Consiliul
Uniunii Europene

Bruxelles, 7 septembrie 2023
(OR. en)

12485/23

Dosar interinstituțional:
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**

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:	Propunere 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

2023/0318 (NLE)

Propunere 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

(Text cu relevanță pentru SEE)

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

În contextul geopolitic actual, caracterizat de o instabilitate crescândă, cauzată în special de războiul de agresiune al Rusiei împotriva Ucrainei și de complexitatea tot mai mare a amenințărilor la adresa securității, precum și de efectele schimbărilor climatice, cum ar fi intensificarea evenimentelor climatice neobișnuite sau deficitul de apă, Uniunea trebuie să rămână vigilentă și să se adapteze în mod constant. Cetățenii, întreprinderile și autoritățile din Uniune se bazează pe infrastructura critică[1], având în vedere serviciile esențiale pe care le furnizează entitățile care operează această infrastructură. Astfel de servicii sunt esențiale pentru menținerea funcțiilor societale vitale, a activităților economice, a sănătății și siguranței publice sau a mediului și trebuie furnizate în mod neobstrucționat pe piața internă. Așadar, având în vedere importanța acestor servicii esențiale pentru piața internă și, în consecință, necesitatea de îmbunătăți reziliența infrastructurii critice și, în sens mai larg, de a asigura reziliența entităților critice care furnizează aceste servicii, Uniunea trebuie să ia măsuri pentru a spori această reziliență și a atenua orice perturbări în furnizarea serviciilor esențiale respective. Astfel de perturbări pot avea consecințe grave pentru cetățenii Uniunii, pentru economiile noastre și pentru încrederea în sistemele noastre democratice și pot afecta buna funcționare a pieței interne, în special în contextul unor interdependențe tot mai mari între sectoare și la nivel transfrontalier.

Uniunea a luat deja o serie de măsuri pentru a îmbunătăți protecția infrastructurii critice, în special în ceea ce privește infrastructura transfrontalieră, precum și reziliența entităților critice, pentru a evita sau a atenua efectele perturbărilor serviciilor esențiale pe care acestea le furnizează pe piața internă.

Directiva 2008/114/CE privind identificarea și desemnarea infrastructurilor critice europene[2] („Directiva ICE”) a fost primul instrument juridic care a stabilit o procedură la nivelul UE pentru identificarea și desemnarea infrastructurilor critice europene și a definit o abordare comună la nivelul Uniunii pentru evaluarea necesității de a îmbunătăți protecția acestor infrastructuri împotriva amenințărilor provocate de om – atât intenționate, cât și accidentale –, precum și împotriva dezastrelor naturale. Directiva s-a concentrat însă doar pe sectoarele energiei și transporturilor și pe protecția infrastructurii critice și nu a prevăzut măsuri mai ample de consolidare a rezilienței entităților care operează această infrastructură.

Având în vedere că operațiunile de pe piața internă sunt din ce în ce mai interconectate și se desfășoară la nivel transfrontalier, s-a profilat nevoia de a acoperi mai mult de două sectoare și de a merge dincolo de măsurile de protecție a activelor individuale. Acesta este motivul pentru care, în 2022, au fost adoptate Directiva (UE) 2022/2557 privind reziliența entităților critice[3] („Directiva REC”) și Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun

---

[1] Infrastructură critică înseamnă un activ, o instalație, un echipament, o rețea ori un sistem sau o componentă a unui activ, a unei instalații, a unui echipament, a unei rețele ori a unui sistem, care este necesar(ă) pentru furnizarea unui serviciu esențial [articolul 2 alineatul (4) din Directiva (UE) 2022/2557 privind reziliența entităților critice].

[2] Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

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

ridicat de securitate cibernetică în Uniune[4] („Directiva NIS 2”). Scopul urmărit este de a asigura un nivel cuprinzător de reziliență fizică și digitală a entităților critice. Directiva REC a intrat în vigoare la 16 ianuarie 2023 și vizează sprijinirea statelor membre în ceea ce privește consolidarea rezilienței globale a entităților critice, îmbunătățind în același timp coordonarea la nivelul Uniunii. Aceasta va înlocui Directiva ICE începând cu 18 octombrie 2024, dată până la care statele membre vor trebui să ia măsurile necesare pentru a se conforma Directivei REC. Directiva REC se aplică în 11 sectoare[5]. Aceasta deplasează accentul de la protecția infrastructurii critice la conceptul mai larg de reziliență a entităților critice care operează această infrastructură critică, acoperind perioadele dinaintea, din timpul și de după producerea unui incident. Directiva NIS 2 a intrat în vigoare tot la 16 ianuarie 2023 și modernizează cadrul juridic existent pentru a-l adapta la digitalizarea mai amplă și la evoluția situației amenințărilor la adresa securității cibernetice. Directiva NIS 2 extinde totodată domeniul de aplicare al normelor în materie de securitate cibernetică pentru a include noi sectoare și entități și îmbunătățește reziliența și capacitățile de răspuns la incidente ale entităților publice și private, ale autorităților competente și ale Uniunii, în ansamblu.

Directiva REC cuprinde dispoziții privind notificarea incidentelor de către entitatea critică către autoritatea națională competentă, notificarea altor state membre (potențial) afectate de către autoritatea națională competentă și notificarea Comisiei în cazul în care incidentul afectează șase sau mai multe state membre. Directiva REC prevede anumite obligații de notificare a incidentelor dacă incidentul are sau ar putea avea un efect semnificativ asupra entităților critice și asupra continuității furnizării de servicii esențiale pentru unul sau mai multe alte state membre sau pe teritoriul acestora[6].

După cum a demonstrat sabotajul gazoductelor Nord Stream din septembrie 2022, contextul de securitate în care funcționează infrastructura critică s-a schimbat în mod semnificativ și sunt necesare acțiuni suplimentare urgente la nivelul Uniunii pentru a spori reziliența infrastructurii critice, nu numai în ceea ce privește pregătirea, ci și în ceea ce privește furnizarea unui răspuns coordonat.

În acest context, la 8 decembrie 2022, în urma unei propuneri a Comisiei, a fost adoptată Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice[7] („Recomandarea privind reziliența infrastructurilor critice”). Recomandarea respectivă subliniază, printre altele, necesitatea de a asigura, la nivelul Uniunii, un răspuns coordonat și eficace la riscurile actuale și viitoare legate de furnizarea serviciilor esențiale. Mai precis, Consiliul a invitat Comisia să elaboreze un „plan de acțiune privind un răspuns coordonat la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă”. Recomandarea menționează că planul de acțiune ar trebui să fie coerent cu Protocolul UE pentru combaterea amenințărilor hibride[8], să țină seama de Recomandarea 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele

[4] 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).

[5] Energie, transporturi, servicii bancare, infrastructura pieței financiare, infrastructură digitală, administrație publică, spațiu, sănătate, apă potabilă, ape reziduale, producție, prelucrare și distribuție de alimente.

[6] În conformitate cu articolul 15 alineatele (1) și (3) din Directiva REC.

[7] Recomandarea Consiliului din 8 decembrie 2022 privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice 2023/C 20/01 (JO C 20, 20.1.2023, p. 1).

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

de securitate cibernetică de mare amploare[9] („Planul de acțiune în materie de securitate cibernetică”) și să respecte mecanismul integrat pentru un răspuns politic la crize[10] („IPCR”).

În acest context, prezenta propunere vizând o recomandare suplimentară a Consiliului conține un astfel de plan. Propunerea urmărește să completeze cadrul juridic actual prin descrierea răspunsului coordonat la nivelul Uniunii în cazul perturbărilor infrastructurii critice cu o relevanță transfrontalieră semnificativă, utilizând în același timp mecanismele existente la nivelul Uniunii. În mod concret, propunerea descrie domeniul de aplicare și obiectivele planului de acțiune, actorii, procesele și instrumentele existente care ar putea fi utilizate pentru a răspunde în mod coordonat la nivelul Uniunii la un incident care perturbă infrastructura critică și are un efect transfrontalier semnificativ, și descrie modurile de cooperare dintre statele membre și instituțiile, organele, oficiile și agențiile Uniunii în astfel de situații.

- **Coerența cu dispozițiile existente în domeniul de politică vizat**

Prezenta propunere de recomandare a Consiliului este în concordanță cu cadrul juridic actual privind protecția infrastructurii critice și reziliența entităților critice – Directiva ICE și, respectiv, Directiva REC, precum și Recomandarea privind reziliența infrastructurilor critice – și îl completează, întrucât urmărește să asigure, în mod complementar, coordonarea dintre statele membre și dintre acestea și instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește răspunsul la incidentele care cauzează perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă și ale furnizării de servicii esențiale. Propunerea utilizează structurile și mecanismele existente la nivelul Uniunii, inclusiv cele instituite prin Directiva REC, și anume cooperarea dintre autoritățile competente și Grupul privind reziliența entităților critice, care este un grup instituit prin Directiva REC pentru a sprijini Comisia și a facilita cooperarea dintre statele membre, precum și schimbul de informații cu privire la aspecte legate de Directiva REC.

Prezenta propunere de recomandare a Consiliului este, de asemenea, conformă cu cadrul Uniunii privind securitatea cibernetică, astfel cum este prevăzut în Directiva NIS 2, și îl completează.

Prezenta propunere urmărește să prezinte, în domeniul rezilienței entităților critice și al protecției infrastructurii critice, un Plan de acțiune pentru infrastructura critică similar cu Planul de acțiune în materie de securitate cibernetică.

Punctul 4 litera (b) din partea I a anexei explică, de asemenea, legăturile cu Planul de acțiune în materie de securitate cibernetică, care se aplică incidentelor de securitate cibernetică ce afectează statul membru vizat într-o măsură prea mare pentru ca acesta să gestioneze situația pe cont propriu sau incidentelor care afectează două sau mai multe state membre ori instituții ale Uniunii, consecințele tehnice sau politice fiind atât de ample și de importante încât trebuie să se asigure prompt coordonarea politicilor și a răspunsului la nivelul politic al Uniunii. Directiva NIS 2 definește „incidentul” drept „un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora” („incident de securitate cibernetică”).

[9] 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).

[10] Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28).

Autoritățile competente desemnate în temeiul Directivei CER și al Directivei NIS 2 au obligația de a coopera și de a face schimb de informații cu privire la incidentele de securitate cibernetică și la incidentele care afectează entitățile critice, inclusiv în ceea ce privește măsurile relevante adoptate. Într-o situație în care un incident semnificativ la nivelul infrastructurii critice și un incident de securitate cibernetică de mare amploare afectează aceeași entitate, ar trebui să existe o coordonare între actorii relevanți cu privire la posibilele răspunsuri.

Propunerea este coerentă cu Protocolul UE pentru combaterea amenințărilor hibride, care se aplică în cazul incidentelor hibride. Punctul 4 litera (a) din partea I a anexei explică legăturile cu protocolul UE, inclusiv ce instrument se aplică în cazul unui incident semnificativ la nivelul infrastructurii critice cu o dimensiune hibridă.

Propunerea este, de asemenea, coerentă cu alte mecanisme existente de gestionare a crizelor la nivelul Uniunii, cum ar fi mecanismele IPCR ale Consiliului, ARGUS[11] – procesul de coordonare internă în caz de criză al Comisiei și mecanismul de protecție civilă al Uniunii[12] („UCPM") sprijinit de Centrul său de coordonare a răspunsului la situații de urgență („ERCC"), și Mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă.

Propunerea este, de asemenea, coerentă cu alte acte legislative sectoriale relevante și, în special, cu măsurile specifice din cadrul acestora care reglementează anumite aspecte ale răspunsului la perturbări furnizat de entitățile care își desfășoară activitatea în sectoarele în cauză.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Propunerea se întemeiază pe articolul 114 din Tratatul privind funcționarea Uniunii Europene („TFUE"), care prevede apropierea legislațiilor în vederea îmbunătățirii pieței interne, coroborat cu articolul 292 din TFUE, care stabilește normele relevante privind adoptarea de recomandări.

Alegerea articolului 114 din TFUE ca temei juridic material este justificată de faptul că propunerea de recomandare a Consiliului vizează asigurarea unui răspuns coordonat în cazul unor perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă. Astfel de perturbări afectează mai multe state membre și riscă să perturbe funcționarea pieței interne, având în vedere interconexiunile tot mai mari dintre infrastructură și sectoare într-o economie a Uniunii din ce în ce mai interdependentă. Îmbunătățirea răspunsului la perturbări va contribui, la rândul său, la evitarea perturbării funcționării pieței interne, întrucât infrastructura critică și serviciile esențiale furnizate sunt esențiale pentru menținerea funcțiilor societale vitale, a activităților economice, a sănătății și siguranței publice sau a mediului.

[11] Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Dispozițiile Comisiei privind sistemul general de alertă rapidă „ARGUS", COM(2005) 662 final.

[12] Regulamentul (UE) 2021/836 al Parlamentului European și al Consiliului din 20 mai 2021 de modificare a Deciziei nr. 1313/2013/UE privind un mecanism de protecție civilă al Uniunii (JO L 185, 26.5.2021, p. 1).

Propunerea ar urma să completeze Directiva ICE și Directiva REC, care se întemeiază tot pe articolul 114 din TFUE. La fel ca prezenta propunere de recomandare, Recomandarea privind reziliența infrastructurilor critice are ca temei juridic tot articolele 114 și 292 din TFUE.

- **Subsidiaritatea (în cazul competențelor neexclusive)**

Deși răspunsul la perturbările infrastructurii critice sau ale serviciilor furnizate de entitățile critice care operează această infrastructură critică este în primul rând responsabilitatea statelor membre, Uniunea are un rol important în cazul unei perturbări a infrastructurii critice cu o relevanță transfrontalieră semnificativă, întrucât o astfel de perturbare poate afecta mai multe sau chiar toate sectoarele de activitate economică din cadrul pieței unice, precum și securitatea și relațiile internaționale ale Uniunii. Cu scopul de a asigura funcționarea pieței interne, coordonarea la nivelul Uniunii în cazul unor perturbări ale infrastructurii critice cu efecte transfrontaliere semnificative este nu numai adecvată, ci și necesară, întrucât un astfel de răspuns coordonat la nivelul Uniunii va sprijini răspunsul statelor membre la perturbare prin conștientizarea comună a situației, prin comunicarea publică coordonată și prin atenuarea consecințelor perturbării pe piața internă.

- **Proporționalitatea**

Prezenta propunere este conformă cu principiul proporționalității, astfel cum este prevăzut la articolul 5 alineatul (4) din Tratatul privind Uniunea Europeană.

Nici conținutul, nici forma prezentei propuneri de recomandare a Consiliului nu depășesc ceea ce este necesar pentru atingerea obiectivelor sale. Acțiunile propuse sunt proporționale cu obiectivele urmărite, care vizează asigurarea unui răspuns coordonat la nivelul Uniunii în cazul perturbării infrastructurii critice sau a serviciilor furnizate de entitățile critice care operează această infrastructură critică și care au o relevanță transfrontalieră semnificativă. Răspunsul coordonat propus este proporțional cu prerogativele și obligațiile statelor membre prevăzute în legislația națională. Incidentele care perturbă infrastructura critică sau furnizarea de servicii esențiale de către entitățile critice se situează adesea sub pragul unui incident semnificativ la nivelul infrastructurii critice și pot fi abordate în mod eficace la nivel național. Prin urmare, utilizarea mecanismului prevăzut în prezenta propunere se limitează la perturbările majore care au o relevanță transfrontalieră semnificativă și care afectează mai multe state membre.

- **Alegerea instrumentului**

Pentru a atinge obiectivele menționate mai sus, TFUE prevede adoptarea de către Consiliu de recomandări, în special la articolul 292 din tratat, pe baza unei propuneri din partea Comisiei. În conformitate cu articolul 288 din TFUE, recomandările nu au caracter obligatoriu. O recomandare a Consiliului este un instrument adecvat în acest caz, întrucât semnalează angajamentul statelor membre față de măsurile incluse în aceasta și oferă o bază solidă pentru cooperarea aferentă unui răspuns coordonat în cazul unor perturbări semnificative ale infrastructurii critice. În acest mod, recomandarea propusă ar urma să completeze cadrul juridic obligatoriu (în special Directiva REC), precum și Recomandarea privind reziliența infrastructurilor critice, adoptată anterior, care solicită adoptarea unor astfel de măsuri complementare, cu respectarea deplină, în același timp, a responsabilităților statelor membre în domeniul vizat.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- **Consultările cu părțile interesate**

Pentru elaborarea prezentei propuneri au fost consultate statele membre, instituțiile și agențiile Uniunii. De asemenea, au fost luate în considerare punctele de vedere ale experților din statele membre, exprimate atât în cadrul atelierului din 24 aprilie 2023, cât și trimise în scris după atelierul respectiv.

S-a înregistrat un consens general cu privire la utilitatea unei mai bune coordonări a răspunsului la nivelul Uniunii la perturbările infrastructurii critice cu o relevanță transfrontalieră semnificativă în contextul actual al amenințărilor, care să respecte, în același timp, competența statelor membre în acest domeniu și confidențialitatea informațiilor sensibile. De asemenea, a existat un consens privind necesitatea de a se evita duplicarea instrumentelor și de a se utiliza în mod adecvat mecanismele existente la nivelul Uniunii în materie de coordonare, schimb de informații și răspuns.

În timp ce anumite state membre au avut o opinie pozitivă asupra domeniului de aplicare mai larg al Planului de acțiune pentru infrastructura critică, altele au considerat că pragul de șase sau mai multe state membre prevăzut în Directiva REC în ceea ce privește identificarea entităților critice de importanță europeană deosebită este suficient și că nu este necesară introducerea unui al doilea tip de incident. Câteva state membre au punctat importanța implicării, după caz, a operatorilor de infrastructuri critice care furnizează servicii esențiale, având în vedere expertiza lor și importanța luării în considerare a dimensiunii cibernetice.

- **Explicarea detaliată a dispozițiilor specifice ale propunerii**

Propunerea de recomandare a Consiliului este alcătuită dintr-o parte principală și o anexă.

Partea principală cuprinde 11 puncte, după cum se menționează mai jos.

Punctul (1) descrie necesitatea unei cooperări consolidate în ceea ce privește răspunsul la incidentele semnificative la nivelul infrastructurii critice în conformitate cu Planul de acțiune pentru infrastructura critică inclus în prezenta propunere de recomandare, inclusiv cu părțile relevante din anexa la acesta.

Punctul (2) specifică domeniul de aplicare al Planului de acțiune pentru infrastructura critică, care se referă la două tipuri de situații de incidente perturbatoare care ar declanșa aplicarea Planului de acțiune pentru infrastructura critică: incidentul are un efect perturbator semnificativ asupra furnizării de servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora; sau incidentul are un efect perturbator semnificativ pe teritoriul a două sau mai multe state membre și există un acord între actorii relevanți menționați în plan cu privire la necesitatea unei coordonări la nivelul Uniunii din cauza impactului semnificativ al incidentului.

Punctul (3) se referă la identificarea actorilor relevanți care urmează să fie implicați în Planul de acțiune pentru infrastructura critică și la nivelurile la care va funcționa planul (nivel operațional, strategic/politic). Anexa la recomandare furnizează mai multe detalii în acest sens.

Punctul (4) cuprinde recomandarea de a aplica Planul de acțiune pentru infrastructura critică în mod coerent cu alte instrumente relevante, astfel cum se precizează în anexă.

Punctul (5) cuprinde recomandarea ca statele membre să răspundă în mod eficace la nivel național în cazul perturbărilor semnificative ale infrastructurii critice.

Punctul (6) cuprinde recomandarea ca actorii relevanți să stabilească sau să desemneze puncte de contact care să sprijine utilizarea Planului de acțiune pentru infrastructura critică. În măsura posibilului, aceste puncte de contact ar trebui să fie aceleași cu punctele unice de contact desemnate în temeiul Directivei CER.

Punctul (7) se referă la fluxul de informații în cazul unui incident semnificativ la nivelul infrastructurii critice.

Punctul (8) detaliază modul în care ar trebui să se desfășoare schimbul de informații.

Punctul (9) cuprinde recomandarea privind testarea prin exerciții a funcționării Planului de acțiune pentru infrastructura critică.

Punctul (10) cuprinde recomandarea ca lecțiile învățate să fie discutate în cadrul Grupului privind reziliența entităților critice, care ar trebui să întocmească un raport incluzând recomandări. Raportul ar trebui adoptat de Comisie.

Punctul (11) cuprinde recomandarea ca statele membre să discute raportul în cadrul Consiliului.

Anexa descrie obiectivele, principiile, principalii actori, interacțiunea cu mecanismele existente de răspuns la situații de criză și funcționarea Planului de acțiune pentru infrastructura critică, cu cele două moduri de cooperare prevăzute de acesta: schimbul de informații și răspunsul.

2023/0318 (NLE)

Propunere 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

(Text cu relevanță pentru SEE)

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolele 114 și 292,

având în vedere propunerea Comisiei Europene,

întrucât:

(1) Buna funcționare a pieței interne și a societății în ansamblu se bazează în mare parte pe existența unor infrastructuri critice reziliente și a unor entități critice reziliente care furnizează servicii esențiale pentru menținerea funcțiilor societale vitale, a activităților economice, a sănătății și siguranței publice sau a mediului.

(2) În contextul situației actuale, aflată în schimbare, în materie de riscuri și având în vedere interdependențele tot mai mari dintre infrastructură și sectoare și, în sens mai larg, interconexiunile transsectoriale și transfrontaliere, este necesar să se abordeze și să se consolideze, într-un mod cuprinzător și coordonat, protecția infrastructurii critice, precum și reziliența entităților critice care operează această infrastructură.

(3) Un incident care perturbă infrastructura critică și, prin urmare, întrerupe sau împiedică serios furnizarea serviciilor esențiale, poate avea efecte transfrontaliere semnificative și poate avea un impact negativ asupra pieței interne. Cu scopul de a asigura o abordare specifică, proporțională și eficace, ar trebui luate măsuri pentru a aborda în special incidentele semnificative la nivelul infrastructurii critice, astfel cum se specifică în prezenta recomandare, care să vizeze, de exemplu, situațiile în care perturbarea cauzată de incident este de lungă durată sau în care aceasta poate avea efecte în cascadă considerabile în același sector sau în alte sectoare ori state membre.

(4) Un răspuns coordonat la incidentele semnificative la nivelul infrastructurii critice este esențial pentru a evita perturbări majore pe piața internă și pentru a asigura restabilirea furnizării acestor servicii esențiale cât mai curând posibil, întrucât astfel de incidente pot avea consecințe grave asupra economiei și cetățenilor Uniunii. Un răspuns prompt și eficace la nivelul Uniunii la astfel de incidente necesită o cooperare rapidă și eficace între toți actorii relevanți, precum și acțiuni coordonate sprijinite la nivelul Uniunii. Prin urmare, un astfel de răspuns se bazează pe existența unor proceduri și mecanisme de cooperare care să fie instituite în prealabil și, în măsura posibilului, supuse unor simulări adecvate, cu definirea clară a rolurilor și responsabilităților actorilor-cheie la nivel național și la nivelul Uniunii.

(5) Deși responsabilitatea principală pentru răspunsul la incidentele semnificative la nivelul infrastructurii critice revine statelor membre și entităților care operează infrastructura critică și furnizează servicii esențiale, o coordonare sporită la nivelul Uniunii este oportună în cazul unor perturbări cu relevanță transfrontalieră semnificativă. Un răspuns prompt și eficace depinde nu numai de implementarea mecanismelor naționale de către statele membre, ci și de acțiuni coordonate sprijinite la nivelul Uniunii, inclusiv de existența unei cooperări relevante, rapide și eficace.

(6) Protecția infrastructurilor critice europene este reglementată în prezent de Directiva 2008/114/CE a Consiliului[1], care vizează doar două sectoare, respectiv transporturile și energia. Directiva menționată stabilește o procedură pentru identificarea și desemnarea infrastructurii critice europene și o abordare comună privind evaluarea necesității de a îmbunătăți protecția acestei infrastructuri. Aceasta reprezintă pilonul central al Programului european privind protecția infrastructurilor critice[2] („PEPIC”), adoptat de Comisie în 2006, care a stabilit un cadru la nivel european privind toate pericolele pentru protecția infrastructurilor critice.

(7) Pentru a acoperi și alte aspecte în afara protecției infrastructurii critice și pentru a asigura, în sens mai larg, reziliența entităților critice care operează astfel de infrastructuri și care furnizează servicii esențiale pe piața internă, Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului[3] va înlocui Directiva 2008/114/CE începând cu 18 octombrie 2024. Directiva (UE) 2022/2557 vizează 11 sectoare și prevede obligații pentru statele membre și entitățile critice de consolidare a rezilienței, cooperarea dintre statele membre și cu Comisia, sprijinirea de Comisie a autorităților naționale și a entităților critice și sprijinirea de către statele membre a entităților critice.

(8) În urma sabotajului gazoductelor Nord Stream, este necesar să se adopte, la nivelul Uniunii, măsuri de consolidare a rezilienței pentru infrastructura critică. Prin urmare, pe baza unei propuneri a Comisiei, Consiliul a adoptat Recomandarea privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice („Recomandarea 2023/C 20/01”)[4], care vizează îmbunătățirea gradului de pregătire, a răspunsului și a cooperării internaționale în acest domeniu. Recomandarea respectivă a subliniat în special necesitatea de a asigura, la nivelul Uniunii, un răspuns coordonat și eficace la riscurile legate de furnizarea serviciilor esențiale.

(9) Prin urmare, este necesară completarea cadrului juridic existent cu o recomandare suplimentară a Consiliului care să stabilească un Plan de acțiune privind un răspuns coordonat la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă („Planul de acțiune pentru infrastructura critică”), utilizând în același timp mecanismele care există deja la nivelul Uniunii.

(10) Prezenta recomandare ar trebui să fie aliniată la Recomandarea 2023/C 20/01, pentru a se asigura coerența și a se evita suprapunerile. Prin urmare, prezenta recomandare nu

---

[1] Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

[2] COM(2006) 786 final din 12 decembrie 2006 – Comunicarea Comisiei referitoare la Programul european privind protecția infrastructurilor critice.

[3] 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).

[4] Recomandarea Consiliului din 8 decembrie 2022 privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice 2023/C 20/01 (JO C 20, 20.1.2023, p. 1).

ar trebui să vizeze, ca atare, celelalte elemente ale ciclului de viață al gestionării crizelor, și anume prevenirea, pregătirea și redresarea.

(11) Prezenta recomandare ar trebui să completeze Directiva (UE) 2022/2557, în special în ceea ce privește răspunsul coordonat, și ar trebui să fie pusă în aplicare asigurând, în același timp, coerența cu directiva menționată și cu orice alte norme aplicabile din dreptul Uniunii. Prin urmare, prezenta recomandare ar trebui, de asemenea, să se bazeze și să utilizeze, în măsura posibilului, noțiunile, instrumentele și procesele prevăzute de directiva menționată, cum ar fi Grupul privind reziliența entităților critice, acționând în limitele sarcinilor sale, astfel cum sunt prevăzute în directiva menționată, și punctele de contact. În plus, noțiunea de „infrastructură critică", astfel cum este utilizată în prezenta recomandare, ar trebui înțeleasă în același mod ca la considerentul 7 din Recomandarea 2023/C 20/01, și anume ca incluzând infrastructura critică relevantă identificată de un stat membru la nivel național sau desemnată drept infrastructură critică europeană în temeiul Directivei 2008/114/CE, precum și entitățile critice care urmează să fie identificate în temeiul Directivei (UE) 2022/2557. Pentru a asigura coerența cu Directiva (UE) 2022/2557, noțiunile utilizate în prezenta recomandare ar trebui, prin urmare, să fie interpretate ca având același înțeles ca în directiva respectivă. De exemplu, conceptul de reziliență, astfel cum este definit la articolul 2 punctul 2 din directiva menționată, ar trebui înțeles ca referindu-se la capacitatea unei infrastructuri critice de a preveni apariția unor evenimente care perturbă în mod semnificativ sau au potențialul de a perturba în mod semnificativ furnizarea serviciilor esențiale pe piața internă, și anume serviciile care sunt esențiale pentru menținerea unor funcții societale și economice vitale, a siguranței și securității publice, a sănătății populației sau a mediului, de a se proteja în fața acestora, de a le răspunde, de a rezista, de a le atenua impactul, de a le absorbi, de a se adapta la acestea sau a-și reveni în urma lor.

(12) În plus, noțiunea de „efect perturbator semnificativ" ar trebui înțeleasă în lumina criteriilor prevăzute la articolul 7 alineatul (1) din Directiva (UE) 2022/2557, care se referă la: i) numărul de utilizatori care se bazează pe serviciul esențial furnizat de entitatea în cauză; ii) gradul de dependență al altor sectoare și subsectoare prevăzute în anexa la directiva menționată de serviciul esențial respectiv; iii) efectele pe care l-ar putea avea incidentele, ca intensitate și durată, asupra activităților economice și societale, a mediului, a siguranței și securității publice, sau a sănătății populației; iv) cota de piață a entității pe piața serviciului esențial sau a serviciilor esențiale respective; v) zona geografică ce ar putea fi afectată de un incident, inclusiv eventualele efecte transfrontaliere, ținând seama de vulnerabilitatea asociată cu gradul de izolare al anumitor tipuri de zone geografice, cum ar fi regiunile insulare, regiunile îndepărtate sau zonele montane; vi) importanța entității pentru menținerea unui nivel suficient al serviciului esențial, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului esențial respectiv.

(13) Din motive de eficiență și eficacitate, Planul de acțiune pentru infrastructura critică ar trebui să fie pe deplin coerent și interoperabil cu protocolul operațional revizuit al Uniunii pentru combaterea amenințărilor hibride[5] și să țină seama de Planul de acțiune existent privind răspunsul coordonat la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare instituit prin Recomandarea (UE) 2017/1584 a

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

Comisiei[6] („Planul de acțiune în materie de securitate cibernetică”) și de mandatul Rețelei europene a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe”) prevăzut în Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[7] și ar trebui să evite suprapunerea structurilor și a activităților. Planul de acțiune pentru infrastructura critică ar trebui, de asemenea, să respecte pe deplin mecanismul integrat al UE pentru un răspuns politic la crize[8] (IPCR) al Consiliului pentru a asigura coordonarea răspunsului.

(14) Prezenta recomandare se bazează pe mecanismele instituite de Uniune pentru gestionarea crizelor și este, în sens mai larg, coerentă și complementară cu mecanismul IPCR al Consiliului, cu ARGUS[9] – procesul de coordonare internă în caz de criză al Comisiei – și cu mecanismul de protecție civilă al Uniunii („UCPM”)[10], sprijinit de Centrul de coordonare a răspunsului la situații de urgență („ERCC”)[11], cu mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă („SEAE”), precum și cu Instrumentul pentru situații de urgență pe piața unică[12], toate acestea putând juca un rol în răspunsul la o perturbare majoră a operațiunilor infrastructurii critice.

(15) Pentru a răspunde unui incident semnificativ la nivelul infrastructurii critice, pot fi utilizate instrumentele sau mecanismele la nivelul Uniunii menționate mai sus, în conformitate cu normele și procedurile aplicabile, pe care prezenta recomandare ar trebui să le completeze, fără să le aducă atingere. De exemplu, mecanismul IPCR al Consiliului continuă să fie principalul instrument de coordonare a răspunsului la nivelul politic al Uniunii între statele membre. Coordonarea internă în interiorul Comisiei are loc în cadrul ARGUS, care este procesul de coordonare transsectorială în situații de criză. În cazul în care criza are o dimensiune externă sau de politică de securitate și apărare comună („PSAC”), poate fi utilizat mecanismul de răspuns în caz de criză al SEAE. În conformitate cu Decizia 1313/2013/UE privind un mecanism de protecție civilă al Uniunii („UCPM”), răspunsurile operaționale în cadrul UCPM la dezastre naturale și provocate de om reale sau iminente în interiorul și în afara Uniunii (inclusiv cele care afectează infrastructura critică) 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,

---

6 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).

7 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).

8 Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28).

9 Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor: Dispozițiile Comisiei privind sistemul general de alertă rapidă „ARGUS”, COM(2005) 662 final.

10 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).

11 Decizia nr. 1313/2013/UE privind un mecanism de protecție civilă al Uniunii (UCPM) a creat un cadru care ia în considerare toate pericolele și care stabilește mecanisme de prevenire, pregătire și răspuns la nivelul Uniunii pentru a gestiona toate tipurile de dezastre naturale și provocate de om sau de dezastre iminente în interiorul și în afara UE.

12 Regulamentul …/… al Parlamentului European și al Consiliului de instituire a unui instrument pentru situații de urgență pe piața unică și de abrogare a Regulamentului (CE) nr. 2679/98 al Consiliului, COM(2022) 459 final.

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 UE, cât și între UE și autoritățile naționale relevante, inclusiv cele responsabile cu protecția civilă și reziliența infrastructurii critice.

(16) Deși procesele prevăzute în prezenta recomandare ar trebui să fie luate în considerare, după caz, în conexiune cu aceste alte instrumente sau mecanisme atunci când sunt utilizate, prezenta recomandare ar trebui să descrie și acțiunile care ar putea fi întreprinse la nivelul Uniunii în ceea ce privește conștientizarea comună a situației, comunicarea publică coordonată și răspunsul eficace în afara cadrului respectivelor mecanisme ale Uniunii de coordonare a crizelor, în cazul în care acestea nu sunt utilizate.

(17) Pentru o mai bună coordonare a răspunsului în cazul unor incidente semnificative la nivelul infrastructurii critice, ar trebui să existe o cooperare consolidată între statele membre, instituțiile Uniunii și agențiile, organele și oficiile relevante ale Uniunii care funcționează prin acorduri existente, în conformitate cu cadrul aferent Planului de acțiune pentru infrastructura critică. Prin urmare, Planul de acțiune pentru infrastructura critică ar trebui să se aplice atunci când este atins pragul de șase sau mai multe state membre prevăzut în Directiva (UE) 2022/2557 în ceea ce privește identificarea entităților critice de importanță europeană deosebită, precum și atunci când apar incidente care afectează un număr mai mic de state membre, deoarece astfel de incidente ar putea avea un impact amplu, din cauza efectelor în cascadă la nivel transfrontalier și, prin urmare, coordonarea răspunsului la nivelul Uniunii ar fi benefică.

(18) Deși este considerată necesară existența unui cadru de cooperare la nivelul Uniunii pentru un răspuns coordonat la incidentele semnificative la nivelul infrastructurii critice, acesta nu ar trebui să deturneze resursele entităților critice și ale autorităților competente de la gestionarea incidentelor, care ar trebui să reprezinte aspectul prioritar.

(19) Actorii relevanți implicați în punerea în aplicare a Planului de acțiune pentru infrastructura critică ar trebui să fie identificați în mod clar, astfel încât să existe o imagine de ansamblu clară și cuprinzătoare a instituțiilor, organelor, oficiilor, agențiilor și autorităților care ar putea răspunde unui incident semnificativ la nivelul infrastructurii critice.

(20) Răspunsul la incidentele la nivelul infrastructurii critice, inclusiv la incidentele semnificative, este responsabilitatea principală a autorităților competente ale statelor membre. Prezenta recomandare nu ar trebui să afecteze responsabilitatea statelor membre de a proteja securitatea și apărarea națională sau competența acestora de a proteja alte funcții esențiale ale statului, în special în materie de siguranță publică, integritate teritorială și menținerea ordinii publice, în conformitate cu dreptul Uniunii. În plus, prezenta recomandare nu ar trebui să aducă atingere proceselor naționale, cum ar fi comunicarea și legătura operatorilor de infrastructuri critice cu autoritățile naționale competente. Prezenta recomandare ar trebui să se aplice fără a aduce atingere acordurilor bilaterale sau multilaterale relevante încheiate între statele membre.

(21) Desemnarea sau stabilirea de puncte de contact de către actorii relevanți este esențială pentru o cooperare eficace și promptă în cadrul Planului de acțiune pentru infrastructura critică. Pentru a asigura coerența, statele membre ar trebui să ia în considerare posibilitatea de a avea ca puncte de contact desemnate sau instituite în

acest cadru punctele unice de contact care urmează să fie desemnate sau instituite în temeiul Directivei (UE) 2022/2557.

(22) În interesul eficacității, testarea și exersarea Planului de acțiune pentru infrastructura critică, precum și raportarea și discutarea lecțiilor învățate după aplicarea acestuia ar trebui să reprezinte o parte esențială a menținerii unui nivel ridicat de pregătire în cazul unor incidente semnificative la nivelul infrastructurii critice, precum și a asigurării capacității de a răspunde rapid și în mod bine coordonat, cu implicarea actorilor relevanți.

(23) Având în vedere structura mecanismului IPCR al Consiliului de coordonare a crizelor și ținând seama, în sens mai larg, de posibila activare a mecanismelor de coordonare a crizelor deja existente la nivelul Uniunii, Planul de acțiune pentru infrastructura critică ar trebui să cuprindă două moduri de cooperare pentru a răspunde unui incident semnificativ la nivelul infrastructurii critice. Primul mod de operare ar trebui să constea în schimbul de informații, cu implicarea tuturor actorilor relevanți, coordonarea comunicării publice și, dacă sunt utilizate, coordonarea prin intermediul mecanismelor deja existente, cum ar fi mecanismul IPCR din cadrul Consiliului, sau coordonarea ARGUS în cadrul Comisiei, cu sprijinul ERCC în calitate de punct de contact ce funcționează 24 de ore din 24, 7 zile pe săptămână, și al mecanismului de răspuns în caz de criză al SEAE. Al doilea mod de operare ar trebui să cuprindă acțiuni suplimentare de răspuns, în funcție de amploarea incidentului. Această cooperare ar trebui să implice un angajament la nivel operațional și strategic/politic care să reflecte nivelurile din Recomandarea 2017/1584 și din Protocolul Uniunii pentru combaterea amenințărilor hibride, în scopul de a coordona acțiunile și a răspunde în mod eficace și eficient la incidentul semnificativ la nivelul infrastructurii critice. Pe baza principiilor proporționalității, subsidiarității, confidențialității informațiilor și complementarității și pentru a asigura o cooperare eficace, Planul de acțiune pentru infrastructura critică ar trebui să descrie modul în care actorii relevanți conștientizează în comun situația, precum și modul în care se asigură comunicarea publică coordonată și răspunsul eficace.

(24) Schimbul de informații în temeiul prezentei recomandări ar trebui să se desfășoare fără a pune în pericol securitatea națională sau securitatea și interesele comerciale ale entităților care operează infrastructuri critice. Prin urmare, informațiile sensibile ar trebui accesate, comunicate și manipulate cu prudență, în conformitate cu normele aplicabile și acordând o atenție deosebită canalelor de transmisie și capacităților de stocare utilizate,

ADOPTĂ PREZENTA RECOMANDARE:

(1) Statele membre, Consiliul, Comisia și, după caz, Serviciul European de Acțiune Externă („SEAE”), precum și organele, oficiile și agențiile relevante ale Uniunii ar trebui să coopereze între ele în cadrul Planului de acțiune pentru infrastructura critică cuprins în prezenta recomandare, cu scopul de a atinge obiectivele stabilite în secțiunea 1 a părții I din anexă și, ținând seama de principiile prevăzute în secțiunea 2 a părții I din anexă, de a oferi un răspuns coordonat la incidentele semnificative la nivelul infrastructurii critice.

(2) Statele membre, Consiliul, Comisia și, după caz, SEAE, precum și organele, oficiile și agențiile relevante ale Uniunii ar trebui să aplice Planul de acțiune pentru infrastructura critică fără întârzieri nejustificate ori de câte ori are loc un incident

semnificativ la nivelul infrastructurii critice, și anume un incident care implică o infrastructură critică și care are unul dintre următoarele efecte:

(a) un efect perturbator semnificativ asupra furnizării de servicii esențiale pentru șase sau mai multe state membre sau pe teritoriul acestora, inclusiv atunci când incidentul afectează o entitate critică de importanță europeană deosebită în sensul articolului 17 din Directiva (UE) 2022/2557 privind reziliența entităților critice[13]; sau

(b) un efect perturbator semnificativ asupra furnizării de servicii esențiale pe teritoriul a două sau mai multe state membre, în cazul în care statul membru care deține președinția prin rotație a Consiliului, de comun acord cu aceste alte state membre și în consultare cu Comisia, consideră că este necesară coordonarea promptă în ceea ce privește răspunsul la nivelul Uniunii, având în vedere impactul amplu și semnificativ din punct de vedere tehnic sau politic al incidentului.

(3) Actorii relevanți ai Planului de acțiune pentru infrastructura critică, identificați la nivel operațional și strategic/politic în conformitate cu secțiunea 3 a părții I din anexă, ar trebui să depună eforturi pentru a interacționa și a coopera în complementaritate. Aceștia ar trebui să asigure schimbul adecvat și prompt de informații, inclusiv coordonarea comunicării publice, precum și răspunsul coordonat, astfel cum se prevede în partea II din anexă.

(4) Planul de acțiune pentru infrastructura critică ar trebui aplicat având în vedere alte instrumente relevante și în mod coerent cu acestea, în conformitate cu secțiunea 4 a părții I din anexă. În cazul în care un incident afectează atât aspectele fizice, cât și securitatea cibernetică a infrastructurii critice, ar trebui asigurate sinergii cu procesele relevante instituite în Planul de acțiune în materie de securitate cibernetică.

(5) Statele membre ar trebui să se asigure că răspund în mod eficace la nivel național și în conformitate cu dreptul Uniunii la perturbările infrastructurii critice cauzate de incidente semnificative la nivelul infrastructurii critice.

(6) Statele membre, Consiliul, SEAE, Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii („Europol”) și alte agenții relevante ale Uniunii, precum și Comisia, ar trebui să desemneze sau să stabilească un punct de contact pentru aspectele legate de Planul de acțiune pentru infrastructura critică. Punctele de contact ar trebui să sprijine aplicarea Planului de acțiune pentru infrastructura critică prin furnizarea informațiilor necesare și să faciliteze măsurile de coordonare ca răspuns la un incident semnificativ la nivelul infrastructurii critice. Pentru statele membre, în măsura posibilului, punctele de contact respective ar trebui să fie aceleași cu punctele unice de contact care urmează să fie desemnate sau instituite în temeiul articolului 9 alineatul (2) din Directiva (UE) 2022/2557. 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.

[13] 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).

(7) Statul membru care deține președinția prin rotație a Consiliului, de comun acord cu statele membre afectate, ar trebui să informeze toți actorii relevanți, prin intermediul punctelor de contact menționate la punctul 6, cu privire la incidentul semnificativ la nivelul infrastructurii critice și la aplicarea Planului de acțiune pentru infrastructura critică. Schimbul de informații cu privire la un incident semnificativ la nivelul infrastructurii critice ar trebui să aibă loc prin intermediul unor canale de comunicare adecvate, inclusiv, după caz și dacă acest lucru este adecvat, prin platforma mecanismului integrat al UE pentru un răspuns politic la crize[14] („IPCR") și, în cadrul ERCC, prin intermediul Sistemului comun de comunicare și informare în caz de urgență („CECIS") – o aplicație web de alertă și notificare care permite schimbul de informații în timp real.

(8) Dacă este necesar, canalele de transmisie ar trebui să includă canale securizate, pentru a nu pune în pericol securitatea națională sau securitatea și interesele comerciale ale entităților în cauză. Schimbul de informații descris în secțiunea 1 a părții II din anexa la prezenta recomandare ar trebui, de asemenea, să se desfășoare fără a pune în pericol securitatea națională sau securitatea și interesele comerciale ale entităților critice și în conformitate cu dreptul Uniunii, în special cu Regulamentul (UE).../... al Parlamentului European și al Consiliului[15]. În special, informațiile sensibile ar trebui accesate, comunicate și manipulate cu prudență. Pentru manipularea și schimbul de informații clasificate ar trebui utilizate instrumente acreditate disponibile, precum și măsuri de securitate adecvate.

(9) Actorii relevanți ar trebui să organizeze simulări și să testeze în mod regulat, la nivel național, regional și la nivelul Uniunii, funcționarea Planului de acțiune pentru infrastructura critică și răspunsul lor coordonat la un incident semnificativ la nivelul infrastructurii critice, de exemplu în contextul unor exerciții. Astfel de simulări și teste pot include, după caz, entități din sectorul privat. Un exercițiu la nivelul Uniunii care să includă aspecte fizice și cibernetice ar trebui să aibă loc până la [*data adoptării prezentei recomandări + 12 luni*].

(10) În urma aplicării Planului de acțiune pentru infrastructura critică în cazul unui incident semnificativ la nivelul infrastructurii critice, Grupul privind reziliența entităților critice menționat la articolul 19 din Directiva (UE) 2022/2557 ar trebui să discute prompt cu actorii relevanți lecțiile învățate, care pot indica lacune și domenii în care sunt necesare îmbunătățiri și, ulterior, să întocmească un raport, incluzând recomandări pentru efectuarea unor astfel de îmbunătățiri. Actorii relevanți implicați în aplicarea Planului de acțiune pentru infrastructura critică ar trebui să sprijine întocmirea raportului respectiv. Raportul ar trebui adoptat de Comisie.

(11) Statele membre ar trebui să discute raportul menționat la punctul 10 în cadrul grupurilor de pregătire relevante ale Consiliului sau în cadrul Consiliului.

---

[14] Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize ST/13422/2018/INIT (JO L 320, 17.12.2018, p. 28).

[15] Regulamentul (UE) …/… privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii, COM(2022) 119 final.

Adoptată la Bruxelles,

Pentru Consiliu,
Președintele