coinvolga, tra l'altro, EU CyCLONe e il gruppo per la resilienza dei soggetti critici.

iii) Coordinamento della comunicazione pubblica

Gli Stati membri interessati dall'incidente significativo dell'infrastruttura critica coordinano, per quanto possibile, la loro comunicazione pubblica sulla crisi, nel rispetto delle competenze nazionali in materia, con il coinvolgimento, se del caso, della rete IPCR per le comunicazioni in caso di crisi.

Sulla base della conoscenza situazionale condivisa, il gruppo per la resilienza dei soggetti critici e gli Stati membri interessati sostengono, se del caso, la formulazione di linee di comunicazione pubblica concordate.

Sempre sulla base della conoscenza situazionale condivisa, Europol e le altre agenzie competenti dell'Unione coordinano le loro attività di comunicazione pubblica con il servizio del portavoce della Commissione.

Se l'incidente significativo delle infrastrutture critiche comporta una dimensione esterna, ibrida, o di politica di sicurezza e di difesa comune, la comunicazione pubblica è coordinata con il SEAE e con il servizio del portavoce della Commissione conformemente al Protocollo per contrastare le minacce ibride[14].

2. RISPOSTA (COMPRESE AZIONI CONTINUE DESCRITTE NELL'AMBITO DELLO SCAMBIO DI INFORMAZIONI E AZIONI SUPPLEMENTARI A LIVELLO STRATEGICO/POLITICO)

(a) A livello strategico

i) Elaborazione continua di relazioni situazionali

Il gruppo "Protezione civile — Resilienza dei soggetti critici" (PROCIV-CER) del Consiglio è informato dell'elaborazione di una relazione situazionale politico/strategica (ad esempio l'ISAA in caso di attivazione degli IPCR o la relazione sulla conoscenza situazionale condivisa redatta dalla Commissione), e prepara la riunione del Coreper, qualora quest'ultimo non sia ancora stato convocato, o del comitato politico e di sicurezza, a seconda dei casi.

[14] Documento di lavoro congiunto dei servizi - Protocollo dell'UE per contrastare le minacce ibride SWD(2023) 116 final.

La SIAC intensifica i suoi contatti con i servizi di intelligence degli Stati membri, aggrega le informazioni di tutte le fonti ed elabora un'analisi e una valutazione dell'incidente, nonché aggiornamenti periodici, se necessario.

ii) Attivazione completa dei meccanismi di coordinamento dell'Unione in caso di crisi e uso degli strumenti dell'Unione

Nel caso in cui il Presidente della Commissione attivi il processo interno di coordinamento della Commissione in caso di crisi, ARGUS Fase II, sono convocate riunioni del comitato di coordinamento in caso di crisi con la partecipazione dei servizi della Commissione e delle agenzie competenti e del SEAE, se del caso, con breve preavviso al fine di organizzare tutti gli aspetti dell'incidente significativo delle infrastrutture critiche.

Nel caso in cui la Presidenza del Consiglio attivi gli IPCR in modalità completa:

- la Presidenza di turno del Consiglio convoca tempestivamente una tavola rotonda informale che riunisca gli attori nazionali, europei e internazionali competenti, in cui il rappresentante della Commissione che funge da presidente del gruppo per la resilienza dei soggetti critici (Direzione generale della Migrazione e degli affari interni) possa riferire in merito alle riunioni del gruppo precedentemente tenutesi, eventualmente con l'intervento di altri servizi della Commissione e del SEAE;

- in tale riunione la SIAC e le agenzie dell'Unione competenti possono essere invitate a presentare un aggiornamento sulla situazione in relatzione all'incidente significativo dell'infrastruttura critica.

Il servizio capofila per l'ISAA (il servizio capofila della Commissione o il SEAE) prepara la relazione ISAA con i contributi dei servizi competenti della Commissione, degli uffici, organi e agenzie competenti dell'Unione e delle autorità competenti nazionali. Gli Stati membri sono invitati a contribuire, tramite la piattaforma web IPCR, all'elaborazione delle relazioni ISAA.

In caso di incidente significativo delle infrastrutture critiche con una rilevanza a livello di sicurezza internazionale, i servizi della Commissione e il SEAE possono convocare una riunione nel quadro del dialogo strutturato UE-NATO sulla resilienza per contribuire alla condivisione della conoscenza situazionale e allo scambio di informazioni sulle misure adottate rispettivamente dall'Unione e dalla NATO.

iii) Comunicazione pubblica

Il Consiglio prepara messaggi comuni di comunicazione pubblica. La rete informale dei responsabili della comunicazione in caso di crisi istituita tramite gli IPCR può coadiuvare in questo lavoro. Messaggi di comunicazione pubblica sono elaborati, se del caso, anche dal servizio del portavoce della Commissione.

Se l'incidente significativo delle infrastrutture critiche comporta una dimensione esterna, ibrida, o di politica di sicurezza e di difesa comune, la comunicazione pubblica è coordinata con il SEAE e con il servizio del portavoce della Commissione.

iv) Sostegno agli Stati membri e risposta efficace

La Presidenza di turno può convocare una riunione del PROCIV-CER per coadiuvare nelle attività svolte nel quadro degli IPCR, se attivati.

Gli Stati membri interessati da un incidente significativo delle infrastrutture critiche possono chiedere il supporto tecnico di altri Stati membri o delle istituzioni, degli organi e delle agenzie competenti dell'Unione tramite il gruppo per la resilienza dei soggetti critici (ad esempio competenze specifiche per attenuare gli effetti negativi dell'incidente).

Gli Stati membri interessati da un incidente significativo delle infrastrutture critiche possono anche chiedere il supporto tecnico e/o finanziario della Commissione o delle agenzie competenti dell'Unione. La Commissione, in coordinamento con le agenzie competenti dell'Unione, valuta il possibile supporto e attiva, se del caso, misure tecniche di attenuazione a livello dell'Unione seguendo le procedure ad esse attinenti e coordina le capacità tecniche necessarie per arrestare o ridurre l'impatto dell'incidente significativo delle infrastrutture critiche.

Nel contesto specifico dell'UCPM, i paesi colpiti potrebbero chiedere assistenza attraverso il sistema comune di comunicazione e di informazione in caso di emergenza ("CECIS"') - e a seguito di ciò l'ERCC si adopererebbe per coordinare la prestazione di tale assistenza da parte degli Stati membri e degli Stati partecipanti all'UCPM - come pure attraverso "rescEU".

Nell'ambito dei loro rispettivi mandati e su richiesta, Europol e le altre agenzie competenti dell'Unione assistono gli Stati membri colpiti da un incidente significativo delle infrastrutture critiche nelle indagini relative all'evento.

(b) A livello politico

La Presidenza del Consiglio potrebbe considerare la necessità di convocare tavole rotonde IPCR, riunioni dei gruppi di lavoro del Consiglio, il Coreper, il Consiglio dei Ministri e/o vertici, allo scopo di scambiare informazioni sulla possibile origine e le conseguenze previste dell'incidente significativo delle infrastrutture critiche per gli Stati membri e per l'Unione, concordare orientamenti comuni, e adottare le misure necessarie per fornire sostegno agli Stati membri colpiti dall'incidente significativo delle infrastrutture critiche ed attenuarne gli effetti.

Grafico 1: Quadro schematico del programma per le infrastrutture critiche

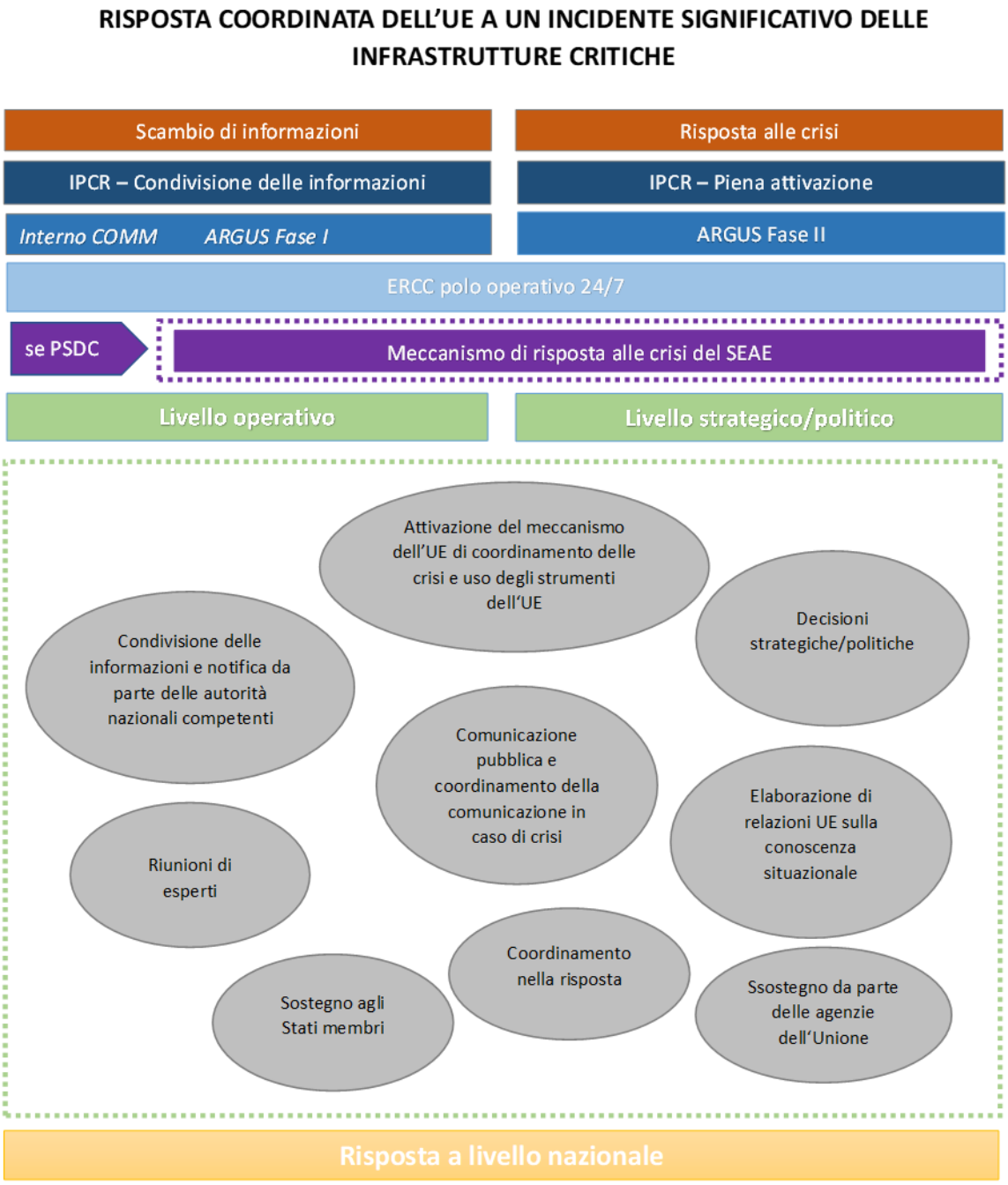

Grafico 2: Quadro decisionale del programma per le infrastrutture critiche