Consiliul
Uniunii Europene

Bruxelles, 6 iunie 2025
(OR. en)

9794/25

Dosar interinstituțional:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Data:	6 iunie 2025
Destinatar:	Delegațiile
Subiect:	Recomandare a Consiliului privind un Plan de acțiune al UE pentru gestionarea crizelor cibernetice – Recomandare a Consiliului aprobată de Consiliu în cadrul reuniunii sale din 6 iunie 2025

În anexă, se pune la dispoziția delegațiilor recomandarea Consiliului, astfel cum a fost aprobată de Consiliu în cadrul reuniunii sale din 6 iunie 2025.

ANEXĂ

RECOMANDARE A CONSILIULUI

privind un Plan de acțiune al UE pentru gestionarea crizelor cibernetice

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) Tehnologia digitală și conectivitatea globală reprezintă coloana vertebrală a creșterii economice, a competitivității și a transformării infrastructurii critice a Uniunii. Într-o economie interconectată și din ce în ce mai digitalizată crește însă și riscul de incidente de securitate cibernetică și de atacuri cibernetice. În plus, intensificarea tensiunilor geopolitice, a conflictelor și a rivalității strategice se reflectă în impactul, volumul și sofisticarea sporite ale activităților cibernetice răuvoitoare. Astfel de activități pot face parte din campanii hibride sau din operații militare. De asemenea, acestea pot afecta direct securitatea, economia și societatea Uniunii. În plus, ele au un potențial de propagare, în special atunci când aceste activități vizează țările care sunt parteneri strategici internaționali, cum ar fi țările candidate sau învecinate.

(2) Un incident de securitate cibernetică de mare amploare poate provoca un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau are un impact semnificativ asupra mai multor state membre. În funcție de cauza și impactul său, un astfel de incident ar putea escalada, transformându-se într-o criză propriu-zisă care poate afecta buna funcționare a pieței interne sau poate prezenta riscuri de securitate și siguranță publică grave pentru entități sau cetățeni în mai multe state membre sau în Uniune în ansamblul său. Gestionarea eficace a crizelor este esențială pentru menținerea stabilității economice și protejarea autorităților guvernamentale, a infrastructurii critice, a întreprinderilor și a cetățenilor europeni, precum și pentru consolidarea securității și a stabilității internaționale în spațiul cibernetic. Prin urmare, gestionarea crizelor cibernetice face parte integrantă din cadrul general al UE de gestionare a crizelor.

(3) Având în vedere interdependențele și interconexiunile dintre mediile TIC ale entităților Uniunii și ale statelor membre, un incident într-o entitate a Uniunii ar putea prezenta un risc de securitate cibernetică pentru statele membre și invers. Schimbul de informații relevante și coordonarea în ceea ce privește atât incidentele de securitate cibernetică de mare amploare, cât și incidentele majore, astfel cum sunt definite la articolul 3 punctul 8 din Regulamentul (UE, Euratom) 2023/2841[1], sunt esențiale în contextul Planului de acțiune al UE pentru gestionarea crizelor cibernetice (în continuare „Planul de acțiune pentru gestionarea crizelor cibernetice”).

[1] Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii, JO L, 2023/2841, 18.12.2023, p. 1.

(4) În cazul unei crize pentru care a fost activat mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) în temeiul Deciziei de punere în aplicare (UE) 2018/1993 a Consiliului[2] (în continuare „mecanismul IPCR”), Planul de acțiune pentru gestionarea crizelor cibernetice ar trebui să respecte pe deplin mecanismul IPCR în ceea ce privește coordonarea și răspunsul. Coordonarea politică și strategică ar urma să aibă loc în cadrul IPCR. Mecanismul IPCR este instrumentul de coordonare orizontală și de răspuns la nivelul politic al Uniunii. În temeiul mecanismului IPCR, decizia de activare sau de dezactivare a IPCR este luată de președinția Consiliului Uniunii Europene. Rapoartele privind analiza și conștientizarea integrată a situației (ISAA) elaborate de serviciile Comisiei și de Serviciul European de Acțiune Externă (SEAE) sprijină activitatea IPCR atât în modul „schimb de informații”, cât și în modul „activare integrală”.

(5) Statele membre au responsabilitatea principală în gestionarea incidentelor de securitate cibernetică și a crizelor cibernetice. Potențialul caracter transfrontalier și transsectorial al incidentelor de securitate cibernetică impune însă statelor membre și entităților relevante ale Uniunii să coopereze la nivel tehnic, operațional și politic pentru a se coordona în mod eficace în întreaga Uniune. Gestionarea crizelor cibernetice pe durata întregului lor ciclu de viață include pregătirea și conștientizarea comună a situației pentru a anticipa incidentele de securitate cibernetică de mare amploare, capacități de detectare necesare pentru identificarea instrumentelor de răspuns și de redresare de care e nevoie pentru a atenua și limita incidentele de securitate cibernetică de mare amploare, precum și capacități de reacție pentru a descuraja și preveni noi incidente.

[2] 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.

(6) Recomandarea (UE) 2017/1584 a Comisiei[3] privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare stabilește obiectivele și modurile de cooperare între statele membre și entitățile Uniunii în ceea ce privește răspunsul la incidentele și crizele de securitate cibernetică de mare amploare. Ea a realizat un inventar al actorilor relevanți la nivel tehnic, operațional și politic și a explicat modul în care aceștia au fost integrați în mecanismele existente de gestionare a crizelor la nivelul Uniunii, cum ar fi mecanismul IPCR. Principiile de bază prevăzute în Recomandarea (UE) 2017/1584 rămân valabile, și anume subsidiaritatea, complementaritatea și confidențialitatea informațiilor, precum și abordarea pe trei niveluri (tehnic, operațional și politic). Prezenta recomandare pornește de la aceste principii de bază și este menită să înlocuiască Recomandarea (UE) 2017/1584, stabilind un nou cadru al Uniunii pentru gestionarea crizelor în materie de securitate cibernetică.

(7) Unele definiții utilizate în prezenta recomandare se bazează pe definițiile și termenii utilizați în Directiva (UE) 2022/2555[4]. Domeniul de aplicare al prezentei recomandări este însă diferit de domeniul de aplicare al Directivei (UE) 2022/2555. Prezenta recomandare stabilește cadrul Uniunii pentru gestionarea crizelor cibernetice în contextul pregătirii generale a UE pentru incidentele de securitate cibernetică de mare amploare și crizele cibernetice care decurg din astfel de incidente – indiferent de ce sector sau entitate sunt afectate. În măsura posibilului, definițiile se bazează pe cele cuprinse în Directiva (UE) 2022/2555.

---

[3] 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.

[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 (Directiva NIS 2), JO L 333, 27.12.2022, p. 80.

(8) Este necesar un Plan de acțiune pentru gestionarea crizelor cibernetice actualizat care să ofere orientări clare și accesibile prin care să se explice ce este un incident de securitate cibernetică de mare amploare sau o criză cibernetică la nivelul Uniunii, cum se activează cadrul de gestionare a crizelor și care sunt rolurile rețelelor, ale actorilor și ale mecanismelor relevante de la nivelul Uniunii, precum și cum interacționează acești actori și aceste mecanisme pe parcursul întregului ciclu de viață al crizei cibernetice. Planul de acțiune pentru gestionarea crizelor cibernetice urmărește să sprijine cadrul mai larg al relațiilor civile și militare ale UE în contextul gestionării crizelor cibernetice, inclusiv pe fondul aprofundării relațiilor UE-NATO, inclusiv, acolo unde este posibil, prin mecanisme consolidate de schimb de informații favorabile incluziunii, reciproce și nediscriminatorii în gestionarea crizelor cibernetice.

(9) Ar trebui consolidată gestionarea transsectorială a crizelor la nivelul Uniunii pentru a permite un răspuns integrat la situații de criză, în special în cazurile în care incidentele de securitate cibernetică de mare amploare și crizele au urmări fizice. Prezenta recomandare completează mecanismul IPCR și alte mecanisme de gestionare a crizelor ale Uniunii, inclusiv sistemul general de alertă rapidă ARGUS al Comisiei, mecanismul de protecție civilă al Uniunii (UCPM) sprijinit de Centrul de coordonare a răspunsului la situații de urgență (ERCC) instituit în cadrul UCPM prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului privind un mecanism de protecție civilă al Uniunii[5] (în continuare „Decizia privind UCPM”), mecanismul de răspuns în caz de criză al SEAE (CRM), precum și alte procese, cum ar fi cele descrise în setul de instrumente al UE pentru diplomația cibernetică[6], în setul de instrumente al UE pentru contracararea amenințărilor hibride[7] și în protocolul revizuit al UE pentru combaterea amenințărilor hibride[8]. De asemenea, aceasta completează și ar trebui să fie coerentă cu Recomandarea (UE) 2024/4371 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[9] (în continuare „Planul de acțiune al UE pentru infrastructura critică”), care acoperă reziliența fizică necibernetică și care vizează îmbunătățirea coordonării răspunsului la nivelul Uniunii în acest domeniu.

---

5 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.

6 Concluziile Consiliului referitoare la un cadru privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare (9916/17).

7 Concluziile Consiliului privind un cadru pentru un răspuns coordonat al UE la campaniile hibride, 22 iunie 2022.

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

9 JO C, C/2024/4371, 5.7.2024.

(10) Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) este rețeaua pentru coordonarea gestionării incidentelor și crizelor de securitate cibernetică de mare amploare la nivel operațional, inclusiv în cazul incidentelor de securitate cibernetică de mare amploare și în cel al crizelor cibernetice transsectoriale. Pentru a nu face cadrele existente și mai complicate, ar trebui evitată crearea de structuri sectoriale care să se suprapună sarcinilor EU-CyCLONe. EU-CyCLONe ar trebui să primească informații operaționale legate de securitatea cibernetică și din partea sectoarelor și să transmită contribuții nivelului politic.

(11) Statele membre sunt încurajate să utilizeze pe deplin resursele financiare disponibile pentru securitatea cibernetică furnizate de programele relevante ale Uniunii. Ar trebui să se garanteze că aceste programe impun sarcini administrative minime solicitanților de finanțare și că participarea statelor membre la aceste programe este facilitată prin oferirea de orientări relevante privind opțiunile de sprijin financiar viabile.

(12) Prezenta recomandare contribuie la acțiuni de pregătire mai ample necesare Uniunii în situația unor crize transsectoriale, în conformitate cu principiile integrate în Strategia UE privind o uniune a pregătirii pentru situații de criză, și anume o abordare integrată care să ia în considerare toate riscurile, la nivelul întregii administrații și la nivelul întregii societăți, în special în ceea ce privește îmbunătățirea gradului de sensibilizare cu privire la riscuri și amenințări și răspunsul transsectorial la situații de criză,

ADOPTĂ PREZENTA RECOMANDARE:

I: Scopul, domeniul de aplicare și principiile directoare ale cadrului UE de gestionare a crizelor cibernetice

Scop și domeniu de aplicare

1. Prezenta recomandare privind Planul UE de gestionare a crizelor cibernetice („Planul de acțiune pentru gestionarea crizelor cibernetice”) stabilește cadrul Uniunii pentru gestionarea crizelor cibernetice în contextul pregătirii generale a UE pentru incidente de securitate cibernetică de mare amploare și pentru crize cibernetice. Cadrul reflectă atât rolurile statelor membre, cât și pe cele ale instituțiilor, organelor, oficiilor și agențiilor Uniunii (în continuare „entitățile Uniunii”), în limitele competențelor fiecăreia dintre acestea, cu respectarea deplină a legislației naționale și a normelor interne, în asigurarea unei acțiuni cuprinzătoare și coordonate la nivelul Uniunii.

2. Planul de acțiune pentru gestionarea crizelor cibernetice ar trebui aplicat asigurându-i-se coerența cu Planul de acțiune al UE pentru infrastructura critică, în special în cazul incidentelor care afectează atât reziliența fizică, cât și securitatea cibernetică a infrastructurii critice[10].

3. Planul de acțiune pentru gestionarea crizelor cibernetice oferă orientări pentru răspunsul la incidentele de securitate cibernetică de mare amploare sau la crize cibernetice și ar trebui utilizat în completarea oricărui mecanism sectorial de răspuns relevant, cum ar fi cele enumerate în anexa II. Părțile interesate relevante din domeniul securității cibernetice ar trebui să acorde ajutor și asistență la atingerea obiectivelor acestor mecanisme sectoriale, atât la nivel național, cât și la nivelul Uniunii.

4. În cazul unei crize transsectoriale la nivelul UE cu aspecte cibernetice pentru care este activat IPCR, coordonarea răspunsului la nivelul politic al Uniunii ar trebui să fie efectuată de Consiliu, utilizând mecanismul IPCR. După activarea IPCR, măsurile din cadrul Planului de acțiune pentru gestionarea crizelor cibernetice ar trebui să sprijine răspunsul UE la nivel politic, oferind sprijin specific în materie de securitate cibernetică.

---

10 Planul de acțiune pentru infrastructura critică detaliază coordonarea în astfel de cazuri în partea I secțiunea 4 din anexa sa.

Principii generale

5. În gestionarea crizelor cibernetice la nivelul Uniunii se aplică următoarele principii directoare:

(a) *Proporționalitate*: majoritatea incidentelor de securitate cibernetică care afectează statele membre se situează sub nivelul a ceea ce ar putea fi considerat incident de securitate cibernetică de mare amploare sau criză cibernetică la nivel național sau la nivelul Uniunii. În cazul incidentelor și amenințărilor de securitate cibernetică, statele membre cooperează și fac schimb de informații voluntar și periodic în cadrul rețelei echipelor de intervenție în caz de incidente de securitate informatică (în continuare „rețeaua CSIRT") și în cadrul EU-CyCLONe, în conformitate cu procedurile standard de operare (PSO) ale rețelelor.

(b) *Subsidiaritate*: statelor membre le revine responsabilitatea principală în ceea ce privește răspunsul și remedierea în cazul unui incident de securitate cibernetică, al unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice care le afectează. Având în vedere potențialele efecte transfrontaliere, Consiliul, Comisia, Înaltul Reprezentant, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE), Europol și toate celelalte entități relevante ale Uniunii ar trebui să coopereze pe parcursul întregului ciclu de viață al crizei. Acest rol decurge din dreptul Uniunii și reflectă modul în care incidentele de securitate cibernetică de mare amploare și crizele cibernetice afectează unul sau mai multe sectoare de activitate economică din cadrul pieței unice, securitatea și relațiile internaționale ale Uniunii și chiar entitățile acesteia.

(c) *Complementaritate*: prezenta recomandare ține seama integral de mecanismele existente de gestionare a crizelor la nivelul Uniunii enumerate în anexa II, în special mecanismul IPCR, ARGUS și mecanismul de răspuns în caz de criză al SEAE. Prezenta recomandare ține seama de mandatul rețelei CSIRT și de cel al EU-CyCLONe, precum și de Regulamentul (UE, Euratom) 2023/2841. În cazul în care IPCR este activat, activitatea rețelelor, a entităților și a mecanismelor sectoriale activate relevante ar trebui să continue și să contribuie la coordonarea politică și strategică care are loc în cadrul IPCR și să o sprijine.

(d) *Confidențialitatea informațiilor*: toate schimburile de informații realizate în contextul prezentei recomandări ar trebui să respecte normele aplicabile privind securitatea și privind protecția datelor cu caracter personal. Atunci când este cazul, ar trebui luate în considerare acordurile informale de nedivulgare, precum protocolul de tip semafor pentru clasificarea informațiilor sensibile. Pentru schimbul de informații clasificate, indiferent de sistemul de clasificare aplicat, normele și acordurile obligatorii existente privind prelucrarea informațiilor clasificate ar trebui utilizate împreună cu instrumentele acreditate disponibile.

6. În conformitate cu principiile directoare menționate mai sus, statele membre și entitățile Uniunii ar trebui să își aprofundeze cooperarea în gestionarea crizelor cibernetice, promovând încrederea reciprocă și bazându-se pe rețelele și mecanismele existente. Această cooperare, în cadrul Planului de acțiune pentru gestionarea crizelor cibernetice, beneficiază de punerea în aplicare a articolelor 22 și 23 din Regulamentul (UE, Euratom) 2023/2841. În special, planul de gestionare a crizelor cibernetice instituit în temeiul articolului 23 din Regulamentul (UE, Euratom) 2023/2841 contribuie, printre altele, la schimbul periodic de informații relevante între entitățile Uniunii și cu statele membre și definește măsuri privind coordonarea și fluxul de informații între entitățile Uniunii.

II: Definiții

7. În sensul prezentului Plan de acțiune pentru gestionarea crizelor cibernetice, se aplică următoarele definiții:

(a) „incident” înseamnă 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;

(b) „incident semnificativ” înseamnă un incident care:

a. a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză;

b. a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile.

(c) „incident de securitate cibernetică de mare amploare” înseamnă un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre;

(d) „criză cibernetică” înseamnă un incident de securitate cibernetică de mare amploare care a escaladat, transformându-se într-o criză propriu-zisă, care împiedică buna funcționare a pieței interne sau prezintă riscuri grave de securitate și siguranță publică pentru entități sau cetățeni în mai multe state membre sau în Uniune în ansamblul său.

III: Structuri și responsabilități naționale de gestionare a crizelor cibernetice

8. Statelor membre le revine responsabilitatea principală în ceea ce privește răspunsul la incidentele de securitate cibernetică de mare amploare sau la crizele cibernetice care le afectează. În conformitate cu Directiva (UE) 2022/2555, fiecare stat membru are una sau mai multe autorități de gestionare a crizelor cibernetice, precum și una sau mai multe echipe CSIRT.

9. Prin adoptarea Directivei (UE) 2022/2555 și a altor instrumente legislative și fără caracter legislativ în materie de securitate cibernetică, statele membre și-au aliniat cadrele de securitate cibernetică prin stabilirea de norme minime privind funcționarea cadrului de reglementare coordonat, prin stabilirea de mecanisme de cooperare eficace între autoritățile responsabile din fiecare stat membru și prin asigurarea de căi de atac și de măsuri eficace de aplicare a legii, care sunt esențiale pentru asigurarea efectivă a respectării acestor obligații.

10. În conformitate cu articolul 9 alineatul (4) din Directiva (UE) 2022/2555, statele membre ar trebui să adopte planuri naționale de răspuns la incidente de securitate cibernetică de mare amploare și la crize. Aceste planuri includ, printre altele, măsuri naționale de pregătire, proceduri de gestionare a crizelor cibernetice și proceduri naționale și acorduri între autoritățile și organismele naționale pentru a asigura participarea lor efectivă la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor cibernetice la nivelul Uniunii, precum și sprijinirea acesteia. Procedurile de gestionare a crizelor cibernetice includ și dispoziții privind integrarea acestora în cadrul național general de gestionare a crizelor și în canalele de schimb de informații.

11. În conformitate cu articolul 9 alineatul (1) din Directiva (UE) 2022/2555, statele membre ar trebui să asigure corelarea cu cadrele existente pentru gestionarea națională generală a crizelor. În cazul activării IPCR, autoritățile naționale de gestionare a crizelor ar trebui să colecteze contribuții de la autoritățile de gestionare a crizelor cibernetice și de la mecanismele sectoriale naționale de gestionare a crizelor, în scopul informării IPCR.

12. În conformitate cu articolul 9 alineatul (5) din Directiva (UE) 2022/2555, la cererea unui stat membru în cauză, EU-CyCLONe ar trebui să facă schimb de informații cu privire la părțile relevante ale planurilor naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize, în special în ceea ce privește dispozițiile menite să asigure participarea efectivă la gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor cibernetice la nivelul Uniunii și sprijinul pentru aceasta, pentru a face schimb de bune practici și a reflecta asupra fezabilității practice a cadrului general.

13. EU-CyCLONe și Consiliul interinstituțional pentru securitate cibernetică (IICB) sunt invitate să facă schimb, după caz, de informații privind coerența dintre planul de gestionare a crizelor stabilit de IICB în conformitate cu articolul 23 din Regulamentul (UE, Euratom) 2023/2841 și planurile naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize.

14. EU-CyCLONe, cu sprijinul ENISA în calitate de secretariat, ar trebui să mențină o listă actualizată a autorităților naționale de gestionare a crizelor cibernetice care să cuprindă datele de contact ale persoanelor cu funcții de execuție și de conducere din cadrul EU-CyCLONe și să o pună la dispoziția membrilor EU-CyCLONe.

IV: Principalele rețele și principalii actori din ecosistemul de gestionare a crizelor cibernetice al UE

15. Rețeaua CSIRT este principala rețea tehnică pentru schimbul de informații relevante cu privire la incidente, în special în domeniul de aplicare al prezentei recomandări, în conformitate cu sarcinile relevante descrise la articolul 15 alineatul (3) din Directiva (UE) 2022/2555. Ea contribuie la dezvoltarea încrederii și promovează o cooperare operațională rapidă și eficace între statele membre. Președintele rețelei CSIRT poate participa la IICB în calitate de observator.

16. CERT-UE este serviciul de securitate cibernetică pentru toate entitățile Uniunii. CERT-UE acționează ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente pentru entitățile Uniunii, în conformitate cu articolul 13 din Regulamentul (UE) 2023/2841. CERT-UE este membru al rețelei CSIRT și sprijină Comisia în cadrul EU-CyCLONe. CERT-UE funcționează la nivel tehnic și este responsabil de coordonarea gestionării incidentelor majore care afectează entitățile Uniunii.

17. EU-CyCLONe acționează ca intermediar între nivelul tehnic și cel politic, în special în timpul incidentelor de securitate cibernetică de mare amploare și al crizelor cibernetice. Sprijină gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor cibernetice și asigură schimbul periodic de informații relevante între statele membre și instituțiile, organele, oficiile și agențiile Uniunii, în conformitate cu articolul 16 din Directiva (UE) 2022/2555. Președintele EU-CyCLONe poate participa la IICB în calitate de observator.

18. ENISA este agenția Uniunii care îndeplinește sarcinile atribuite în temeiul Regulamentului (UE) 2019/881[11] în scopul atingerii unui nivel comun ridicat de securitate cibernetică în întreaga Uniune, inclusiv prin sprijinirea activă a statelor membre și a instituțiilor, organelor și agențiilor Uniunii. ENISA asigură, printre altele, secretariatul rețelei CSIRT și al EU-CyCLONe, servicii de conștientizare a situației și asistă statele membre prin organizarea periodică de exerciții de securitate cibernetică la nivelul Uniunii. În conformitate cu Directiva (UE) 2022/2555 și cu Regulamentul (UE) 2024/2847[12], ENISA primește informații cu privire la incidentele transfrontaliere semnificative și la vulnerabilitățile și incidentele exploatate în mod activ care afectează produsele digitale.

19. Consiliul Uniunii Europene (în continuare „Consiliul”) este instituția Uniunii cu funcții de definire a politicilor și de coordonare în temeiul articolului 16 din Tratatul privind Uniunea Europeană (TUE) și i se încredințează IPCR, care vizează coordonarea și răspunsul la nivelul politic al Uniunii. Consiliul funcționează prin intermediul formațiunilor Consiliului, al Comitetului Reprezentanților Permanenți și al grupurilor de pregătire relevante ale Consiliului, în special al Grupului de lucru orizontal pentru chestiuni cibernetice (HWPCI), precum și, după caz, al mecanismului IPCR.

---

[11] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), JO L 151, 7.6.2019, p. 15.

[12] Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică), JO L, 2024/2847, 20.11.2024, p. 1.

20. Comisia, în calitate de instituție care promovează interesul general al Uniunii și care adoptă inițiative adecvate în acest scop, precum și care asigură aplicarea tratatelor și a măsurilor adoptate de instituții în temeiul articolului 17 din TUE, este responsabilă de anumite acțiuni generale de pregătire la nivelul Uniunii și de anumite acțiuni de conștientizare a situației, inclusiv de gestionarea ERCC și a sistemului comun de comunicare și informare în caz de urgență (CECIS), în conformitate cu Decizia privind UCPM. Ea facilitează coerența și coordonarea la nivel operațional între acțiunile conexe de răspuns în situații de criză la nivelul Uniunii. Comisia este consultată în legătură cu deciziile de activare sau dezactivare a IPCR. Serviciile Comisiei pregătesc, împreună cu SEAE, rapoartele ISAA. Comisia este membră a EU-CyCLONe în cazurile în care un incident de securitate cibernetică de mare amploare potențial sau în desfășurare are sau este probabil să aibă un impact semnificativ asupra serviciilor și activităților care intră în domeniul de aplicare al Directivei (UE) 2022/2555, precum și observator în alte cazuri. Ea este punctul de contact cu EU-CyCLONe în cadrul IICB. Comisia este observator în cadrul rețelei CSIRT.

21. Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (în continuare „Înaltul Reprezentant”), asistat de SEAE, conduce politica externă și de securitate comună (PESC) a Uniunii și contribuie prin propunerile sale la dezvoltarea acestei politici, inclusiv a politicii de securitate și apărare comune (PSAC). Aceasta include structurile și mecanismele diplomatice, de informații și militare, în special Capacitatea unică de analiză a informațiilor (SIAC) ca punct unic de acces pentru serviciile de informații ale statelor membre, Statul-Major al UE (EUMS) ca sursă de competență militară, setul de instrumente al UE pentru diplomația cibernetică, precum și rețeaua delegațiilor UE, care pot contribui la gestionarea crizelor dintr-o perspectivă externă. De asemenea, SEAE pregătește, împreună cu Comisia, rapoartele ISAA.

22. Anexa II descrie rolurile și competențele actorilor relevanți de la nivelul Uniunii în ceea ce privește gestionarea crizelor cibernetice, inclusiv ale principalelor rețele și actori.

V: Pregătirea pentru incidentele de securitate cibernetică de mare amploare și pentru o criză cibernetică

Peisajul amenințărilor

23. Statele membre și entitățile relevante ale Uniunii ar trebui să ia măsurile necesare pentru a îmbunătăți conștientizarea situației, recunoscând că peisajul amenințărilor și conștientizarea situației specifice unui incident necesită moduri de operare distincte. Statele membre și entitățile relevante ale Uniunii ar trebui să colaboreze pe baza unor date verificate și fiabile, inclusiv a tendințelor în materie de incidente, tactici, tehnici și proceduri, și a vulnerabilităților exploatate activ.

24. Atunci când fac schimb de informații la nivelul UE, statele membre ar trebui să utilizeze pe deplin platformele existente pentru cooperare tehnică și operațională, cum ar fi cele utilizate de rețeaua CSIRT și de EU-CyCLONe.

25. Pentru a îmbunătăți conștientizarea comună a situației și pentru a facilita evaluarea impactului la nivelul UE, EU-CyCLONe și rețeaua CSIRT, cu sprijinul ENISA, ar trebui să utilizeze un mecanism de raportare convenit la nivel intern pentru a produce o imagine de ansamblu la nivelul UE a activităților tehnice și operaționale pe baza informațiilor colectate la nivel național.

26. EU-CyCLONe și rețeaua CSIRT ar trebui:

    (a) să coopereze pentru a îmbunătăți schimbul de informații între nivelul tehnic și cel operațional și conștientizarea situației în ansamblu;

    (b) să continue să construiască un climat de încredere între membrii lor și între rețele;

    (c) să utilizeze pe deplin instrumentele disponibile pentru schimbul de informații, cu sprijinul ENISA, să reflecteze asupra modalităților de a îmbunătăți aceste instrumente și să asigure interoperabilitatea între rețele.

27. EU-CyCLONe, rețeaua CSIRT și IICB ar trebui să coopereze pentru a asigura un schimb eficace de informații relevante.

28. ENISA, în calitate de secretariat al rețelei CSIRT și al EU-CyCLONe, are un rol central în sprijinirea statelor membre și a instituțiilor, organelor și agențiilor Uniunii în vederea realizării unei conștientizări comune a situației la nivelul UE pe plan tehnic și operațional pentru a sprijini pregătirea pentru incidentele de securitate cibernetică de mare amploare și pentru crize.

29. În conformitate cu Directiva (UE) 2022/2555 și cu Regulamentul (UE) 2019/881, statele membre și entitățile relevante ale Uniunii ar trebui să se coordoneze cu sectorul privat, inclusiv cu producătorii și cu comunitățile de utilizatori de software cu sursă deschisă, pentru a îmbunătăți schimbul de informații. În special, ENISA ar trebui să utilizeze programul său de parteneriat în acest sens. În plus, statele membre și entitățile relevante ale Uniunii s-ar putea baza și pe centrele de schimb de informații și de analiză (ISAC) existente la nivelul UE și la nivel național pentru a consolida capacitatea de securitate cibernetică și pentru a răspunde la incidente de securitate cibernetică, inclusiv prin reuniuni comune ale sectorului privat cu EU-CyCLONe sau cu rețeaua CSIRT.

30. Pentru a intensifica schimbul de informații în cadrul rețelelor și între acestea și pentru a clarifica așteptările reciproce în ceea ce privește acest schimb, în termen de 24 de luni de la adoptarea prezentei recomandări EU-CyCLONe ar trebui să convină asupra unei taxonomii comune aliniate a nivelurilor de gravitate a incidentelor, cu sprijinul ENISA în calitate de secretariat și după consultarea rețelei CSIRT și a Grupului de cooperare NIS. Această taxonomie ar trebui să permită o comparare a gravității incidentelor din statele membre, luând în considerare impactul asupra furnizării de servicii, numărul de entități afectate și relevanța acestora, impactul asupra altor servicii și infrastructuri, precum și prejudiciile monetare, de reputație și politice cauzate. Taxonomia ar trebui să se bazeze pe scalele sau taxonomiile existente relevante, cum ar fi taxonomia de referință a clasificării incidentelor.

Nivelul tehnic

31. Rețeaua CSIRT este platforma pentru cooperare tehnică și schimb de informații între toate statele membre și, prin intermediul CERT-UE, cu entitățile Uniunii.

32. În conformitate cu Directiva (UE) 2022/2555, fiecare echipă CSIRT are sarcina de a monitoriza și analiza amenințările, vulnerabilitățile și incidentele cibernetice la nivel național. Echipele CSIRT ar trebui să facă schimb, atât în cadrul rețelei CSIRT, cât și la nivel bilateral, de informații relevante cu privire la incidente, incidente evitate la limită, amenințări cibernetice, riscuri și vulnerabilități pentru a realiza o conștientizare comună a situației.

33. Pentru a consolida cooperarea operațională la nivelul Uniunii, rețeaua CSIRT ar trebui să aibă în vedere să invite organele și agențiile Uniunii implicate în politica de securitate cibernetică, cum ar fi Europol, să participe la activitatea sa.

34. În conformitate cu Regulamentul 2023/2841, CERT-UE ar trebui să colecteze, să gestioneze, să analizeze și să facă schimb de informații cu instituțiile, organele, oficiile și agențiile Uniunii cu privire la amenințările cibernetice, vulnerabilitățile și incidentele legate de infrastructura TIC neclasificată și, atunci când este necesar, să prezinte IICB propuneri specifice de orientări și recomandări adresate instituțiilor, organelor, oficiilor și agențiilor Uniunii. CERT-UE ar trebui să coopereze și să facă schimb de informații cu omologii din statele membre, inclusiv prin intermediul rețelei CSIRT.

Nivelul operațional

35. În conformitate cu Directiva (UE) 2022/2555, EU-CyCLONe ar trebui să servească drept platformă de cooperare între autoritățile de gestionare a crizelor cibernetice din statele membre și, prin intermediul Comisiei, cu entitățile relevante ale Uniunii, cu scopul de a spori nivelul de pregătire pentru gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor cibernetice și de a dezvolta o conștientizare comună a situației în ceea ce privește incidentele de securitate cibernetică de mare amploare și crizele cibernetice.

36. În conformitate cu Directiva (UE) 2022/2555 și cu Regulamentul (UE) 2024/2847, ENISA primește informații cu privire la incidentele transfrontaliere semnificative și la vulnerabilitățile și incidentele exploatate în mod activ care afectează produsele digitale. Acționând în calitate de secretariat, ENISA ar trebui să consilieze rețeaua CSIRT și EU-CyCLONe cu scopul de a ajuta rețelele să stabilească dacă ar trebui luate măsuri suplimentare și pentru a contribui la conștientizarea comună a situației.

Nivelul politic

37. Statele membre și entitățile relevante ale Uniunii ar trebui să monitorizeze evoluțiile internaționale care afectează securitatea cibernetică [inclusiv amenințările cibernetice, amenințările hibride și acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI), inclusiv dezinformarea, după caz]. Ar trebui să se țină seama de inițiative precum rapoartele comune de evaluare cibernetică, analizele furnizate de SIAC și alte produse relevante care oferă informații specializate.

38. Înaltul Reprezentant ar trebui să continue să informeze și să implice statele membre în eforturile diplomatice ale Uniunii legate de amenințările cibernetice, în special de cele care implică actori statali, de colaborarea sa cu țări terțe și organizații internaționale, inclusiv NATO, și de punerea în aplicare de măsuri diplomatice, inclusiv de măsuri restrictive.

39. Președinția Consiliului Uniunii Europene poate crea o pagină de monitorizare pe platforma web a IPCR unde statele membre și instituțiile și organismele UE pot face schimb de informații cu privire la o posibilă criză în desfășurare.

Exerciții comune

40. Comisia, în coordonare cu Înaltul Reprezentant, sprijinită de ENISA, după consultarea EU-CyCLONe și a rețelei CSIRT, ar trebui să elaboreze un program anual continuu eficient de exerciții cibernetice în vederea pregătirii pentru crizele cibernetice și a creșterii eficienței organizaționale. Programul continuu de exerciții cibernetice ar trebui să țină seama de exercițiile UCPM și de alte exerciții ale mecanismelor de răspuns la situații de criză la nivelul Uniunii, inclusiv de exercițiul prezentat în Planul de acțiune al UE pentru infrastructura critică. Primul program continuu ar trebui elaborat în termen de 12 luni de la adoptarea Planului de acțiune pentru gestionarea crizelor cibernetice, programele ulterioare urmând să fie finalizate până la data de 31 martie a fiecărui an. Programul continuu ar trebui transmis Consiliului spre informare.

41. Programul continuu ar trebui să acopere și exercițiile elaborate utilizând scenariile de evaluare a riscurilor coordonate la nivelul UE. El ar trebui să acopere exerciții care implică toți actorii relevanți, în special sectorul privat și NATO.

42. ENISA, acționând în calitate de secretariat al rețelei CSIRT și al EU-CyCLONe, ar trebui să asigure colectarea sistematică a învățămintelor desprinse din exerciții, precum și identificarea și propunerea de modalități de punere în aplicare a acțiunilor rezultate, pentru a garanta executarea lor efectivă și impactul pozitiv asupra rezilienței comune a UE, inclusiv asupra PSO respective.

43. Toți actorii și toate rețelele ar trebui să îmbunătățească coordonarea în cazul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice pe baza învățămintelor desprinse în urma exercițiilor. În special, EU-CyCLONe și rețeaua CSIRT ar trebui să abordeze provocările identificate în timpul exercițiilor pentru a îmbunătăți coordonarea, mai ales cele referitoare la cooperarea dintre rețele și, dacă este necesar, să adapteze rapid PSO.

44. Grupul de cooperare NIS ar trebui să invite rețeaua CSIRT, EU-CyCLONe și ENISA să prezinte învățăminte desprinse în urma exercițiilor, precum și identificarea și modalitatea propusă de punere în aplicare a acțiunilor rezultate.

45. Consiliul îi poate invita pe președintele rețelei CSIRT, al EU-CyCLONe, al Grupului de cooperare NIS și al ENISA să prezinte modul în care au fost puse în aplicare învățămintele desprinse în urma exercițiilor.

46. ENISA, în cooperare cu Comisia și cu Înaltul Reprezentant, este invitată să organizeze un exercițiu pentru a testa Planul de acțiune pentru gestionarea crizelor cibernetice în cursul următorului exercițiu „Cyber Europe". Exercițiul ar trebui să implice toți actorii relevanți, inclusiv nivelul politic. ENISA este invitată să coordoneze, împreună cu președinția Consiliului Uniunii Europene, implicarea nivelului politic. Exercițiul poate include, de asemenea, sectorul privat și NATO.

VI: Detectarea unui incident care ar putea escalada, transformându-se într-un incident de securitate cibernetică de mare amploare sau într-o criză cibernetică

47. Toți actorii ar trebui să furnizeze rețelelor relevante, în conformitate cu mandatele lor și pe baza unei abordări care ține seama de toate riscurile, informații care indică un potențial incident de securitate cibernetică de mare amploare sau o potențială criză cibernetică.

48. În conformitate cu Regulamentul (UE) 2025/38[13], în cazul în care centrele cibernetice transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în desfășurare, acestea ar trebui să se asigure, în scopul conștientizării comune a situației, că sunt furnizate informații relevante autorităților statelor membre și Comisiei prin intermediul EU-CyCLONe și al rețelei CSIRT, fără întârzieri nejustificate.

[13] Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului din 19 decembrie 2024 de stabilire a unor măsuri de consolidare a solidarității și a capacităților la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea și de modificare a Regulamentului (UE) 2021/694 (Regulamentul privind solidaritatea cibernetică), JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49. Atunci când se observă un incident semnificativ, mai ales dacă are un impact imediat, acesta ar putea fi notificat unei echipe CSIRT sau detectat de aceasta, precum și de autoritățile de gestionare a crizelor cibernetice ale statelor membre sau de alte autorități sectoriale. Statele membre sunt încurajate să facă schimb de informații referitoare la un astfel de incident în cadrul rețelelor, care ar trebui să aibă în vedere luarea de măsuri adecvate. Activarea rețelei CSIRT și a EU-CyCLONe pot fi independente una de cealaltă, în funcție de natura incidentului și de răspunsul necesar. Ambele rețele sunt însă încurajate să continue cooperarea reciprocă pe baza modalităților procedurale convenite. Decizia de activare revine exclusiv și independent fiecărei rețele în parte.

50. Rețeaua CSIRT ar trebui să consilieze EU-CyCLONe în legătură cu posibilitatea ca un incident de securitate cibernetică observat să fie considerat un incident de securitate cibernetică de mare amploare potențial sau în desfășurare.

51. Astfel cum se precizează în Directiva (UE) 2022/2555, rețeaua CSIRT și EU-CyCLONe ar trebui să convină fără întârziere modalități procedurale în cazul unui incident de securitate cibernetică de mare amploare potențial sau în desfășurare, pentru a asigura coordonarea tehnico-operațională și furnizarea în timp util de informații relevante nivelului politic.

VII: Răspunsul la un incident de securitate cibernetică de mare amploare sau la o criză cibernetică la nivelul Uniunii

Răspunsul la un incident de securitate cibernetică de mare amploare sau la o criză cibernetică pentru care IPCR nu este activat în modul „activare integrală”

52. Un răspuns eficace la incidentele de securitate cibernetică de mare amploare sau la crizele cibernetice la nivelul UE depinde de o cooperare tehnică, operațională și politică eficace în cadrul unei abordări la nivelul întregii administrații, care include, acolo unde este posibil, autoritățile de aplicare a legii.

53. La fiecare nivel, actorii implicați ar trebui să desfășoare activități specifice pentru a realiza o conștientizare comună a situației și un răspuns coordonat. Aceste măsuri asigură difuzarea ordonată și eficace a informațiilor.

54. Răspunsul ar trebui să fie adecvat impactului incidentului de securitate cibernetică de mare amploare sau al crizei cibernetice. În conformitate cu Directiva (UE) 2022/2555, autoritățile de gestionare a crizelor cibernetice din statele membre ar trebui să asigure coerența și coordonarea la nivel național între răspunsurile sectoriale la criza cibernetică.

55. În cazul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice, toți actorii și toate rețelele ar trebui să răspundă în strânsă coordonare după cum urmează:

(a) la nivel tehnic:

i. statele membre afectate și echipele lor CSIRT ar trebui să coopereze cu entitățile afectate pentru a răspunde la incidente și pentru a oferi asistență, după caz;

ii. echipele CSIRT ar trebui să coopereze prin intermediul rețelei CSIRT pentru a face schimb de informații tehnice relevante cu privire la incident; echipele CSIRT cooperează în eforturile lor de a analiza elementele tehnice disponibile și alte informații tehnice legate de incident în vederea stabilirii cauzei și a posibilelor măsuri tehnice de atenuare;

iii. atunci când o echipă CSIRT sau o autoritate de gestionare a crizelor cibernetice a unui stat membru ia cunoștință de un incident semnificativ, acestea sunt încurajate să facă schimb de informații în cadrul rețelei CSIRT sau al EU-CyCLONe.

iv. rețeaua CSIRT, cu sprijinul ENISA, ar trebui să pregătească o sinteză a rapoartelor naționale furnizate de CSIRT, care ar trebui prezentată EU-CyCLONe;

v. atunci când un incident de securitate cibernetică are potențialul de a escalada, transformându-se într-un incident de securitate cibernetică de mare amploare sau într-o criză cibernetică, rețeaua CSIRT ar trebui să facă schimb de informații relevante cu EU-CyCLONe. EU-CyCLONe ar trebui să utilizeze aceste informații pentru a informa Consiliul;

vi. rețeaua CSIRT ar trebui să mențină o strânsă legătură cu Europol pentru a asigura schimbul de informații tehnice relevante. Rețeaua CSIRT și Europol ar trebui să stabilească puncte de contact pentru a îmbunătăți schimbul de informații atunci când este relevant în cazul unui incident de securitate cibernetică de mare amploare;

(b) la nivel operațional:

i. statele membre ar trebui să atenueze impactul incidentului la nivel național, luând măsuri adecvate;

ii. rețeaua CSIRT ar trebui să furnizeze EU-CyCLONe evaluări tehnice ale incidentelor în desfășurare, care să poată fi utilizate de EU-CyCLONe;

iii. EU-CyCLONe ar trebui să evalueze consecințele și impactul incidentelor de securitate cibernetică de mare amploare și ale crizelor cibernetice relevante și să propună posibile măsuri de atenuare, să sprijine gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor cibernetice, precum și să sprijine procesul decizional la nivel politic;

iv. în cazul în care un incident de securitate cibernetică de mare amploare cu impact transsectorial necesită activarea de acțiuni de răspuns la nivelul Uniunii, în special a mecanismelor de gestionare a crizelor orizontale și sectoriale relevante la nivelul Uniunii enumerate în anexa II,

(a) actorii în cauză pot, în funcție de tipul de mecanisme sectoriale de gestionare a crizelor la nivelul Uniunii, să solicite activarea mecanismului menționat;

(b) în cazul activării unui astfel de mecanism sectorial, entitățile relevante sprijină entitățile sectoriale în atenuarea impactului incidentului;

(c) Comisia ar trebui să faciliteze fluxul de informații necesare între punctele de contact pentru mecanismele orizontale și sectoriale relevante de gestionare a crizelor la nivelul Uniunii enumerate în anexa II și EU-CyCLONe și ar trebui să efectueze o analiză transsectorială integrată, precum și să propună opțiuni pentru un plan de răspuns integrat adecvat;

(d) Comisia, prin intermediul EU-CyCLONe, după caz, în cooperare cu Înaltul Reprezentant, ar trebui să asigure coerența și coordonarea măsurilor operaționale la nivelul UE în domeniul cibernetic cu acțiunile de răspuns conexe la nivelul Uniunii, în special în ceea ce privește cererile de asistență prin intermediul UCPM;

(e) în cazul în care a fost creată o pagină IPCR de monitorizare, informațiile despre incident, impactul acestuia și măsurile luate ar trebui, de asemenea, să fie transmise statelor membre și entităților Uniunii prin intermediul platformei web a IPCR;

v. statele membre pot solicita servicii din rezerva UE pentru securitate cibernetică în conformitate cu articolul 15 din Regulamentul (UE) 2025/38. Fără a aduce atingere niciunui viitor act de punere în aplicare în temeiul regulamentului respectiv, serviciile din rezerva UE pentru securitate cibernetică ar trebui să fie mobilizate în termen de 24 de ore de la solicitare.

(c) la nivel politic:

i. Consiliul poate solicita informări din partea principalelor părți interesate, în special din partea Comisiei, a Înaltului Reprezentant și a EU-CyCLONe, pentru a oferi un răspuns politic și strategic adecvat;

ii. Consiliul, sprijinit de Comisie și de Înaltul Reprezentant, ar putea decide cu privire la măsurile adecvate pentru a răspunde incidentului de securitate cibernetică de mare amploare, inclusiv cu privire la posibilele răspunsuri diplomatice în conformitate cu capitolul IX;

iii. statele membre pot activa mecanisme sau instrumente suplimentare de gestionare a crizelor cibernetice, în funcție de natura și impactul incidentului;

iv. atunci când IPCR este activat în modul „schimb de informații”, se declanșează capacitatea de sprijin pentru ISAA, sporind schimburile de informații prin intermediul platformei web a IPCR și asigurând o imagine de ansamblu situațională comună. Rapoartele asupra situației ale EU-CyCLONe și ale rețelei CSIRT ar trebui să rămână principalele instrumente care prezintă conștientizarea comună a situației la nivel operațional și, respectiv, tehnic. Aceste rapoarte pot sta la baza rapoartelor ISAA;

v. în cazul unui incident care necesită activarea acțiunilor de răspuns la nivelul Uniunii, în special a mecanismelor orizontale și sectoriale relevante de gestionare a crizelor la nivelul Uniunii enumerate în anexa II, Consiliul, în cooperare cu Comisia și cu Înaltul Reprezentant, ar trebui să asigure coerența și coordonarea între răspunsurile la criza cibernetică și acțiunile conexe de răspuns la nivelul Uniunii;

vi. atunci când sunt solicitate mecanisme relevante, în special serviciile rezervei pentru securitate cibernetică, serviciile Comisiei și, după caz, SEAE, precum și organismele relevante ale Consiliului, în special HWPCI și Grupul de lucru orizontal pentru sporirea rezilienței și contracararea amenințărilor hibride (HWP-ERCHT), după caz, ar trebui să se coordoneze în ceea ce privește conceperea și punerea în aplicare a măsurilor, precum și procesul decizional adecvat însoțit de măsuri suplimentare, în concordanță cu setul de instrumente pentru contracararea amenințărilor hibride[14] în cazul activităților cibernetice răuvoitoare care fac parte dintr-o campanie hibridă mai amplă.

Răspunsul la un incident de securitate cibernetică de mare amploare sau la o criză cibernetică pentru care IPCR este activat în modul „activare integrală”

56. Ar trebui puse în aplicare etapele enumerate în secțiunea „Răspunsul la un incident de securitate cibernetică de mare amploare sau la o criză cibernetică pentru care IPCR nu este activat în modul «activare integrală»” de mai sus.

57. Atunci când IPCR este activat în modul „activare integrală”, rapoartele ISAA servesc la asigurarea unei conștientizări comune a situației la nivel politic. Rapoartele asupra situației ale EU-CyCLONe și ale rețelei CSIRT ar trebui să rămână principalele instrumente care prezintă conștientizarea comună a situației la nivel operațional și, respectiv, tehnic. Aceste rapoarte pot sta la baza rapoartelor ISAA.

58. În cazul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice care are ca rezultat activarea IPCR în modul „activare integrală”, toți actorii ar trebui să răspundă în strânsă coordonare printr-o abordare la nivelul întregii administrații, după cum urmează:

(a) coordonarea răspunsului la nivelul politic al Uniunii se realizează de către Consiliu, prin intermediul mecanismului IPCR;

---

14 Setul de instrumente pentru contracararea amenințărilor hibride este un cadru pentru un răspuns coordonat la campaniile hibride care afectează UE și statele sale membre, cadru care cuprinde, de exemplu, măsuri preventive, de cooperare, de stabilitate, restrictive și de redresare și sprijină solidaritatea și asistența reciprocă.

(b) EU-CyCLONe, în cooperare cu rețeaua CSIRT, ar trebui să furnizeze nivelului politic informații clare cu privire la impactul, posibilele consecințe și măsurile de răspuns și de remediere a incidentului, inclusiv prin contribuția la rapoartele ISAA;

(c) pe lângă capacitatea pentru analiza și conștientizarea integrată a situației, președinția Consiliului Uniunii Europene ar urma să convoace mese rotunde ale IPCR pentru a permite coordonarea politică și strategică a răspunsului UE, acțiunile din cadrul Planului de acțiune pentru gestionarea crizelor cibernetice și activitatea mecanismelor sectoriale relevante contribuind la activitatea IPCR. În plus, mesele rotunde pot identifica unele lacune specifice în răspuns și pot invita anumiți actori din UE să le remedieze și să raporteze în cadrul următoarelor mese rotunde, pentru a sprijini coordonarea politică și strategică în cadrul IPCR;

(d) președinția Consiliului Uniunii Europene ar trebui să aibă în vedere invitarea EU-CyCLONe la reuniunile relevante, inclusiv la mese rotunde în cadrul mecanismului IPCR și la alte reuniuni relevante ale Consiliului;

(e) autoritățile de gestionare a crizelor din statele membre, sprijinite de autoritățile de gestionare a crizelor cibernetice, ar trebui să asigure coerența și coordonarea între răspunsurile sectoriale la criza cibernetică;

(f) posibilele răspunsuri diplomatice ar trebui avute în vedere și aplicate în conformitate cu capitolul IX.

VIII: Eforturi de comunicare publică

59. Deși comunicarea către populația unui anumit stat membru cu privire la un incident de securitate cibernetică de mare amploare sau o criză cibernetică în desfășurare, inclusiv ca parte a acțiunilor de sensibilizare, este o competență națională, statele membre, Comisia și Înaltul Reprezentant ar trebui să urmărească coordonarea comunicării lor publice în măsura posibilului. Rețeaua informală de comunicatori în situații de criză a IPCR poate fi implicată, după caz.

60. În vederea pregătirii pentru incidentele de securitate cibernetică de mare amploare și pentru crizele cibernetice, statele membre și, după caz, Comisia și CERT-UE sunt invitate să facă schimb de opinii cu privire la eforturile lor de comunicare în cadrul EU-CyCLONe și al rețelei CSIRT, inclusiv cu privire la bunele practici, cum ar fi recomandările publice sau campaniile de sensibilizare. ENISA ar trebui să pună la dispoziție instrumente care să sprijine un astfel de schimb de opinii și să asigure un acces facil.

61. În cazul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice, statele membre sunt invitate să facă schimb de informații în cadrul EU-CyCLONe cu privire la eforturile lor de comunicare publică pentru a realiza o conștientizare comună și a coordona acțiunile. Din proprie inițiativă sau la solicitarea Consiliului, EU-CyCLONe poate transmite Consiliului o prezentare generală a acestor abordări.

IX: Răspunsul diplomatic și cooperarea cu partenerii strategici

62. Înaltul Reprezentant, în strânsă cooperare cu Comisia și cu alte entități relevante ale Uniunii, ar trebui:

(a) să sprijine procesul decizional din cadrul Consiliului, inclusiv prin analize, rapoarte și propuneri, cu privire la luarea de posibile măsuri ca parte a setului de instrumente al UE pentru diplomația cibernetică. Acest lucru va permite utilizarea întregului spectru de instrumente ale Uniunii disponibile pentru a preveni, a descuraja și a răspunde la activitățile cibernetice răuvoitoare, consolidându-și postura de securitate cibernetică și promovând pacea, securitatea și stabilitatea internațională în spațiul cibernetic;

(b) în cazul în care se identifică un incident relevant, să faciliteze fluxul de informații necesare cu partenerii strategici, inclusiv cu NATO, când este cazul;

(c) să intensifice coordonarea cu partenerii strategici, inclusiv cu NATO, când este cazul, în ceea ce privește răspunsul la activități cibernetice răuvoitoare inițiate de actori care generează amenințări persistente, în special atunci când se utilizează setul UE de instrumente pentru diplomația cibernetică, în conformitate cu orientările de punere în aplicare.

63. Statele membre, Înaltul Reprezentant, Comisia și alte entități relevante ale Uniunii ar trebui să coopereze cu partenerii strategici și cu organizațiile internaționale pentru a promova bunele practici și comportamentul responsabil al statelor în spațiul cibernetic și pentru a asigura un răspuns rapid și coordonat în cazul unor incidente de securitate cibernetică potențiale sau de mare amploare.

64. Cooperarea dintre Uniunea Europeană și NATO ar trebui să se desfășoare în conformitate cu principiile directoare convenite privind incluziunea, reciprocitatea și transparența și cu respectarea deplină a procesului decizional autonom al Uniunii.

65. Comisia și Înaltul Reprezentant, ținând seama de acordurile existente, cum ar fi acordul tehnic dintre CERT-UE și NATO din 2016, ar trebui să stabilească puncte de contact pentru coordonarea cu NATO pentru ca în cazul unei crize cibernetice să facă schimb de informații necesare cu privire la situație și la utilizarea mecanismelor de răspuns în situații de criză pentru a intensifica cooperarea privind răspunsul, precum și eficacitatea acestuia. În acest scop, Uniunea ar trebui să exploreze modalități de îmbunătățire a schimbului de informații cu NATO, într-un mod incluziv, reciproc și nediscriminatoriu, în special prin asigurarea de instrumente de comunicare securizată, ținând seama, în același timp, de standardele în materie de schimb de informații ale diferitelor state membre.

66. Ca parte a programului continuu de exerciții cibernetice al Uniunii menționat în capitolul V de mai sus, serviciile Comisiei și SEAE ar trebui să aibă în vedere organizarea unui exercițiu la nivel de personal cu NATO pentru a testa cooperarea dintre entitățile civile și militare în cazul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice, în situația în care statele membre sau aliații NATO intenționează să răspundă unui atac cibernetic care le afectează securitatea. Exercițiul ar trebui să se desfășoare într-un mod incluziv și nediscriminatoriu și cu respectarea deplină a principiilor convenite ale parametrilor cooperării UE-NATO. Exercițiul ar trebui să se desfășoare în cadrul exercițiului „EU Integrated Resolve” (exercițiu paralel și coordonat, „PACE”). Ar trebui luate toate măsurile necesare pentru a asigura participarea tuturor actorilor menționați în Planul de acțiune pentru gestionarea crizelor cibernetice.

67. De asemenea, ar trebui avute în vedere exerciții cibernetice comune la nivelul Uniunii cu țările din Balcanii de Vest, Republica Moldova, Ucraina, precum și cu alți parteneri strategici și țări terțe care au aceeași viziune, în consultare cu Consiliul, Comisia și Înaltul Reprezentant.

X. Coordonarea gestionării crizelor cibernetice cu actorii militari la nivelul UE

68. Statele membre ar trebui să continue să consolideze cooperarea dintre actorii cibernetici civili și militari la nivel național.

69. EU-CyCLONe și rețeaua CSIRT ar trebui să identifice posibile modalități și proceduri de cooperare cu actorii militari relevanți ai UE, cum ar fi Conferința comandanților cibernetici ai UE și Rețeaua operațională a echipelor militare de intervenție în caz de incidente de securitate informatică (MICNET), pentru a beneficia de o perspectivă militară și civilă comună, în special prin reuniuni comune. EU-CyCLONe și rețeaua CSIRT ar trebui să informeze Consiliul cu privire la progresele înregistrate în ceea ce privește o astfel de cooperare.

70. Statul membru afectat este invitat să informeze EU-CyCLONe, precum și SEAE, în cazul în care sunt utilizate capabilități de răspuns militar naționale sau multinaționale relevante în contextul unui incident de securitate cibernetică de mare amploare sau al unei crize cibernetice, iar furnizarea acestor informații este convenită de comun acord între utilizatorul și furnizorul unei astfel de capabilități de răspuns.

71. Ca parte a programului continuu de exerciții cibernetice al Uniunii menționat în capitolul V de mai sus, Comisia și Înaltul Reprezentant ar trebui să aibă în vedere organizarea unui exercițiu comun pentru a testa cooperarea dintre actorii cibernetici civili și militari în cazul unui incident de securitate cibernetică de mare amploare care afectează statele membre.

XI: Redresarea și învățămintele desprinse în urma unei crize cibernetice

72. Statele membre, entitățile și rețelele relevante ale Uniunii ar trebui să colaboreze în faza de redresare după o criză cibernetică pentru a asigura restabilirea rapidă a funcționalităților de bază. Dacă este cazul, și comunitățile de aplicare a legii ar trebui să fie implicate într-o astfel de cooperare. În această etapă, cooperarea cu sectorul privat este esențială, în special pentru facilitarea recuperării datelor și a restabilirii sistemelor. Coordonarea eficace între părțile interesate ar trebui să acorde prioritate reducerii la minimum a perturbărilor și asigurării continuității activității.

73. Statele membre, entitățile și rețelele relevante ale Uniunii ar trebui să colaboreze în etapa de redresare, valorificând învățămintele desprinse din crizele cibernetice sau din incidentele de securitate cibernetică gestionate în trecut, precum și din rapoartele privind incidentele, în special în contextul mecanismului european de analiză a incidentelor de securitate cibernetică instituit prin Regulamentul (UE) 2025/38.

74. EU-CyCLONe ar trebui să pună la dispoziția rețelei CSIRT, a Grupului de cooperare NIS și a Consiliului o listă cuprinzătoare de învățăminte desprinse din crizele cibernetice sau din incidentele de securitate cibernetică gestionate în trecut, precum și de bune practici. ENISA ar trebui să se asigure că aceste învățăminte desprinse sunt reflectate în mod adecvat în viitoarele activități de pregătire și atunci când se are în vedere planificarea exercițiilor viitoare.

XII: Comunicare securizată

75. Pe baza cartografierii instrumentelor de comunicare securizată existente[15], Comisia ar trebui să propună, până la sfârșitul anului 2026, un set interoperabil de soluții de comunicare securizată. Consiliul, Comisia, Înaltul Reprezentant, EU-CyCLONe și rețeaua CSIRT ar trebui să convină asupra acestui set până la sfârșitul anului 2027. Aceste soluții ar trebui să beneficieze de pe urma acțiunilor în domeniul comunicării securizate pe care instituțiile UE le-ar putea întreprinde în cadrul Strategiei UE privind o uniune a pregătirii pentru situații de criză și ar trebui să acopere întreaga gamă de moduri de comunicare necesare (voce, date, videoteleconferință, mesagerie, colaborare și schimb de documente și consultare). Soluțiile ar trebui să îndeplinească cerințe definite în comun pentru protecția informațiilor sensibile neclasificate. Ar trebui utilizate soluții bazate pe un protocol deschis cu aplicări cu sursă deschisă adecvate pentru comunicarea în timp real, gestionate de o entitate cu sediul în UE.

76. Dacă este necesar, în scopul schimbului de informații clasificate RESTREINT UE/EU RESTRICTED, EU-CyCLONe și rețeaua CSIRT ar trebui să poată utiliza canale de comunicare securizate asigurate pentru instituțiile, organele și agențiile UE pentru schimbul de informații clasificate între ele și cu statele membre.

[15] WK 862/2023.

77. Fără a aduce atingere viitorului cadru financiar multianual, Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) instituit în temeiul Regulamentului (UE) 2021/887[16] ar trebui să aibă în vedere finanțarea prin intermediul programului „Europa digitală” pentru a sprijini statele membre în implementarea de instrumente de comunicare securizată. Ar trebui evitată orice suprapunere a investițiilor în sisteme securizate interoperabile.

78. În special, entitățile UE și statele membre ar trebui să elaboreze planuri pentru situații neprevăzute în cazul crizelor grave în care canalele normale de comunicare care se bazează pe internet sau pe rețele de telecomunicații sunt perturbate sau indisponibile.

79. Pentru un răspuns eficace în situații de criză cibernetică ar trebui create mecanisme de comunicare și de schimb de informații între autoritățile de aplicare a legii și rețelele de securitate cibernetică, în special la nivel tehnic. Aceste mecanisme ar trebui să respecte rolul fiecărei părți și să evite interferența cu operațiunile în curs, precum și să garanteze redundanța comunicării. Sistemul UE de comunicații critice (EUCCS), aflat în prezent în curs de dezvoltare, poate aduce beneficii răspunsului comun cu comunitățile cibernetice relevante.

XIII: Dispoziții finale

80. EU-CyCLONe, în cooperare cu rețeaua CSIRT și cu alți actori principali din ecosistemul UE de gestionare a crizelor cibernetice, cu sprijinul ENISA, ar trebui să elaboreze, în termen de un an de la publicarea recomandării, diagrame detaliate ale proceselor care să prezinte fluxurile de informații dintre actorii relevanți, procesele decizionale și rapoartele elaborate în timpul gestionării incidentelor de securitate cibernetică de mare amploare sau a crizelor cibernetice, astfel cum sunt descrise în prezenta recomandare. Diagramele ar trebui să acopere diferite moduri și niveluri de cooperare. Ele ar trebui actualizate atunci când este necesar.

[16] Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare, JO L 202, 8.6.2021, p. 1.

81. Pentru a sprijini aplicarea eficace a Planului de acțiune revizuit pentru gestionarea crizelor cibernetice și pe baza experienței dobândite prin exercițiile cibernetice comune desfășurate în cadrul acestuia, Consiliul poate elabora, dacă este necesar, un set de orientări de punere în aplicare. Aceste orientări ar putea aborda provocările practice identificate în cursul exercițiilor și ar putea elimina lacunele și verigile lipsă identificate în ceea ce privește coordonarea, comunicarea și interacțiunea operațională.

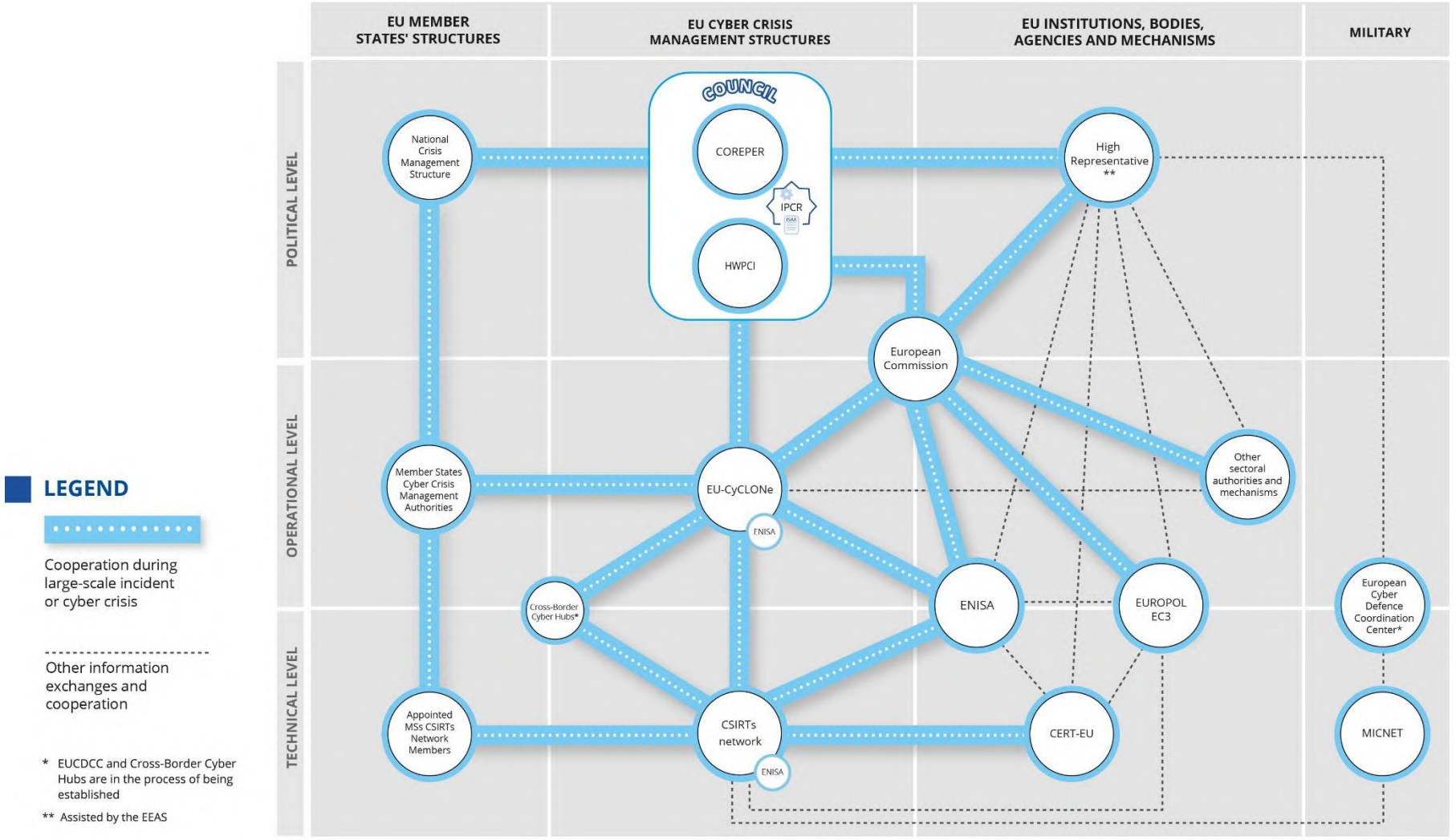
82. Prezenta recomandare ar trebui revizuită de Comisie în cooperare cu statele membre, cel puțin o dată la patru ani după publicarea sa. După fiecare revizuire, Comisia ar trebui să publice un raport și să îl prezinte Consiliului. Comisia și statele membre ar trebui să țină seama în mod special de impactul evoluției peisajului amenințărilor, de rezultatele exercițiilor comune și de modificările legislative – în special de eventualele modificări care decurg din revizuirea Regulamentului (UE) 2019/881.

Adoptată la Bruxelles,

Pentru Consiliu

Președintele

ANEXA I – Planul de acțiune al Uniunii de răspuns la o criză de securitate cibernetică



ANEXA II – ACTORII RELEVANȚI DE LA NIVELUL UNIUNII (ENTITĂȚI ȘI REȚELE) ȘI MECANISMELE DE GESTIONARE A CRIZELOR

(1) Implicarea principalilor actori pe tot parcursul ciclului de viață al gestionării crizelor cibernetice (incidente de securitate cibernetică de mare amploare și crize cibernetice)

	Pregătire	Detectare	Răspunsul la un incident de securitate cibernetică de mare amploare sau la o criză cibernetică			Comunicare publică	Redresarea și învățămintele desprinse
			la nivel tehnic	la nivel operațional	la nivel politic		
Statele membre	X	X	X	X	X	X	X
Comisia	X			X	X	X	
Înaltul Reprezentant, asistat de SEAE	X			X	X	X	
Consiliul	X				X	X	X
ENISA	X		X	X			
CERT-UE	X	X	X	X		X	X
Rețeaua CSIRT	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Rolurile și competențele actorilor relevanți de la nivelul Uniunii și mecanismele (în ordine alfabetică) legate de gestionarea crizelor cibernetice

Actor	Nivel	Rol și competență	Referință
CERT-UE	Tehnic/operațional	Coordonează răspunsul la situații de criză la nivel tehnic și gestionarea incidentelor majore care afectează entitățile Uniunii. Menține un inventar al expertizei tehnice disponibile necesare pentru răspunsul la incidente în cazul unor incidente majore și sprijină IICB în coordonarea planurilor de gestionare a crizelor cibernetice ale entităților Uniunii pentru incidentele majore. Membru al rețelei CSIRT. Sprijină Comisia în cadrul EU-CyCLONe în ceea ce privește gestionarea coordonată a incidentelor de securitate cibernetică de mare amploare și a crizelor. Acționează ca centru de schimb de informații în materie de securitate cibernetică și de coordonare a răspunsului la incidente, facilitând schimbul de informații privind incidentele, amenințările cibernetice, vulnerabilitățile și	Regulamentul (UE, Euratom) 2023/2841 Regulamentul (UE) 2025/38

Actor	Nivel	Rol și competență	Referință
		incidentele evitate la limită între entitățile Uniunii și omologii lor. Solicită implementarea rezervei UE pentru securitate cibernetică în numele entităților Uniunii. Cooperează cu Centrul de securitate cibernetică al NATO pe baza acordului tehnic dintre acestea.	
Consiliul Uniunii Europene	Politic	Funcții de definire a politicilor și de coordonare. I se încredințează IPCR, care vizează coordonarea și răspunsul la nivelul politic al Uniunii.	Articolul 16 din Tratatul privind Uniunea Europeană
Președinția Consiliului Uniunii Europene	Politic	Decide (cu excepția cazului în care este invocată clauza de solidaritate în temeiul articolului 222 din Tratatul privind funcționarea Uniunii Europene) dacă să activeze IPCR, în consultare cu statele membre afectate, după caz, precum și cu Comisia și ÎR.	Articolul 16 din Tratatul privind Uniunea Europeană Decizia de punere în aplicare (UE) 2018/1993 a Consiliului
Centrele cibernetice transfrontaliere	Tehnic	Un centru cibernetic transfrontalier este o platformă multinațională instituită printr-un acord de consorțiu scris care reunește într-o structură coordonată de rețea centre	Regulamentul (UE) 2025/38

Actor	Nivel	Rol și competență	Referință
		cibernetice naționale din cel puțin trei state membre și care este concepută pentru a consolida monitorizarea, detectarea și analizarea amenințărilor cibernetice și a preveni incidentele și pentru a sprijini producerea de informații privind amenințările cibernetice, în special prin schimbul de date și informații relevante, anonimizate dacă este cazul, precum și prin utilizarea în comun a instrumentelor de ultimă generație și dezvoltarea în comun a capacităților de detectare, de analiză și prevenire și de protecție în domeniul cibernetic într-un mediu de încredere; Cooperează strâns cu rețeaua CSIRT pentru a face schimb de informații. Furnizează informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în desfășurare autorităților statelor membre și Comisiei prin intermediul EU-CyCLONe și al rețelei CSIRT.	

Actor	Nivel	Rol și competență	Referință
Rețeaua CSIRT	Tehnic	Contribuie la dezvoltarea încrederii și promovează o cooperare operațională rapidă între statele membre. Este principala rețea pentru schimbul de informații relevante privind incidentele, incidentele evitate la limită, amenințările cibernetice, riscurile și vulnerabilitățile. La cererea unui membru potențial afectat de un incident, rețeaua face schimb de informații și poartă discuții cu privire la incidentul respectiv și la amenințările cibernetice asociate. Rețeaua poate, de asemenea, să faciliteze un răspuns coordonat la un incident care a fost identificat în jurisdicția unui membru solicitant. Furnizează asistență statelor membre în gestionarea incidentelor transfrontaliere și explorează noi forme de cooperare, inclusiv în legătură cu asistența reciprocă. Primește informații de la statele membre cu privire la cererile	Directiva (UE) 2022/2555 Regulamentul (UE) 2025/38

Actor	Nivel	Rol și competență	Referință
		acestora adresate rezervei UE pentru securitate cibernetică.	
Conferința comandanților cibernetici		Un forum pentru comandanții cibernetici la nivel național din statele membre pentru a colabora și a face schimb de informații vitale cu privire la operațiunile și strategiile în curs din spațiul cibernetic pentru atenuarea efectelor incidentelor cibernetice de mare amploare. Este organizată de președinția prin rotație a Consiliului Uniunii Europene cu sprijinul Agenției Europene de Apărare (AEA) și al Serviciului European de Acțiune Externă (SEAE), inclusiv al Statului-Major al UE (EUMS).	Comunicarea comună privind politica UE în domeniul apărării cibernetice (2022)
Comisia	Operațional/politic	Organul executiv al Uniunii Europene. Asigură buna funcționare a pieței interne. Facilitează coerența acțiunilor conexe de răspuns în situații de criză desfășurate la nivelul Uniunii, precum și coordonarea acestor acțiuni.	Articolul 17 din Tratatul privind Uniunea Europeană Decizia de punere în aplicare (UE) 2018/1993 Decizia nr. 1313/2013/UE

Actor	Nivel	Rol și competență	Referință
		Anumite acțiuni generale de pregătire la nivelul Uniunii în temeiul Deciziei privind UCPM, inclusiv gestionarea Centrului de coordonare a răspunsului la situații de urgență și a sistemului comun de comunicare și informare în caz de urgență. Observator în cadrul EU-CyCLONe și membru în cazul unui incident de mare amploare potențial sau în desfășurare care are sau este probabil să aibă un impact semnificativ asupra serviciilor și activităților care intră în domeniul de aplicare al Directivei (UE) 2022/2555. Observator în cadrul rețelei CSIRT. Responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Punct de contact în cadrul Consiliului interinstituțional pentru securitate cibernetică pentru schimbul de informații relevante cu EU-CyCLONe în legătură cu incidentele majore. Consultată de președinția Consiliului cu privire la deciziile de activare sau dezactivare a IPCR (cu	Directiva (UE) 2022/2555 Regulamentul (UE) 2025/38 Regulamentul (UE, Euratom) 2023/2841

Actor	Nivel	Rol și competență	Referință
		excepția cazului în care este invocată clauza de solidaritate în temeiul articolului 222 din TFUE). Serviciile Comisiei pregătesc, împreună cu SEAE, rapoartele ISAA.	
Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)	Tehnic/operațional	Îndeplinește sarcini în scopul atingerii unui nivel ridicat de securitate cibernetică în întreaga Uniune, inclusiv prin sprijinirea activă a statelor membre și a instituțiilor Uniunii Asigură secretariatul rețelei CSIRT și al EU-CyCLONe. Întocmește periodic un raport asupra situației tehnice în materie de securitate cibernetică la nivelul UE cu privire la incidente și la amenințările cibernetice (împreună cu EC3 și CERT-UE și în strânsă cooperare cu statele membre). Contribuie la dezvoltarea unui răspuns comun la incidentele sau crizele transfrontaliere de mare amploare, în special prin: - agregarea și analizarea rapoartelor din surse naționale;	Directiva (UE) 2022/2555 Regulamentul (UE) 2019/881 Regulamentul (UE) 2025/38 Regulamentul (UE) 2024/2847

Actor	Nivel	Rol și competență	Referință
		- asigurarea fluxului de informații între nivelul tehnic, operațional și politic; - facilitarea gestionării incidentelor, la cerere; - sprijinirea entităților Uniunii în ceea ce privește comunicarea publică; - sprijinirea statelor membre în ceea ce privește comunicarea publică, la cerere; - testarea capacităților de răspuns la incidente și organizarea periodică de exerciții de securitate cibernetică. Acționează în calitate de autoritate contractantă în cazul în care i s-a încredințat sarcina de a asigura funcționarea și de a administra, parțial sau integral, rezerva UE pentru securitate cibernetică. Organizează, o dată la doi ani, un exercițiu cuprinzător de securitate cibernetică la nivelul Uniunii, cu elemente tehnice, operaționale sau strategice. Întocmește un raport de analiză a incidentelor în colaborare cu statul	

Actor	Nivel	Rol și competență	Referință
		membru în cauză și cu alte părți interesate relevante, pentru a evalua cauzele, impactul și atenuarea unui incident (la cererea Comisiei sau a EU-CyCLONe și cu aprobarea statului membru în cauză). Informează EU-CyCLONe dacă informațiile furnizate în temeiul obligațiilor de raportare prevăzute în Regulamentul privind reziliența cibernetică sunt relevante pentru gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor.	
Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe)	Operațional	Sprijină gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor Asigură schimbul periodic de informații relevante între statele membre și instituțiile, organele, oficiile și agențiile Uniunii. Coordonează gestionarea incidentelor de securitate cibernetică de mare amploare și a crizelor și sprijină procesul decizional la nivel politic în	Directiva (UE) 2022/2555 Regulamentul (UE) 2025/38

Actor	Nivel	Rol și competență	Referință
		legătură cu astfel de incidente și crize. Evaluează consecințele și impactul incidentelor de securitate cibernetică de mare amploare și crizelor relevante și propune măsuri posibile de atenuare. Discută, la solicitarea unui stat membru în cauză, planurile naționale de răspuns la incidente de securitate cibernetică de mare amploare și crize. Elaborează, împreună cu ENISA și Comisia, modelul menit să faciliteze transmiterea cererilor de sprijin din rezerva UE pentru securitate cibernetică. Primește informații de la statele membre cu privire la cererile acestora adresate rezervei UE pentru securitate cibernetică. Primește informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în desfășurare de la centrele cibernetice transfrontaliere sau de la rețeaua CSIRT.	

Actor	Nivel	Rol și competență	Referință
Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate, sprijinit de Serviciul European de Acțiune Externă	Politic	Conduce și coordonează eforturile Uniunii de a aborda amenințările externe la adresa securității în domeniul hibrid și cibernetic Responsabil pentru diplomația cibernetică și instrumentele de apărare cibernetică ale Uniunii pentru a descuraja amenințările externe și a răspunde la acestea, inclusiv prin utilizarea seturilor de instrumente ale Uniunii pentru contracararea amenințărilor hibride și pentru diplomația cibernetică. Colaborează cu parteneri externi, inclusiv prin implicarea în cadrul PSAC. Asigură pregătirea Uniunii și a statelor membre pentru conștientizarea situației și capacitatea de a reacționa la amenințările hibride și cibernetice, de exemplu prin exerciții practice, formare și rețele. Gestionează implicațiile în materie de securitate și apărare ale activelor spațiale ale Uniunii, în special în cadrul politicii de securitate și apărare comune (PSAC) a Uniunii. Sprijină Conferința comandanților cibernetici ai UE. Sprijină rețeaua operațională a echipelor militare de intervenție în	Decizia 2010/427/UE a Consiliului

Actor	Nivel	Rol și competență	Referință
		caz de incidente de securitate informatică (MICNET) a UE. Este consultat de președinția Consiliului cu privire la deciziile de activare sau dezactivare a IPCR (cu excepția cazului în care este invocată clauza de solidaritate în temeiul articolului 222 din TFUE). SEAE pregătește, împreună cu serviciile Comisiei, rapoartele ISAA.	
Centrul UE de coordonare a apărării cibernetice	Orizontal	Obiectivul său inițial este în principal de a consolida conștientizarea comună a situației de către Uniune și statele sale membre cu privire la activitățile răuvoitoare din spațiul cibernetic, în special în ceea ce privește misiunile și operațiile militare PSAC.	Comunicarea comună privind politica UE în domeniul apărării cibernetice (2022)
Europol	Operațional	Oferă sprijin operațional și tehnic autorităților competente ale statelor membre pentru prevenirea și descurajarea criminalității informatice. Acordă asistență autorităților competente ale statelor membre, la cererea acestora, pentru a răspunde atacurilor cibernetice în privința cărora se bănuiește că au la origine infracțiuni.	Regulamentul (UE) 2016/794, inclusiv toate modificările

Actor	Nivel	Rol și competență	Referință
Consiliul interinstituțional pentru securitate cibernetică		Stabilește un plan de gestionare a crizelor cibernetice pentru a sprijini, la nivel operațional, gestionarea coordonată a incidentelor majore care afectează entitățile Uniunii și pentru a contribui la schimbul periodic de informații relevante. Coordonează adoptarea planurilor individuale de gestionare a crizelor cibernetice ale entităților Uniunii. Adoptă, pe baza unei propuneri a CERT-UE, orientări sau recomandări privind cooperarea în ceea ce privește răspunsul la incidente în cazul incidentelor semnificative care afectează entitățile Uniunii.	Regulamentul (UE, Euratom) 2023/2841
Rețeaua operațională a echipelor militare de intervenție în caz de incidente de securitate informatică (MICNET)	Tehnic	Promovează un răspuns mai solid și mai coordonat la amenințările cibernetice care afectează sistemele de apărare din Uniune, inclusiv cele utilizate în misiunile și operațiile militare din cadrul PSAC; este sprijinită de Agenția Europeană de Apărare.	Comunicarea comună privind apărarea cibernetică din 2022

Actor	Nivel	Rol și competență	Referință
Capacitatea unică de analiză a informațiilor (SIAC)		Alcătuită din (1) Centrul de situații și de analiză a informațiilor al UE (INTCEN UE) și (2) Direcția pentru informații a Statului-Major al UE (EUMS INT). Furnizează informații strategice privind politica externă, terorismul și amenințările cibernetice și hibride. Gestionează informațiile militare pentru misiunile PSAC și sprijină operațiunile de apărare și de gestionare a crizelor ale Uniunii. Sub autoritatea Înaltului Reprezentant.	Articolele 38 și 42-46 din Tratatul privind Uniunea Europeană

(3) Mecanismele și platformele relevante de gestionare a crizelor de la nivelul Uniunii

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
ARGUS	Orizontal	Procesul de coordonare și sistemul general de alertă al Comisiei pentru un răspuns coerent în cazul unei crize transfrontaliere majore care necesită o acțiune la nivelul UE. Reunește toate serviciile și cabinetele relevante pentru a decide cu privire la măsurile necesare și a le coordona. Permite Comisiei să facă schimb de informații relevante cu privire la crizele multisectoriale emergente sau la amenințările previzibile sau iminente care necesită o acțiune la nivelul Uniunii.	Comunicarea Comisiei COM(2005) 662
Centrul de răspuns în situații de criză al SEAE (CRC)	Orizontal	Punctul unic de acces pentru toate aspectele legate de crize din cadrul SEAE și capacitatea permanentă de răspuns în situații de criză 24/7 pentru situații de urgență care amenință siguranța personalului din delegațiile UE și/sau ca reacție la crizele care îi afectează pe cetățenii Uniunii în străinătate. Reunește experți în domeniul securității, consular și al conștientizării situației, bazându-se în același timp pe	O Busolă strategică pentru securitate și apărare – Pentru o Uniune Europeană care își protejează cetățenii, valorile și interesele și contribuie la pacea și securitatea

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
		profesioniști implicați pe teren în delegațiile Uniunii.	internaționale (21 martie 2022)
Planul de acțiune pentru infrastructura critică	Orizontal	Coordonează un răspuns la nivelul Uniunii la perturbările infrastructurii critice cu relevanță transfrontalieră semnificativă.	Recomandarea Consiliului C/2024/4371
Sistemul de alertă în materie de securitate cibernetică	Specific domeniului cibernetic	Asigură capacități avansate ale Uniunii de îmbunătățire a capacităților de detectare, analiză și prelucrare a datelor în ceea ce privește amenințările cibernetice și prevenirea incidentelor în Uniune.	Regulamentul (UE) 2025/38
Setul de instrumente pentru diplomația cibernetică (cadrul privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare)	Specific domeniului cibernetic	Permite un răspuns diplomatic comun al Uniunii la activitățile cibernetice răuvoitoare, care contribuie la prevenirea conflictelor, la atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale.	Concluziile Consiliului din 19 iunie 2017 Orientările revizuite de punere în aplicare 10289/23, 8 iunie 2023
Rezerva UE pentru securitate cibernetică	Specific domeniului cibernetic	Mobilizează experți și resurse în materie de securitate cibernetică în timpul crizelor pentru a sprijini eforturile de răspuns din statele membre, din instituțiile, organele sau agențiile Uniunii	Regulamentul (UE) 2025/38

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
Codul de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică	Sectorial	Instituie un proces recurent de evaluare a riscurilor de securitate cibernetică în sectorul energiei electrice, la nivelul Uniunii, al statelor membre, la nivel regional și la nivelul entităților. Conține dispoziții specifice gestionării crizelor și cooperării cu CSIRT și cu EU-CyCLONe în cazurile în care un incident de securitate cibernetică de mare amploare are un impact asupra altor sectoare care depind de securitatea aprovizionării cu energie electrică.	Regulamentul delegat (UE) 2024/1366 al Comisiei
Setul de instrumente pentru contracararea amenințărilor hibride	Orizontal	Include un set de dispoziții menite să asigure o imagine de ansamblu a ceea ce este disponibil la nivelul UE ca răspuns la toate tipurile de amenințări hibride, utilizarea coordonată a acestora, asigurând coerența acțiunilor noastre în toate domeniile. Setul de instrumente pentru contracararea amenințărilor hibride contribuie la asigurarea faptului că procesul decizional este bazat pe o conștientizare cuprinzătoare a situației și pe lecțiile învățate	Concluziile Consiliului privind un cadru pentru un răspuns coordonat al UE la campaniile hibride, 22 iunie 2022 Orientări privind punerea în aplicare a cadrului pentru un răspuns coordonat al UE la campaniile hibride, 14 decembrie 2022

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
Echipele de răspuns rapid în caz de amenințări hibride (EU HRRT)	Orizontal	Ca parte a setului de instrumente al UE pentru contracararea amenințărilor hibride, echipele UE de răspuns rapid în caz de amenințări hibride se bazează pe expertiza civilă și militară sectorială relevantă de la nivel național și de la nivelul UE pentru a oferi asistență pe termen scurt adaptată și specifică statelor membre, misiunilor și operațiilor din cadrul politicii de securitate și apărare comune, precum și țărilor partenere în ceea ce privește contracararea amenințărilor și campaniilor hibride.	Cadrul de orientare pentru instituirea practică a echipelor UE de răspuns rapid în caz de amenințări hibride (21 mai 2024) Orientări operaționale pentru desfășurarea echipelor de răspuns rapid în caz de amenințări hibride, aprobate de Coreper la 4 decembrie 2024
IPCR	Orizontal	Sprijină un proces decizional rapid și coordonat la nivelul politic al Uniunii pentru crize majore și complexe. Decizia de activare și dezactivare este luată de președinția Consiliului, care consultă (cu excepția cazurilor în care a fost invocată clauza de solidaritate) statele membre afectate, Comisia și ÎR. SGC, serviciile Comisiei și SEAE pot conveni, de asemenea, în consultare cu președinția, să activeze IPCR în modul „schimb de informații”.	Decizia de punere în aplicare (UE) 2018/1993 a Consiliului

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
		Activitățile IPCR se bazează pe rapoartele ISAA elaborate de serviciile Comisiei și de SEAE. Aceste rapoarte se bazează și pe informațiile și analizele relevante furnizate de statele membre (de exemplu, din partea centrelor naționale relevante de gestionare a crizelor) și de agențiile și organele relevante ale Uniunii.	
Protocolul UE privind răspunsul în situații de urgență al autorităților de aplicare a legii	Orizontal	Un instrument de sprijinire a autorităților de aplicare a legii din Uniune în furnizarea unui răspuns imediat la atacurile cibernetice transfrontaliere majore printr-o evaluare rapidă, prin schimbul securizat și în timp util de informații critice și prin coordonarea eficace a aspectelor internaționale ale investigațiilor lor.	Concluziile Consiliului (26 iunie 2018) privind răspunsul coordonat al UE la incidentele și crizele de securitate cibernetică de mare amploare.
Echipele de răspuns rapid în domeniul cibernetic (CRRT) din cadrul cooperării structurate	Specific domeniului cibernetic	PESCO CRRT reprezintă o capacitate de apărare cibernetică civilă și militară a statelor membre ale UE, dezvoltată în comun de acestea, pentru a răspunde rapid	Articolul 42 alineatul (6), articolul 46 și Protocolul nr. 10 la Tratatul

Mecanism	Orizontal/sectorial/specific domeniului cibernetic	Descriere	Referință
permanente (PESCO)		incidentelor și crizelor cibernetice, precum și pentru a întreprinde acțiuni de prevenire, cum ar fi evaluări ale vulnerabilității și monitorizarea alegerilor. Misiunea PESCO CRRT este de a oferi sprijin cibernetic, la cerere, statelor membre ale UE, instituțiilor, organelor și agențiilor UE, misiunilor și operațiilor PSAC militare ale UE, precum și țărilor partenere.	privind Uniunea Europeană.

Arhitectura de răspuns la amenințările spațiale (STRA)	Sectorial (Amenințări spațiale, inclusiv în domeniul cibernetic)	Arhitectura de răspuns la amenințările spațiale (STRA) cu privire la responsabilitățile care urmează să fie exercitate de Consiliu și de Înaltul Reprezentant pentru a preveni o amenințare generată de desfășurarea, funcționarea sau utilizarea sistemelor instituite și a serviciilor furnizate în cadrul Programului spațial al Uniunii	Decizia (PESC) 2021/698 a Consiliului
Cadrul de coordonare sistemică a incidentelor cibernetice (EU-SCICF)	Sectorial	Un cadru în curs de elaborare pentru comunicare și coordonare care abordează și gestionează potențialele evenimente cibernetice sistemice din sectorul financiar. Se va baza pe unul dintre rolurile preconizate ale autorităților europene de supraveghere (AES) în temeiul Regulamentului (UE) 2022/2554 de a permite treptat un răspuns coordonat eficace la nivelul Uniunii în cazul unui incident transfrontalier major legat de tehnologiile informației și comunicațiilor (TIC) sau al unei amenințări conexe care are un impact sistemic asupra sectorului financiar al Uniunii în ansamblu.	Recomandarea Comitetului european pentru risc sistemic din 2 decembrie 2021 privind un cadru paneuropean de coordonare sistemică a incidentelor cibernetice pentru autoritățile relevante (CERS/2021/17)

Mecanismul de protecție civilă al Uniunii (UCPM)	Orizontal	Asigură cooperarea în materie de protecție civilă pentru a îmbunătăți prevenirea, pregătirea și răspunsul în caz de dezastre.	Decizia nr. 1313/2013.
CISE – mediul comun pentru schimbul de informații	Specific domeniului maritim, acoperă șapte sectoare.	CISE – este o rețea care face legătura între sistemele autorităților UE/SEE responsabile cu supravegherea maritimă. CISE permite schimbul de informații relevante la nivel transfrontalier și în diferite sectoare într-o manieră fluidă și automatizată.	O Busolă strategică pentru securitate și apărare – Pentru o Uniune Europeană care își protejează cetățenii, valorile și interesele și contribuie la pacea și securitatea internaționale (21 martie 2022).

(4) Sectoarele cu o importanță critică ridicată și alte sectoare critice conform Directivei (UE) 2022/2555 și mecanismele sectoriale de gestionare a crizelor de la nivelul Uniunii (după caz)		
Sectoare	**Subsector**	**Mecanisme sectoriale de gestionare a crizelor aplicabile**
Energie	Energie electrică	Grupul de coordonare în domeniul energiei electrice
	Încălzire și răcire centralizată	nu se aplică
	Petrol	Grupul de coordonare în domeniul petrolier Grupul autorităților offshore din Uniunea Europeană (EUOAG)
	Gaze	Grupul de coordonare pentru gaz
	Hidrogen	nu se aplică
Transporturi	Transport aerian	Celula Europeană de Coordonare a Crizelor din Aviație (EACCC)
	Transport feroviar	nu se aplică

	Transport pe apă	Agenția Europeană pentru Controlul Pescuitului (EFCA) SafeSeaNet (SSN) Serviciile maritime integrate (IMS) Centrul de date pentru identificarea și urmărirea navelor la mare distanță (LRIT) Serviciile de sprijin maritim ale EMSA
	Transport rutier	nu se aplică
	Orizontal	Rețeaua punctelor de contact în domeniul transporturilor, instituită prin Planul de urgență pentru sectorul transporturilor [COM(2022) 211]
Sectorul bancar		EU-SCICF
Infrastructuri ale pieței financiare		EU-SCICF Mecanismul european de stabilizare financiară

Sănătate		Sistemul de alertă precoce și răspuns rapid (SAPR) Dispozitivul operațional pentru situații de urgență în materie de sănătate (HEOF) Sistemul de alertă rapidă pentru țesuturi și celule, precum și pentru componente sanguine (RATC/RAB) Cadrul pentru situații de urgență în domeniul sănătății publice Sistemul de alertă rapidă pentru incidente chimice (RASCHEM) Platforma europeană de supraveghere a bolilor infecțioase Autoritatea pentru Pregătire și Răspuns în caz de Urgență Sanitară (HERA) Sistemul de informații medicale (MediSys) Grupul de coordonare pentru dispozitive medicale (MDSSG) Alerta rapidă de farmacovigilență Grupul operativ al UE în domeniul sănătății (EUHTF) Comitetul pentru securitate sanitară

Apă potabilă		nu se aplică
Ape uzate		nu se aplică
Infrastructură digitală		nu se aplică
Gestionarea serviciilor TIC		nu se aplică
Administrație publică		nu se aplică
Spațiu		Arhitectura de răspuns la amenințările spațiale (STRA)
Serviciile poștale și de curierat		nu se aplică
Gestionarea deșeurilor		nu se aplică
Fabricarea, producția și distribuția de substanțe chimice		Sistemul de alertă rapidă pentru incidente chimice (RASCHEM)

Producția, prelucrarea și distribuția de alimente		Sistemul european de monitorizare a culturilor Detectarea zonelor de anomalie în producția agricolă globală (ASAP) Rețeaua europeană a sistemelor de informații privind sănătatea plantelor (EUROPHYT) Echipa de urgențe veterinare a UE (EUVET) Sistemul de alertă rapidă pentru alimente și furaje (RASFF) Mecanismul european de pregătire și răspuns în caz de criză în materie de securitate alimentară (EFSCM) Regulamentul privind situațiile de urgență pe piața internă și reziliența pieței interne (IMERA)
Industria prelucrătoare	Dispozitive medicale	nu se aplică
	Calculatoare, produse electronice și optice	nu se aplică
	Utilaje și echipamente	nu se aplică
	Fabricarea de autovehicule, remorci și semiremorci	nu se aplică
	Fabricarea altor mijloace de transport	nu se aplică

Furnizori digitali		nu se aplică
Cercetare		nu se aplică

ANEXA III – Cadrul UE de gestionare a crizelor de securitate cibernetică și instrumentele conexe

Începând din 2017, Uniunea și-a dezvoltat cadrul de securitate cibernetică prin mai multe instrumente care conțin dispoziții relevante pentru gestionarea crizelor de securitate cibernetică:

- Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[1],
- Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[2],
- Regulamentul de punere în aplicare 2024/2690 al Comisiei[3], Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului[4],
- Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului[5],
- Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului[6] și
- Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului („Regulamentul privind solidaritatea cibernetică”)[7].

Printre măsurile sectoriale specifice privind crizele de securitate cibernetică se numără Regulamentul delegat (UE) 2024/1366 al Comisiei[8] și viitorul cadru de coordonare sistemică a incidentelor cibernetice (EU-SCICF) în contextul Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului[9].

Directiva 2013/40[10] reprezintă referința pentru definirea activităților infracționale legate de atacurile cibernetice, iar normele Uniunii privind accesul transfrontalier la probele electronice, în special Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului[11], după ce vor fi puse în aplicare, vor facilita semnificativ acțiunile de asigurare a respectării legii în acest domeniu.

Politica UE în domeniul apărării cibernetice[12] subliniază rolul unei Rețele operaționale a UE de echipe militare de intervenție în caz de incidente de securitate informatică (MICNET) și rolul Conferinței comandanților cibernetici ai UE și prevede instituirea unui Centru al UE de coordonare a apărării cibernetice (EUCDCC).

În unele dintre sectoarele critice enumerate în anexele I și II la Directiva (UE) 2022/2555 există și alte mecanisme de conștientizare a situației și de răspuns la situații de criză, care nu sunt legate de domeniul cibernetic.

Recomandarea Consiliului referitoare la un Plan de acțiune privind un răspuns coordonat la nivelul Uniunii la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă[13] prevede cooperarea dintre actorii relevanți în cazul în care un incident afectează atât aspectele fizice, cât și securitatea cibernetică a infrastructurii critice.

[1] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere (JO L 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare (JO L 202, 8.6.2021, p. 1 ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului din 19 decembrie 2024 de stabilire a unor măsuri de consolidare a solidarității și a capacităților la nivelul

Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea și de modificare a Regulamentului (UE) 2021/694 (Regulamentul privind solidaritatea cibernetică) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică (JO L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8, ELI:http://data.europa.eu/eli/dir/2013/40/oj).

[11] Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale și Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale (JO L 191, 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52022JC0049.

[13] *JO C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:C_202404371.