Consiliul
Uniunii Europene

Bruxelles, 7 septembrie 2023
(OR. en)

12485/23
ADD 1

Dosar interinstituțional:
2023/0318 (NLE)

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	6 septembrie 2023
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2023) 526 final
Subiect:	ANEXĂ la Propunerea de RECOMANDARE A CONSILIULUI referitoare la un Plan de acțiune privind un răspuns coordonat la nivelul Uniunii la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă

În anexă, se pune la dispoziția delegațiilor documentul COM(2023) 526 final.

Anexă: COM(2023) 526 final

COMISIA
EUROPEANĂ

Bruxelles, 6.9.2023
COM(2023) 526 final

ANNEX

ANEXĂ

la

Propunerea de RECOMANDARE A CONSILIULUI

referitoare la un Plan de acțiune privind un răspuns coordonat la nivelul Uniunii la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă

ANEXĂ

Prezenta anexă descrie principiile, obiectivele, principalii actori, interacțiunea cu mecanismele existente de răspuns la situații de criză și funcționarea planului de acțiune pentru coordonarea răspunsului la incidentele semnificative la nivelul infrastructurii critice („Planul de acțiune pentru infrastructura critică”) și îmbunătățește cooperarea dintre statele membre și instituțiile, organele, oficiile și agențiile relevante ale Uniunii în legătură cu astfel de incidente, în conformitate cu normele și procedurile aplicabile. Prezentul plan de acțiune nu aduce atingere în niciun fel rolului și funcționării altor acorduri.

PARTEA I: OBIECTIVE, PRINCIPII, ACTORI ȘI ALTE INSTRUMENTE

1. Obiective

Planul de acțiune pentru infrastructura critică vizează realizarea următoarelor trei obiective principale ca răspuns la un incident semnificativ la nivelul infrastructurii critice:

(a) **conștientizarea comună a situației**, întrucât o bună înțelegere a incidentului semnificativ la nivelul infrastructurii critice din statele membre, a originii acestuia și a consecințelor sale potențiale la nivel operațional și strategic/politic pentru toate părțile interesate relevante este esențială pentru furnizarea unui răspuns coordonat adecvat;

(b) **comunicarea publică coordonată**, întrucât aceasta contribuie la atenuarea efectelor negative ale unui incident semnificativ la nivelul infrastructurii critice și reduce la minimum discrepanțele dintre mesajele transmise publicului în statele membre și între acestea. Comunicarea publică clară este, de asemenea, importantă pentru a contracara consecințele dezinformării;

(c) **un răspuns eficace**, întrucât consolidarea răspunsului statelor membre și cooperarea dintre statele membre și cu instituțiile, organele, oficiile și agențiile relevante ale Uniunii contribuie la atenuarea efectelor unui incident semnificativ la nivelul infrastructurii critice și la restabilirea rapidă a serviciilor esențiale într-un mod care reduce la minimum vulnerabilitatea la alte incidente semnificative.

2. Principii

Proporționalitatea

Incidentele care perturbă infrastructura critică și/sau furnizarea de servicii esențiale se situează adesea sub pragul unui incident semnificativ la nivelul infrastructurii critice, astfel cum se specifică la punctul 2 din prezenta recomandare. Ca atare, acestea pot fi, în principiu, abordate în mod eficace la nivel național. Prin urmare, aplicarea Planului de acțiune pentru infrastructura critică este limitată la incidentele semnificative la nivelul infrastructurii critice.

Subsidiaritatea

Statele membre au responsabilitatea principală de a răspunde perturbărilor unei infrastructuri critice sau ale serviciilor esențiale furnizate de entitățile critice, în conformitate cu dreptul Uniunii. Cu toate acestea, instituțiile, organele, oficiile și agențiile relevante ale Uniunii și Serviciul European de Acțiune Externă („SEAE”) au un rol complementar important în cazul unui incident semnificativ la nivelul infrastructurii critice cu relevanță transfrontalieră majoră, deoarece un astfel de incident poate afecta mai multe sau chiar toate sectoarele de activitate economică din cadrul pieței interne, viața cetățenilor care trăiesc în Uniune, securitatea și relațiile internaționale ale Uniunii.

Complementaritatea

Planul de acțiune pentru infrastructura critică ia în considerare și reflectă funcționarea mecanismelor existente de gestionare a crizelor la nivelul Uniunii, și anume mecanismul IPCR (mecanismul integrat al UE pentru un răspuns politic la crize) din cadrul Consiliului, ARGUS – procesul de coordonare internă în caz de criză al Comisiei –, mecanismul de protecție civilă al Uniunii („UCPM”), sprijinit de Centrul de coordonare a răspunsului la situații de urgență („ERCC”) și mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă. Planul de acțiune pentru infrastructura critică se bazează, de asemenea, pe acordurile sectoriale, inclusiv pe dispozițiile privind gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare prevăzute de Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[1] și pe cadrul stabilit în Planul de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare („Planul de acțiune în materie de securitate cibernetică”)[2], pe rețeaua punctelor de contact în domeniul transporturilor[3] și pe Celula Europeană de Coordonare a Crizelor din Aviație[4].

În plus, Planul de acțiune pentru infrastructura critică se bazează pe structurile și mecanismele instituite prin Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului[5] și urmează să fie aplicat în conformitate cu acestea, în special în ceea ce privește cooperarea dintre autoritățile competente și cu Comisia, precum și în cadrul Grupului privind reziliența entităților critice. De asemenea, planul de acțiune ține seama de responsabilitățile instituțiilor, organelor, oficiilor și agențiilor relevante ale Uniunii în temeiul cadrului juridic care li se aplică. Activitățile de răspuns la situațiile de criză la nivelul infrastructurii critice sunt complementare cu alte mecanisme de gestionare a crizelor la nivelul Uniunii, la nivel național și la nivel sectorial, care sprijină coordonarea multisectorială.

Confidențialitatea informațiilor

Planul de acțiune pentru infrastructura critică ține seama de importanța protejării confidențialității informațiilor clasificate și a informațiilor neclasificate sensibile referitoare la infrastructura critică și la entitățile critice.

3. Actori relevanți

Fiecare stat membru și instituțiile, organele, oficiile și agențiile relevante ale Uniunii menționate la literele (a)-(e) de mai jos vor decide, în conformitate cu normele și procedura care li se aplică, cu privire la actorul (actorii) relevant (relevanți) pentru fiecare incident semnificativ la nivelul infrastructurii critice, în funcție de sectorul (sectoarele) afectat(e) și de tipul de incident.

---

[1] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (JO L 333, 27.12.2022, p. 80).

[2] Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

[3] Comunicarea Comisiei intitulată „Un plan de urgență pentru sectorul transporturilor” [COM(2022) 211 final].

[4] Instituită în temeiul articolului 19 din Regulamentul de punere în aplicare (UE) 2019/123 al Comisiei din 24 ianuarie 2019 de stabilire a normelor de punere în aplicare a funcțiilor rețelei de management al traficului aerian (ATM).

[5] Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164).

a) Statele membre

- autoritățile competente [de exemplu, autoritățile responsabile cu infrastructura critică, autoritățile sectoriale relevante, punctele unice de contact desemnate sau instituite în temeiul articolului 9 alineatul (2) din Directiva (UE) 2022/2557, autoritățile desemnate sau instituite în temeiul articolului 9 alineatul (1) din Directiva (UE) 2022/2557];

- după caz, Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe”), astfel cum este menționată la articolul 16 din Directiva (UE) 2022/2555;

- Grupul de cooperare menționat la articolul 14 din Directiva (UE) 2022/2555;

- după caz, alte părți interesate, inclusiv entități sau persoane din sectorul privat, cum ar fi operatorii de infrastructură critică, inclusiv cei identificați ca entități critice;

- miniștrii responsabili cu reziliența infrastructurii critice și/sau ministrul (miniștrii) responsabil(i) cu sectorul sau sectoarele cele mai afectate de incidentul semnificativ la nivelul infrastructurii critice în cauză.

b) Consiliul

- președinția prin rotație;

- grupurile de lucru relevante, cum ar fi Grupul de lucru pentru protecție civilă, inclusiv subgrupul privind reziliența entităților critice PROCIV-CER și președintele (președinții) grupului (grupurilor) de lucru relevant(e), în funcție de sectorul (sectoarele) afectat(e) și de natura incidentului, cum ar fi Grupul de lucru orizontal pentru chestiuni cibernetice și Grupul de lucru orizontal pentru sporirea rezilienței și contracararea amenințărilor hibride;

- Coreper, Comitetul politic și de securitate și IPCR, toate beneficiind de sprijinul Secretariatului General al Consiliului.

c) Comisia, inclusiv grupurile de experți ale Comisiei

- serviciul principal desemnat (în funcție de sectorul afectat), sprijinit de ERCC în calitate de centru operațional care gestionează răspunsurile la situații de criză 24 de ore din 24, 7 zile pe săptămână, și Direcția Generală Migrație și Afaceri Interne, în calitate de serviciu responsabil în domeniu și, în cazul unui incident transsectorial, Direcția Generală Migrație și Afaceri Interne și alte servicii relevante ale Comisiei;

- Direcția Generală Comunicare și serviciul purtătorului de cuvânt;

- Direcția Generală HERA – Autoritatea Europeană pentru Pregătire și Răspuns în caz de Urgență Sanitară;

- Grupul privind reziliența entităților critice, prezidat de un reprezentant al Comisiei (Direcția Generală Migrație și Afaceri Interne), instituit prin Directiva (UE) 2022/2557, și, după caz, alte grupuri de experți și comitete relevante;

- ERCC instituit în cadrul UCPM prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului[6] (centru operațional de gestionare a situațiilor de urgență, care funcționează

[6] Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).

24 de ore din 24, 7 zile pe săptămână în cadrul UCPM și situat în clădirea Direcției Generale Protecție Civilă și Operațiuni Umanitare Europene);

- Grupul de cooperare menționat la articolul 14 din Directiva (UE) 2022/2555;

- Centrul de conștientizare a situației cibernetice și de analiză;

- Comitetul pentru securitate sanitară menționat la articolul 4 din Regulamentul (UE) 2022/2371[7];

- Secretariatul General al Comisiei (secretariatul ARGUS) și secretarul general (adjunct) (procesul ARGUS), Direcția Generală Resurse Umane (Direcția Securitate);

- alte grupuri de experți relevante ale Comisiei, care asistă Comisia în coordonarea măsurilor în situații de urgență sau de criză;

- alte rețele de gestionare a crizelor, inclusiv sectoriale (de exemplu, Rețeaua punctelor de contact în domeniul transporturilor, gestionată de Direcția Generală Mobilitate și Transporturi, Grupul operativ interinstituțional în materie de crize cibernetice[8], Celula Europeană de Coordonare a Crizelor din Aviație);

- Președintele și/sau vicepreședintele/comisarul responsabil.

d) SEAE

- Capacitatea unică de analiză a informațiilor („SIAC”), compusă din Centrul de situații și de analiză a informațiilor („IntCen”) și din Direcția pentru informații a Statului-Major al Uniunii Europene („EUMS Int”);

- Centrul de răspuns în caz de criză („CRC”);

- Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate/Vicepreședinte al Comisiei.

e) Organismele și oficiile relevante ale Uniunii, precum și agențiile relevante ale Uniunii, de exemplu Europol, în funcție de sectorul (sectoarele) afectat(e)[9].

---

[7] Regulamentul (UE) 2022/2371 al Parlamentului European și al Consiliului din 23 noiembrie 2022 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 1082/2013/UE (JO L 314, 6.12.2022, p. 26).

[8] Un grup informal care cuprinde serviciile relevante ale Comisiei, SEAE, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), CERT-UE și Europol, coprezidat de Direcția Generală Rețele de Comunicare, Conținut și Tehnologie și SEAE.

[9] De exemplu Europol; pentru transport: Agenția Uniunii Europene pentru Siguranța Aviației (AESA), Agenția Europeană pentru Siguranță Maritimă (EMSA), Agenția Uniunii Europene pentru Căile Ferate (ERA); pentru sănătate: Centrul European de Prevenire și Control al Bolilor (ECDC) și Agenția Europeană pentru Medicamente (EMA); pentru energie: Agenția Uniunii Europene pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei (ACER); pentru spațiu: Agenția Uniunii Europene pentru Programul spațial (EUSPA); pentru sectorul alimentar: Autoritatea Europeană pentru Siguranța Alimentară (EFSA); pentru domeniul maritim: Agenția Europeană pentru Controlul Pescuitului (EFCA); pentru incidente cibernetice: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), echipele de intervenție în caz de incidente de securitate informatică (CSIRT), Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE).

4. Interacțiunea cu alte mecanisme și instrumente relevante de gestionare a crizelor

Planul de acțiune pentru infrastructura critică este un instrument flexibil care cartografiază diverse acțiuni care ar putea fi întreprinse parțial sau integral utilizând diferitele mecanisme existente, în funcție de natura și gravitatea incidentului semnificativ la nivelul infrastructurii critice și de necesitatea unei coordonări operaționale și strategice/politice.

a) Protocolul UE pentru combaterea amenințărilor hibride[10] („protocolul UE”)

Protocolul UE se aplică în cazul amenințărilor hibride[11], oferind o prezentare generală a proceselor și a instrumentelor aplicabile în cazul unor astfel de amenințări sau campanii.

În cazul unui incident semnificativ la nivelul infrastructurii critice cu o dimensiune hibridă, protocolul UE se aplică în complementaritate cu Planul de acțiune pentru infrastructura critică, după caz, de exemplu pentru informații, analize sau comunicări specifice privind aspectele hibride ale incidentului semnificativ la nivelul infrastructurii critice și în ceea ce privește cooperarea cu partenerii externi.

b) Planul de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare

Planul de acțiune în materie de securitate cibernetică se aplică incidentelor transfrontaliere de mare amploare care afectează statul membru vizat într-o măsură prea mare pentru a gestiona situația pe cont propriu sau care afectează două sau mai multe state membre ori instituții ale UE, consecințele tehnice sau politice fiind atât de ample și de importante încât trebuie să se asigure rapid coordonarea politicilor și răspunsul la nivelul politic al Uniunii.

În cazul unui incident semnificativ la nivelul infrastructurii critice care coincide sau pare să fie legat de un incident de securitate cibernetică de mare amploare, grupurile de lucru relevante ale Consiliului ar trebui să stabilească o coordonare adecvată la nivel operațional, inclusiv cu EU-CyCLONe sau printr-o reuniune comună a Grupului privind reziliența entităților critice și a Grupului de cooperare. Scopul coordonării este de a determina actorul, instrumentul (instrumentele) sau mecanismul (mecanismele) care ar putea răspunde în modul cel mai eficace la incidentul semnificativ la nivelul infrastructurii critice, evitând astfel duplicarea și direcțiile de lucru paralele.

c) Mecanismul de protecție civilă al Uniunii și Centrul de coordonare a răspunsului la situații de urgență

În conformitate cu Decizia nr. 1313/2013/UE privind un mecanism de protecție civilă al Uniunii, răspunsurile operaționale în cadrul UCPM la dezastre naturale și provocate de om reale sau iminente (inclusiv la dezastrele însoțite de perturbări ale infrastructurii critice) în interiorul și în afara Uniunii sunt organizate de ERCC, centrul operațional unic al Comisiei care gestionează răspunsurile la situații de criză 24 de ore din 24, 7 zile pe săptămână. În astfel de cazuri, ERCC poate furniza alerte timpurii, notificări, analize și sprijin pentru schimbul de informații și, în cazul activării UCPM de către un stat membru, poate trimite în zonele afectate asistență operațională și experți. În plus, ERCC poate facilita coordonarea sectorială și transsectorială atât la nivelul Uniunii, cât și între Uniune și autoritățile naționale relevante, inclusiv cele responsabile cu protecția civilă și reziliența infrastructurii critice.

---

[10] Documentul de lucru comun al serviciilor Comisiei - Protocolul operațional al UE pentru combaterea amenințărilor hibride, SWD(2023) 116 final.

[11] Amenințările hibride pot fi caracterizate ca fiind o combinație de activități coercitive și subversive, metode convenționale și neconvenționale, care pot fi utilizate în mod coordonat de actori statali sau nestatali pentru a atinge obiective specifice, rămânând, în același timp, sub limita pragului de stare de război declarată oficial, în conformitate cu Protocolul UE pentru combaterea amenințărilor hibride.

d) Alte mecanisme și instrumente sectoriale sau transsectoriale

Planul de acțiune pentru infrastructura critică nu se suprapune cu alte instrumente sau mecanisme de coordonare sectoriale sau transsectoriale de gestionare a crizelor. În cazul în care în sectorul afectat există deja astfel de instrumente sau mecanisme, Planul de acțiune pentru infrastructura critică, în limitele domeniului său de aplicare, poate fi utilizat ca instrument complementar instrumentelor sau mecanismelor sectoriale sau transsectoriale, însă nu le înlocuiește. Ar trebui asigurată coordonarea necesară între diferiții actori, astfel încât să se evite o suprapunere de acest tip. Acest lucru ar putea fi realizat, de exemplu, în cadrul ARGUS – procesul de coordonare internă în caz de criză al Comisiei –, sprijinit de ERCC, și/sau al reuniunilor de coordonare ale IPCR.

PARTEA II: SCHIMBUL DE INFORMAȚII ȘI RĂSPUNSUL COORDONAT

Acțiunile descrise mai jos constau în modalități de cooperare, și anume schimbul de informații, comunicarea coordonată și răspunsul. Această structură corespunde modalităților din cadrul mecanismului IPCR de coordonare a crizelor al Consiliului și ia în considerare, în sens mai larg, utilizarea potențială a mecanismelor de coordonare a crizelor deja existente la nivelul UE. Această structură arată cum ar putea fi integrate modalitățile de cooperare respective, dacă sunt utilizate. Majoritatea acestor acțiuni pot fi însă întreprinse în mod autonom: ele nu depind de utilizarea acestui mecanism, ci îl completează. Acțiunile sunt prezentate în ordine cronologică, ținând seama totodată de faptul că, în cazul unei crize de mare amploare care constituie un incident semnificativ la nivelul infrastructurii critice, mai multe acțiuni pot fi întreprinse simultan și continuu.

1. SCHIMBUL DE INFORMAȚII

(a) La nivel operațional

Statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice aplică propriile măsuri de contingență, asigură coordonarea cu mecanismele naționale relevante de gestionare a crizelor, precum și, după caz, implicarea tuturor actorilor naționali, regionali și locali relevanți.

După caz, în ceea ce privește asistența în materie de protecție civilă, coordonarea dintre statele membre și cu Comisia este asigurată prin intermediul ERCC în cadrul UCPM.

i) Schimbul de informații și notificarea transmisă de autoritățile naționale competente

Pe lângă obligațiile în materie de notificare și de informare prevăzute la articolul 15 din Directiva (UE) 2022/2557, autoritățile naționale competente responsabile de infrastructura critică din statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice partajează cu președinția prin rotație a Consiliului și cu Comisia, prin intermediul punctelor lor unice de contact și fără întârzieri nejustificate, informațiile relevante primite de la operatorul (operatorii) de infrastructură critică, de la entitățile critice sau din alte surse, precum și informațiile privind mecanismele de gestionare a crizelor care au fost activate. Pentru Comisie, ERCC asigură contactul operațional și capacitatea operațională 24 de ore din 24, 7 zile pe săptămână, și coordonează, monitorizează și sprijină în timp real răspunsul la situații de urgență la nivelul Uniunii; în același timp, pentru statele membre și Comisie, aceste servește drept centru operațional pentru răspunsul în situații de criză, promovând o abordare transsectorială a gestionării dezastrelor.

Un astfel de schimb de informații se referă la natura incidentului semnificativ la nivelul infrastructurii critice, la cauza acestuia, la impactul observat sau estimat al perturbării asupra infrastructurii critice și asupra furnizării serviciilor esențiale, la consecințele incidentului la nivel transsectorial și transfrontalier și la măsurile de atenuare, fie deja luate, fie preconizate, la nivel național sau împreună cu alte state membre relevante și cu Comisia, prin intermediul acordurilor existente, de exemplu acordurile privind schimbul de informații în temeiul articolelor 9 și 15 din Directiva (UE) 2022/2557. Această notificare se transmite fără a deturna resursele infrastructurii critice sau, în unele cazuri, ale entității critice sau ale statului membru de la activitățile legate de gestionarea incidentelor, care trebuie să aibă prioritate.

Pentru a asigura adoptarea de măsuri subsecvente, ERCC sau serviciile Comisiei care au primit notificarea și sunt responsabile de sectorul (sectoarele) în care s-a produs incidentul semnificativ la nivelul infrastructurii critice informează punctul de contact din cadrul Direcției Generale Migrație și Afaceri Interne și Secretariatul General al Comisiei. Între timp, dacă nu s-a început deja monitorizarea, ERCC începe să monitorizeze evenimentele, în special în cazul activării UCPM de către unul sau mai multe dintre statele membre afectate.

În cazul în care informațiile ar putea fi relevante pentru abordarea unei dimensiuni de securitate cibernetică sau ar putea fi legate de un incident de securitate cibernetică, Comisia partajează informațiile relevante cu EU-CyCLONe.

Autoritățile naționale competente în temeiul Directivei (UE) 2022/2557 trebuie să coopereze și să facă schimb de informații cu autoritățile competente în temeiul Directivei (UE) 2022/2555, fără întârzieri nejustificate, în ceea ce privește incidentele cibernetice și incidentele care afectează entitățile critice, inclusiv privind măsurile de securitate cibernetică și măsurile fizice luate de entitățile critice.

Pentru domeniul maritim, autoritățile naționale competente iau în considerare posibilitatea de a utiliza mediul comun pentru schimbul de informații („CISE”) pentru a face schimb de informații fără întârzieri nejustificate.

ii) Organizarea reuniunilor de experți

Comisia convoacă cât mai curând posibil Grupul privind reziliența entităților critice pentru a facilita schimburile de informații relevante între autoritățile naționale competente responsabile de infrastructura critică și instituțiile, organele, oficiile și agențiile relevante ale Uniunii cu privire la incident (natura, cauza, impactul și consecințele transsectoriale și transfrontaliere) și cu privire la acțiunile de răspuns, inclusiv măsurile de atenuare și sprijinul tehnic pentru statele membre afectate. În funcție de centrul de greutate al incidentului, serviciile relevante ale Comisiei vor fi strâns asociate reuniunii Grupului privind reziliența entităților critice, în vederea schimbului de informații colectate prin intermediul instrumentelor sectoriale existente. În cazul unor incidente care prezintă o combinație de aspecte de securitate cibernetică și de aspecte fizice fără legătură cu securitatea cibernetică, serviciile relevante ale Comisiei, CERT-UE și SEAE, după caz, informează și se consultă cât mai curând posibil cu Grupul operativ în materie de crize cibernetice, precum și cu președinții Grupului de cooperare, astfel cum este menționat la articolul 14 din Directiva (UE) 2022/2555, și, după caz, cu UE-CyCLONe, cu privire la necesitatea unor activități de coordonare. De comun acord cu președinții respectivi, Comisia (Direcția Generală Migrație și Afaceri Interne și Direcția Generală Rețele de Comunicare, Conținut și Tehnologie) poate propune o reuniune comună a Grupului privind reziliența entităților critice și a Grupului de cooperare, în vederea unei conștientizări comune a situației și a coordonării răspunsurilor respective.

În cazul unui incident transsectorial semnificativ la nivelul infrastructurii critice care necesită sau este probabil să necesite gestionarea consecințelor la nivelul Uniunii, Comisia poate

convoca reuniuni de coordonare transsectoriale care să implice toate părțile interesate relevante.

În cazul în care un incident semnificativ la nivelul infrastructurii critice afectează și o țară terță, Comisia consultă autoritățile competente din țara terță afectată și le poate invita la o reuniune a Grupului privind reziliența entităților critice.

iii) Sprijin din partea Comisiei și a agențiilor Uniunii

După caz și acționând în conformitate cu mandatul său, Europol prezintă un raport privind situația incidentelor la nivelul Uniunii. După caz și acționând în conformitate cu mandatele lor respective, alte agenții ale Uniunii raportează informații relevante care contribuie la conștientizarea situației sau la răspunsul coordonat la incidentul semnificativ la nivelul infrastructurii critice către direcțiile generale de care depind, care, la rândul lor, raportează Comisiei (Direcția Generală Migrație și Afaceri Interne, în calitate de președinte al Grupului privind reziliența entităților critice).

Comisia poate contribui la conștientizarea situației utilizând activele Programului spațial al Uniunii[12], cum ar fi Copernicus, Galileo și EGNOS, după caz și în conformitate cu cadrul juridic aplicabil.

(b) La nivel strategic

i) Întocmirea de rapoarte privind conștientizarea situației

Pe baza informațiilor comunicate de autoritățile naționale competente în cadrul unei reuniuni a Grupului privind reziliența entităților critice sau al unor reuniuni comune cu serviciile, grupurile de experți sau rețelele relevante, Comisia pregătește un raport privind conștientizarea situației pe baza contribuțiilor autorităților naționale competente și a altor informații disponibile.

După caz, acest raport ține seama de rezultatele evaluării riscurilor, de evaluările și de scenariile din perspectiva securității cibernetice relevante la nivelul UE, inclusiv de cele efectuate de Comisie, de Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate și de Grupul de cooperare.

În cazul activării IPCR, acest raport poate contribui la raportul privind analiza și conștientizarea integrată a situației („ISAA”) întocmit de serviciile Comisiei și de SEAE.

După caz, SIAC prezintă o evaluare actualizată, bazată pe informații, a incidentului.

ii) Activarea mecanismelor Uniunii de coordonare a crizelor și utilizarea instrumentelor Uniunii

ERCC începe, după caz, să ofere sprijin pentru conștientizarea situației cu privire la incident, în special dacă evenimentul duce la activarea UCPM[13]. În plus, statele membre afectate pot solicita imagini prin satelit de pe teritoriul lor prin intermediul serviciului Copernicus de gestionare a situațiilor de urgență.

Atunci când se consideră oportun să se facă schimb de informații între Comisie și SEAE și agențiile relevante ale Uniunii, direcția generală principală sau Direcția Generală Migrație și

[12] Regulamentul (UE) 2021/696 al Parlamentului European și al Consiliului din 28 aprilie 2021 de instituire a Programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial și de abrogare a Regulamentelor (UE) nr. 912/2010, (UE) nr. 1285/2013 și (UE) nr. 377/2014 și a Deciziei nr. 541/2014/UE (JO L 170, 12.5.2021, p. 69).

[13] Cum ar fi publicarea de produse de monitorizare a mass-mediei, mesaje de protecție civilă, note de informare analitice, hărți ECHO zilnice, sinteze ECHO zilnice și alte produse adaptate.

Afaceri Interne, în coordonare cu Secretariatul General, activează procesul de coordonare internă în caz de criză al Comisiei - ARGUS faza I prin deschiderea unui eveniment în instrumentul informatic Argus.

Președinția prin rotație a Consiliului Uniunii poate activa mecanismul IPCR în modul „schimb de informații", ceea ce implică elaborarea de rapoarte ISAA de către Comisie și SEAE, cu contribuții din partea autorităților naționale competente și din alte surse, după caz. Chiar și fără activarea IPCR, în anumite condiții, președinția prin rotație a Consiliului sau Comisia pot iniția o pagină de monitorizare pe platforma web a IPCR.

Alte mecanisme și instrumente (sectoriale) ale Uniunii de gestionare a crizelor pot fi activate în conformitate cu procedurile respective, după caz. Comisia va asigura coordonarea dintre aceste mecanisme și instrumente.

În cazul în care incidentul fizic coincide sau pare să fie legat de un incident de securitate cibernetică de mare amploare, astfel cum este definit la articolul 6 alineatul (7) din Directiva (UE) 2022/2555, președinția prin rotație a Consiliului poate utiliza Planul de acțiune în materie de securitate cibernetică pentru a stabili o coordonare adecvată la nivel operațional, care implică, printre altele, EU-CyCLONe și Grupul privind reziliența entităților critice.

iii) Coordonarea comunicării publice

Statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice își coordonează, în măsura posibilului, comunicarea publică cu privire la criză, respectând în același timp competențele naționale în această privință. După caz, poate fi implicată rețeaua de comunicare în situații de criză a IPCR.

Pe baza conștientizării comune a situației, Grupul privind reziliența entităților critice și statele membre afectate sprijină formularea materialelor de comunicare publică convenite, după caz.

Europol și alte agenții relevante ale Uniunii își coordonează activitățile de comunicare publică cu serviciul purtătorului de cuvânt al Comisiei, pe baza conștientizării comune a situației.

În cazul în care incidentul semnificativ la nivelul infrastructurii critice implică o dimensiune externă, hibridă sau de politică de securitate și apărare comună, comunicarea publică este coordonată cu SEAE și cu serviciul purtătorului de cuvânt al Comisiei, în conformitate cu Protocolul UE pentru combaterea amenințărilor hibride[14].

2. RĂSPUNSUL (CARE IMPLICĂ ACȚIUNILE CONTINUE DESCRISE LA SECȚIUNEA SCHIMBUL DE INFORMAȚII ȘI ACȚIUNILE SUPLIMENTARE LA NIVEL STRATEGIC/POLITIC)

(a) La nivel strategic

i) Întocmirea continuă de rapoarte situaționale

Grupul de lucru pentru protecție civilă – Reziliența entităților critice (PROCIV-CER) al Consiliului este informat cu privire la întocmirea raportului politic/strategic situațional (de exemplu, ISAA în cazul activării IPCR sau raportul privind conștientizarea comună a situației pregătit de Comisie) și pregătește întrunirea Coreper, dacă acesta din urmă nu a fost încă convocat, sau reuniunea Comitetului politic și de securitate, după caz.

[14] Documentul de lucru comun al serviciilor Comisiei - Protocolul operațional al UE pentru combaterea amenințărilor hibride, SWD(2023) 116 final.

SIAC își intensifică interacțiunea cu serviciile de informații ale statelor membre, agregă informațiile din toate sursele și pregătește o analiză și o evaluare a incidentului, precum și actualizări periodice, dacă acest lucru este necesar.

ii) Activarea integrală a mecanismelor Uniunii de coordonare a crizelor și utilizarea instrumentelor Uniunii

În cazul în care președintele Comisiei activează procesul de coordonare internă în caz de criză al Comisiei - ARGUS faza II, reuniunile Comitetului de coordonare a crizelor care implică serviciile și agențiile relevante ale Comisiei și SEAE, după caz, sunt convocate într-un termen scurt pentru a se coordona în ceea ce privește toate aspectele incidentului semnificativ la nivelul infrastructurii critice.

În cazul în care președinția Consiliului activează IPCR în modul integral:

- președinția prin rotație a Consiliului solicită organizarea promptă a unei mese rotunde informale, care să reunească actorii relevanți de la nivel național, european și internațional, în cadrul căreia reprezentantul Comisiei care acționează în calitate de președinte al Grupului privind reziliența entităților critice (Direcția Generală Migrație și Afaceri Interne) poate prezenta informații privind reuniunea (reuniunile) grupului convocat(e) anterior, completate de alte servicii ale Comisiei și de SEAE, după caz;

- în cadrul acestei reuniuni, SIAC și agențiile relevante ale Uniunii pot fi invitate să prezinte o actualizare a situației cu privire la incidentul semnificativ la nivelul infrastructurii critice.

Serviciul principal responsabil de ISAA (serviciul principal din cadrul Comisiei sau SEAE) pregătește raportul ISAA, utilizând contribuții din partea serviciilor relevante ale Comisiei, a oficiilor, organelor și agențiilor relevante ale Uniunii și a autorităților naționale competente. Statele membre sunt invitate să contribuie, prin intermediul platformei web IPCR, la întocmirea rapoartelor ISAA.

În cazul unui incident semnificativ la nivelul infrastructurii critice cu relevanță pentru securitatea internațională, serviciile Comisiei și SEAE pot convoca un dialog structurat UE-NATO privind reziliența pentru a sprijini conștientizarea comună a situației și schimbul de informații privind măsurile luate de Uniune și, respectiv, de NATO.

iii) Comunicare publică

Consiliul pregătește mesaje comune de comunicare publică. Rețeaua informală a persoanelor responsabile cu comunicarea în situații de criză, instituită prin IPCR, poate sprijini această activitate. După caz, serviciul purtătorului de cuvânt al Comisiei pregătește, de asemenea, mesaje de comunicare publică.

În cazul în care incidentul semnificativ la nivelul infrastructurii critice implică o dimensiune externă, hibridă sau de politică de securitate și apărare comună, comunicarea publică este coordonată cu SEAE și cu serviciul purtătorului de cuvânt al Comisiei.

iv) Sprijin pentru statele membre și un răspuns eficace

Președinția prin rotație poate convoca o reuniune a PROCIV-CER pentru a sprijini activitățile din cadrul IPCR, dacă acesta este activat.

Statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice pot solicita sprijin tehnic din partea altor state membre sau a instituțiilor, organelor și agențiilor relevante ale Uniunii prin intermediul Grupului privind reziliența entităților critice, de exemplu, expertiză specifică pentru atenuarea impactului negativ al incidentului semnificativ la nivelul infrastructurii critice.

Statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice pot solicita, de asemenea, sprijin tehnic și/sau financiar din partea Comisiei sau a agențiilor relevante ale Uniunii. Comisia, în coordonare cu agențiile relevante ale Uniunii, își evaluează sprijinul posibil, activează, după caz, măsuri tehnice de atenuare la nivelul Uniunii, în conformitate cu procedurile lor respective, și coordonează capacitățile tehnice necesare pentru a opri sau a reduce impactul incidentului semnificativ la nivelul infrastructurii critice.

În contextul specific al UCPM, țările afectate au posibilitatea de a solicita asistență prin intermediul Sistemului comun de comunicare și informare în caz de urgență („CECIS"), după care ERCC ar putea coordona acordarea de asistență din partea statelor membre și a statelor participante la UCPM, precum și prin intermediul „rescEU"

În limitele mandatelor lor respective și la cerere, Europol și alte agenții relevante ale Uniunii sprijină statele membre afectate de un incident semnificativ la nivelul infrastructurii critice să investigheze incidentul.

(b) La nivel politic

Președinția Consiliului poate lua în considerare necesitatea de a convoca mese rotunde ale IPCR, reuniuni ale grupurilor de lucru ale Consiliului, Coreper, Consiliului de Miniștri și/sau reuniuni la nivel înalt pentru a face schimb de opinii privind originea posibilă și consecințele preconizate ale incidentului semnificativ la nivelul infrastructurii critice asupra statelor membre și asupra Uniunii, pentru a conveni asupra unor orientări comune, precum și pentru a adopta măsurile necesare menite să sprijine statele membre afectate de incidentul semnificativ la nivelul infrastructurii critice și pentru a atenua efectele acestuia.

Diagrama 1: Prezentare schematică a Planului de acțiune pentru infrastructura critică

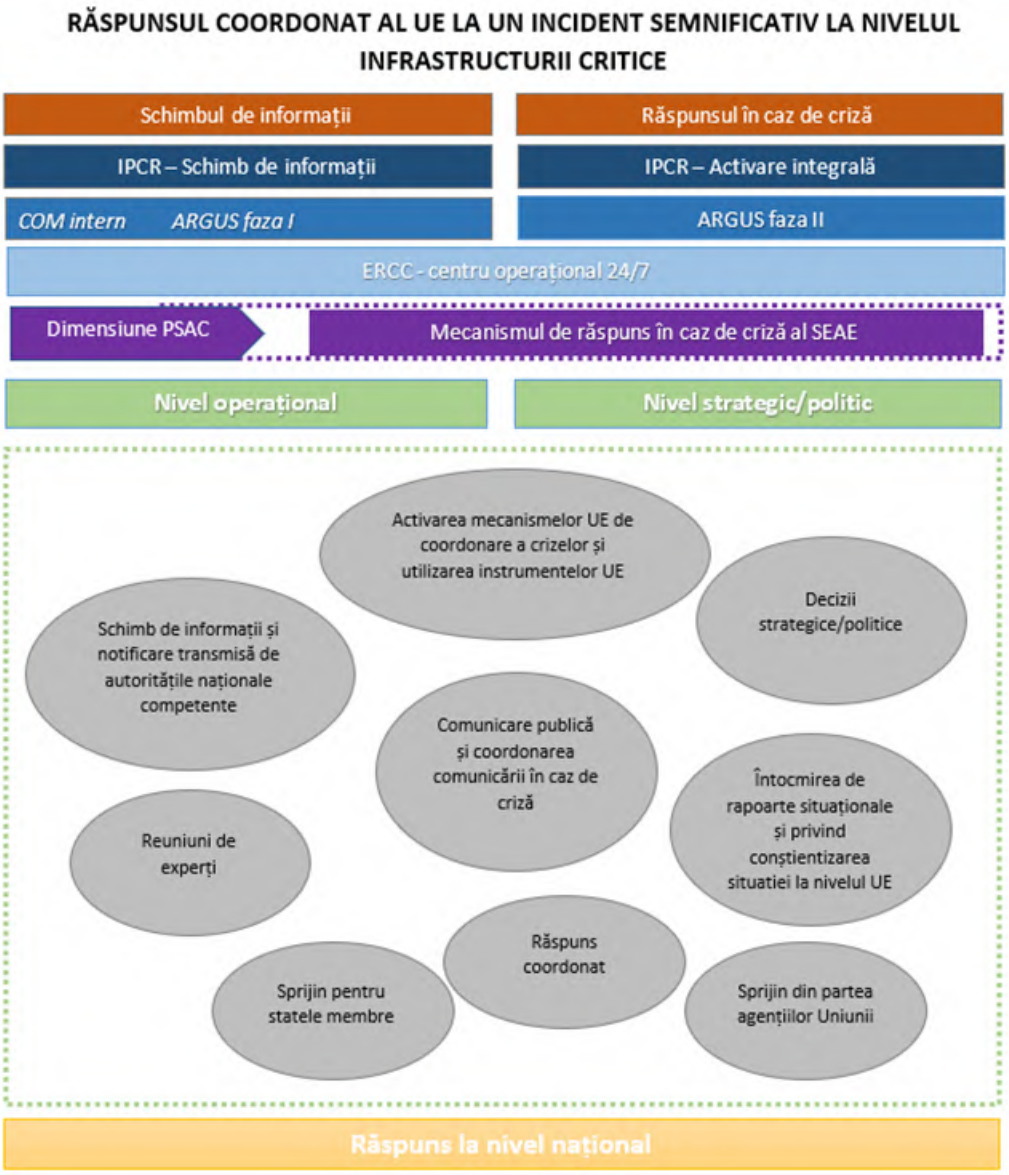

Diagrama 2: Luarea deciziilor în cadrul Planului de acțiune pentru infrastructura critică