COMISIA
EUROPEANĂ

Bruxelles, 24.2.2025
COM(2025) 66 final

2025/0036 (NLE)

Propunere de

RECOMANDARE A CONSILIULUI

privind un Plan de acțiune al UE pentru gestionarea crizelor în materie de securitate cibernetică

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Temeiurile și obiectivele propunerii

Consiliul, în Concluziile sale privind viitorul securității cibernetice din 22 mai 2024,

> *„[a invitat] Comisia să evalueze rapid actualul Plan de acțiune privind securitatea cibernetică și, pe această bază, să propună un Plan de acțiune privind securitatea cibernetică sub forma unei recomandări a Consiliului care va aborda provocările actuale și peisajul complex al amenințărilor cibernetice, va consolida rețelele existente, va consolida cooperarea și va elimina compartimentările dintre organizații, utilizând în acest scop în primul rând structurile existente. În plus, planul de acțiune revizuit ar trebui să se bazeze pe principiile directoare ale cooperării testate în timp (proporționalitatea, subsidiaritatea, complementaritatea și confidențialitatea informațiilor) și să le extindă la întregul ciclu de viață al gestionării crizelor și ar trebui să contribuie la alinierea și consolidarea comunicării securizate în domeniul securității cibernetice. Ar trebui asigurată compatibilitatea planului de acțiune revizuit cu cadrele existente, cum ar fi IPCR, setul de instrumente al UE pentru diplomația cibernetică, setul de instrumente al UE pentru contracararea amenințărilor hibride, Protocolul privind răspunsul în situații de urgență al autorităților de aplicare a legii (LERP), cadrele emergente precum Planul de acțiune privind infrastructura critică, procedurile sectoriale și structurile generale de gestionare a crizelor din cadrul entităților Uniunii, cu implicarea inclusiv a Înaltului Reprezentant și a Europolului. În acest plan revizuit, rolul Comisiei, al Înaltului Reprezentant și al ENISA, conform competențelor lor, ar trebui să se concentreze în special pe sprijinirea coordonării orizontale.”*

Obiectivul prezentului proiect de recomandare a Consiliului privind Planul de acțiune al Uniunii pentru gestionarea crizelor în materie de securitate cibernetică (Planul de acțiune în materie de securitate cibernetică) este de a prezenta, într-un mod clar, simplu și accesibil, cadrul Uniunii Europene (UE) pentru gestionarea crizelor cibernetice. Acesta ar trebui să le permită actorilor relevanți din Uniune (și anume entități individuale și rețele de entități de la nivelul Uniunii) să înțeleagă cum să interacționeze și să utilizeze în mod optim mecanismele disponibile pe parcursul întregului ciclu de viață al gestionării crizelor. Scopul cadrului este de a explica ce este o criză cibernetică și ce declanșează un mecanism de gestionare a crizelor cibernetice la nivelul Uniunii. Prezentul proiect de recomandare a Consiliului explică utilizarea mecanismelor disponibile, cum ar fi mecanismul pentru situații de urgență în materie de securitate cibernetică, inclusiv rezerva UE pentru securitate cibernetică, pentru a pregăti modul de gestionare, de răspuns și de redresare în urma unei crize generate de un incident de securitate cibernetică de mare amploare. În plus, acesta urmărește să promoveze o cooperare mai structurată între actorii civili și militari, inclusiv cooperarea cu Organizația Tratatului Atlanticului de Nord (NATO), având în vedere că un incident cibernetic de mare amploare care afectează infrastructura civilă a Uniunii pe care se bazează armata poate, de asemenea, să activeze mecanismele de răspuns ale NATO.

Planul de acțiune în materie de securitate cibernetică este un instrument fără caracter juridic obligatoriu, care identifică acțiuni specifice pentru actorii relevanți într-o criză cibernetică și care poate spori eficacitatea generală a cadrului de gestionare a crizelor cibernetice. Acesta actualizează planul de acțiune prevăzut în Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare și se bazează pe rezultatele și pe lecțiile învățate în urma exercițiilor desfășurate la nivelul Uniunii de la adoptarea recomandării respective până în prezent. Acest plan face parte din prioritățile politice mai ample în domeniul pregătirii și al securității.

Astfel cum este definit în Directiva (UE) 2022/2555 (Directiva NIS 2), un incident de securitate cibernetică de mare amploare este 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. În funcție de cauza și impactul său, un astfel de incident poate escalada și se poate transforma într-o adevărată criză care să afecteze buna funcționare a pieței interne sau să prezinte riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni, în mai multe state membre sau în Uniune în ansamblul său.

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

Propunerea este în concordanță cu instrumentele relevante ale Uniunii în domeniul securității cibernetice, în special cu Directiva NIS 2 și cu Regulamentul (UE) 2023/2841 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii. Aceasta este, de asemenea, în concordanță cu cadrul mecanismului de protecție civilă al Uniunii (UCPM), instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului, cu Decizia de punere în aplicare (UE) 2018/1993 privind mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și cu instrumentele sectoriale pentru conștientizarea situației și gestionarea crizelor, inclusiv în sectorul energiei electrice.

- **Coerența cu alte politici ale Uniunii**

Planul de acțiune în materie de securitate cibernetică completează și este coerent cu 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, întrucât aceasta acoperă perturbările legate de reziliența fizică necibernetică. Planul de acțiune în materie de securitate cibernetică interacționează îndeaproape cu mecanismele și instrumentele de gestionare a crizelor din cadrul politicii externe și de securitate comune (PESC) și al politicii de securitate și apărare comune (PSAC), prevăzute în Busola strategică pentru securitate și apărare a Consiliului. În plus, inițiativele Uniunii de combatere a criminalității informatice pot sprijini obiectivele urmărite de prezenta recomandare.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

- **Temeiul juridic**

Propunerea se bazează pe articolul 292 din TFUE, care stabilește normele relevante privind adoptarea recomandărilor.

Propunerea ar completa întregul cadru legislativ privind securitatea cibernetică instituit la nivelul Uniunii. Propunerea nu abordează gestionarea incidentelor majore care afectează entitățile Uniunii în sensul Regulamentului (UE, Euratom) 2023/2841, adoptat în temeiul articolului 298 din TFUE. Aceasta abordează însă schimbul de informații dintre entitățile Uniunii și statele membre, inclusiv dispozițiile Regulamentului (UE, Euratom) 2023/2841 conform cărora reprezentantul Comisiei în cadrul Consiliului interinstituțional pentru securitate cibernetică (IICB) este punctul de contact pentru facilitarea transmiterii de către IICB a informațiilor relevante în legătură cu incidentele majore către Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice EU-CyCLONe, ca o contribuție la conștientizarea comună a situației.

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

Deși răspunsul la perturbările infrastructurii critice sau ale serviciilor furnizate de entități esențiale și importante este în primul rând responsabilitatea statelor membre, anumite activități cibernetice răuvoitoare cu caracter transfrontalier pot perturba și prejudicia infrastructurile critice de informații de care depinde buna funcționare a pieței interne. Prin urmare, Uniunea joacă un rol important în cazul unui incident sau al unei crize semnificative. O astfel de perturbare poate afecta mai multe sau chiar toate sectoarele de activitate economică din cadrul pieței unice și ar putea afecta securitatea și relațiile internaționale ale Uniunii. Pentru a asigura funcționarea pieței interne, coordonarea la nivelul Uniunii în cazul unor perturbări ale infrastructurii critice cu efecte transfrontaliere semnificative nu este doar oportună, ci chiar necesară. Răspunsurile coordonate la nivelul Uniunii vor sprijini răspunsurile statelor membre la perturbare prin conștientizarea comună a situației, comunicarea publică coordonată și atenuarea consecințelor perturbării asupra pieței interne.

- **Proporționalitatea**

Prezenta propunere este conformă cu principiul proporționalității, astfel cum este prevăzut la articolul 5 alineatul (4) din Tratatul privind Uniunea Europeană. Nici conținutul, nici forma prezentei propuneri de recomandare a Consiliului nu depășesc ceea ce este necesar pentru atingerea obiectivelor sale. Acțiunile propuse sunt proporționale cu obiectivele urmărite, care se axează pe asigurarea unei gestionări coordonate a crizelor cibernetice la nivelul Uniunii.

- **Alegerea instrumentului**

Pentru a atinge obiectivele menționate anterior, TFUE prevede, în special la articolul 292 din tratat, adoptarea de către Consiliu de recomandări pe baza unei propuneri din partea Comisiei. În conformitate cu articolul 288 din TFUE, recomandările nu au caracter obligatoriu. O recomandare a Consiliului este un instrument adecvat în cazul de față, deoarece semnalează angajamentul statelor membre față de măsurile incluse în aceasta și oferă o bază solidă pentru cooperarea în ceea ce privește coordonarea gestionării incidentelor și crizelor de securitate cibernetică de mare amploare. În acest mod, recomandarea propusă ar completa cadrul juridic obligatoriu (în special Directiva NIS 2).

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

- **Consultările cu părțile interesate**

În procesul de elaborare a prezentei propuneri, Comisia a desfășurat consultări cu privire la revizuirea Planului de acțiune în materie de securitate cibernetică și a invitat statele membre și entitățile relevante ale Uniunii să îi transmită contribuții. Comisia a analizat opiniile exprimate de experții din statele membre, precum și de ENISA, în cadrul atelierului organizat în comun la Karpacz la 5 septembrie 2024 de către Comisie și Polonia.

Comisia a consultat reprezentanții statelor membre din cadrul rețelei CSIRT, al EU-CyCLONe și al Grupului de cooperare NIS în contextul unor reuniuni organizate în septembrie 2024 și a solicitat contribuții scrise.

Comisia a prezentat și a colectat feedback din partea Consiliului în cursul a două discuții specifice din cadrul Grupului de lucru orizontal pentru chestiuni cibernetice, care au avut loc în octombrie și noiembrie 2024.

Comisia a consultat reprezentanți ai sectorului privat, precum și reprezentanți ai statelor membre, ai Serviciului European de Acțiune Externă (SEAE) și ai ENISA în cadrul unui

atelier găzduit de Reprezentanța Permanentă a Poloniei pe lângă UE la Bruxelles, în noiembrie 2024.

Comisia a consultat entitățile relevante ale Uniunii, și anume SEAE, ENISA, Europol și CERT-UE, inclusiv prin discuții la nivel înalt în cadrul reuniunilor Grupului operativ pentru crize cibernetice[1] care au avut loc în iulie și noiembrie 2024.

S-a ajuns la un consens cu privire la necesitatea unui document actualizat, clar, simplu și operațional, care să permită actorilor relevanți să înțeleagă cadrul pentru gestionarea crizelor cibernetice și să utilizeze în mod eficace mecanismele disponibile. De asemenea, a existat un consens cu privire la necesitatea de a evita duplicarea instrumentelor și de a utiliza în mod corespunzător mecanismele existente la nivelul Uniunii pentru coordonare, schimb de informații și răspuns, fără a crea noi structuri sau a interfera cu procedurile operaționale standard interne ale rețelelor existente și ale mecanismelor sectoriale existente.

[1] Un grup informal alcătuit din serviciile Comisiei și alte servicii ale UE.

2025/0036 (NLE)

Propunere de

RECOMANDARE A CONSILIULUI

privind un Plan de acțiune al UE pentru gestionarea crizelor în materie de securitate cibernetică

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 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 cibernetice 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 amenințări hibride multidimensionale sau din operații militare. De asemenea, acestea pot afecta în mod 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 care are un impact semnificativ asupra mai multor state membre. În funcție de cauza și impactul său, un astfel de incident ar putea escalada și s-ar putea transforma într-o adevărată criză care să afecteze buna funcționare a pieței interne sau să prezinte riscuri grave pentru securitatea și siguranța publică, 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 guvernelor, a infrastructurii critice, a cetățenilor și a întreprinderilor europene, 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) În conformitate cu procedurile prevăzute în Decizia de punere în aplicare (UE) 2018/1993 a Consiliului[2], președinția Consiliului, care consultă (cu excepția cazurilor în care a fost invocată clauza de solidaritate) statele membre afectate, Comisia și Înaltul Reprezentant (ÎR), adoptă o decizie de activare și dezactivare a mecanismului integrat al UE pentru un răspuns politic la crize (IPCR). În plus, în conformitate cu

[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, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

procedurile IPCR, Secretariatul General al Consiliului, serviciile Comisiei și SEAE pot conveni, de asemenea, în consultare cu președinția, să activeze IPCR în modul „schimb de informații”. Discuțiile din cadrul IPCR se bazează pe rapoartele privind analiza și conștientizarea integrată a situației elaborate de serviciile Comisiei și de Serviciul European de Acțiune Externă („SEAE”).

(4) Deși statelor membre le revine principala responsabilitate în ceea ce privește gestionarea crizelor cibernetice naționale, potențialul caracter transfrontalier și transsectorial al incidentelor de securitate cibernetică impune 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. În același timp, răspunsul la criză și redresarea sunt costisitoare pentru entitățile și sectoarele afectate. Prin urmare, gestionarea crizelor pe durata întregului lor ciclu de viață include pregătirea și conștientizarea comună a situației pentru a anticipa incidentele de securitate cibernetică, capacitățile de detectare necesare pentru a identifica incidentele de securitate cibernetică și instrumentele de răspuns și de redresare necesare pentru a le atenua, descuraja și limita.

(5) 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. Aceasta a cartografiat actorii relevanți la nivel tehnic, operațional și politic și a explicat modul în care aceștia au fost integrați în gestionarea mai amplă 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).

(6) 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[4], Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[5], Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei[6], Regulamentul (UE,

---

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, ELI: http://data.europa.eu/eli/reco/2017/1584/oj).

4 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).

5 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).

6 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

Euratom) 2023/2841 al Parlamentului European și al Consiliului[7], Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului[8], Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului[9] și Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului („Regulamentul privind solidaritatea cibernetică”)[10]. Printre măsurile sectoriale specifice privind crizele de securitate cibernetică se numără Regulamentul delegat (UE) 2024/1366 al Comisiei[11] și viitorul cadru de coordonare sistemică a incidentelor cibernetice (EU-SCICF) în contextul Regulamentului (UE) 2022/2554 al Parlamentului European și al Consiliului[12]. Directiva 2013/40[13] prevede 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[14] după ce va fi pus în aplicare, vor facilita semnificativ acțiunile de asigurare a respectării legii în acest domeniu. Politica UE în domeniul apărării cibernetice[15] subliniază rolul unei Rețele operaționale a UE de echipe militare de intervenție în caz de incidente de

---

servicii de socializare în rețea, precum și prestatorii de servicii de încredere (JO L 2024/2690, 18.10.2024).

7 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).

8 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).

9 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).

10 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, 2025/28, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

11 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).

12 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).

13 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).

14 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).

15 JOIN(2022) 49 final.

securitate informatică (MICNET) și rolul Conferinței comandanților Comandamentului Apărării Cibernetice 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[16] prevede cooperarea dintre actorii relevanți în cazul în care un incident afectează atât aspectele fizice, cât și securitatea cibernetică a infrastructurii critice.

(7) La nivelul Uniunii, printre actorii relevanți care au responsabilități în materie de gestionare a crizelor cibernetice se numără Comisia, SEAE, inclusiv Capacitatea unică de analiză a informațiilor (SIAC), Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii (CERT-UE), Europol prin intermediul Centrului european de combatere a criminalității informatice (EC3), Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT), Centrul Satelitar al UE (SATCEN), Centrul de monitorizare a securității Galileo și rețeaua de delegații a Uniunii. Acești actori ai Uniunii ar trebui să stabilească împreună domeniile de cooperare și să contribuie la punerea în aplicare a cadrului Uniunii de gestionare a crizelor cibernetice, conform competențelor lor în temeiul legislației aplicabile.

(8) Este necesară o recomandare actualizată de stabilire a unui Plan de acțiune în materie de securitate cibernetică („Planul de acțiune în materie de securitate cibernetică”), care să ofere orientări clare și accesibile prin care să se explice ce este o criză cibernetică la nivelul Uniunii, cum se activează cadrul de gestionare a crizelor și care sunt rolurile actorilor și ale mecanismelor relevante de la nivelul Uniunii, precum și interacțiunea dintre acești actori și mecanisme pe parcursul întregului ciclu de viață al crizei cibernetice. Planul de acțiune în materie de securitate cibernetică trebuie privit în contextul mai larg al relațiilor civile-militare și al relațiilor UE-NATO.

(9) Prezenta recomandare completează mecanismul integrat pentru un răspuns politic la crize (IPCR) și mecanismele mai ample de răspuns la criză ale Uniunii, inclusiv sistemul general de alertă rapidă al Comisiei ARGUS, mecanismul de protecție civilă al Uniunii (UCPM) sprijinit de Centrul de coordonare a răspunsului la situații de urgență (ERCC), mecanismul de răspuns în caz de criză al Serviciului European de Acțiune Externă (CRM), precum și alte procese, cum ar fi cele descrise în setul de instrumente al UE pentru contracararea amenințărilor hibride[17] și în Protocolul revizuit al UE pentru combaterea amenințărilor hibride. De asemenea, aceasta completează și ar trebui să fie coerentă cu 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 („Planul de acțiune pentru infrastructura critică”), care acoperă reziliența fizică necibernetică și care vizează îmbunătățirea coordonării răspunsului la nivelul Uniunii în acest domeniu.

---

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

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

(10) Ar trebui încurajată o abordare cuprinzătoare și integrată a gestionării crizelor în toate sectoarele și la toate nivelurile de guvernanță. 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 cibernetice au consecințe în viața reală. În cazul în care incidentele de securitate cibernetică fac parte dintr-o campanie sau o criză hibridă mai amplă, actorii relevanți ar trebui să sprijine eforturile de elaborare a unui tablou situațional unificat între diferitele sectoare și domenii. Recomandarea contribuie la acțiuni de pregătire mai ample necesare pentru Uniune în fața amenințărilor hibride multidimensionale [în conformitate cu principiile incluse în Strategia privind o uniune a pregătirii pentru situații de criză].

(11) Securitatea infrastructurii digitale critice este fundamentală pentru reziliența economiei, a societății și a apărării Uniunii. Entitățile care intră sub incidența Directivei (UE) 2022/2555, inclusiv cele care furnizează cabluri de comunicații submarine, trebuie să ia măsuri pentru a proteja securitatea fizică și de mediu a rețelelor și a sistemelor informatice pe baza unei abordări care să ia în considerare toate riscurile, cum ar fi defecțiunile sistemelor, erorile umane, actele răuvoitoare sau fenomenele naturale. În plus, entitățile respective ar trebui să raporteze incidentele, inclusiv pe cele legate de cablurile de comunicații submarine, echipelor CSIRT sau, după caz, autorității competente. Deși principiile fundamentale care stau la baza Planului de acțiune în materie de securitate cibernetică sunt relevante pentru securitatea cablurilor submarine, mecanismele pe care le stabilește nu sunt suficient de cuprinzătoare pentru a acoperi întregul ciclu de reziliență la criză. Natura specifică a acestuia justifică un efort concertat și adaptat pentru a răspunde nevoilor de supraveghere integrată a amenințărilor și de conștientizare a situației în bazinele maritime din jurul UE, investiții strategice pentru a crea redundanțe și o abordare europeană comună pentru a consolida capacitățile de reparare și de redresare. Strategia UE în materie de securitate maritimă cuprinde acțiuni de consolidare a securității cibernetice în domeniul maritim și de îmbunătățire a supravegherii și a protecției infrastructurii maritime critice, inclusiv a cablurilor submarine. Pentru gestionarea crizelor la nivelul Uniunii, o soluție care ar merita vedere să fie avută în ar consta într-o rețea specifică de puncte naționale de contact și în interacțiuni civile-militare strânse, inclusiv cu NATO.

(12) Pregătirea pentru o criză necesită o evaluare cuprinzătoare, care să ia în considerare toate riscurile și amenințările, având în vedere convergența intereselor economice și de securitate ale UE. O conștientizare comună a situației la nivelul Uniunii în rândul statelor membre și al entităților Uniunii, facilitată de ajungerea la un acord asupra unei taxonomii comune și asupra unor canale de comunicare securizate, ar trebui să permită un răspuns coordonat și în cunoștință de cauză la incidentele de securitate cibernetică potențiale și de mare amploare, precum și să îi descurajeze pe actorii care generează amenințări persistente. Pe baza principiului necesității de a cunoaște și având în vedere importanța încrederii în schimbul de informații, grupuri de state membre în diferite configurații și, după caz, entitățile relevante ale Uniunii ar putea dori să coopereze și să facă schimb de informații relevante pentru gestionarea incidentelor cibernetice. Statele membre și entitățile Uniunii care se confruntă cu aceleași amenințări, riscuri și lacune în materie de maturitate cibernetică ar trebui să creeze condiții favorabile pentru identificarea priorităților adecvate pentru investiții solide și acțiuni concrete care să conducă la o mai bună reziliență cibernetică.

(13) În conformitate cu articolul 6 din Regulamentul (UE) 2019/881, ENISA, în strânsă cooperare cu statele membre, întocmește periodic un raport aprofundat asupra situației

tehnice în materie de securitate cibernetică la nivelul UE cu privire la incidentele și amenințările cibernetice. Raportul respectiv este denumit Raportul comun de evaluare a securității cibernetice al UE (UE-JCAR) și este întocmit împreună cu Europol/EC3 și CERT-UE, cu scopul de a consolida pregătirea Uniunii, deoarece asigură conștientizarea situației pe baza unei analize a incidentelor și a amenințărilor cibernetice.

(14) Infrastructura critică esențială, cum ar fi infrastructura energetică, de transporturi, digitală, serviciile de sănătate sau financiare, precum și soluțiile de securitate implementate pentru a o proteja sunt de regulă exploatate de întreprinderi private. Protejarea acestei infrastructuri împotriva unor incidente cibernetice de mare amploare necesită o cooperare strânsă între entitățile publice și private, printre care și producătorii și dezvoltatorii de software cu sursă deschisă, bazată pe încredere și pe proceduri clare și specifice pentru schimbul de informații, diseminarea și coordonarea răspunsului.

(15) Exercițiile de securitate cibernetică la nivelul Uniunii reprezintă un instrument extrem de eficace pentru testarea procedurilor și a mecanismelor de cooperare și, prin urmare, pentru îmbunătățirea gradului de pregătire. Întrucât exercițiile consumă multe resurse, agenda acestora trebuie să fie cât mai raționalizată și consolidată și trebuie să ia în considerare scenariile elaborate în cadrul evaluărilor de risc coordonate la nivelul Uniunii și alte inițiative relevante.

(16) Infrastructurile digitale europene prezintă multe dependențe tehnice adânc înrădăcinate. Acestea ar trebui eliminate pentru a se asigura continuitatea activității în situații de criză. Un exemplu este sistemul de nume de domenii (DNS), care este o componentă esențială ce stă la baza activității internetului. Rezolverele DNS sunt esențiale pentru accesarea internetului, inclusiv în timpul unei crize cibernetice majore, deoarece ele traduc numele de domenii de internet în adrese IP. Directiva (UE) 2022/2555 încurajează părțile interesate relevante să adopte o strategie de diversificare a rezoluției DNS. De asemenea, aceasta încurajează statele membre să promoveze dezvoltarea și utilizarea unui rezolver DNS european public și sigur, ca o măsură-cheie pentru a asigura pregătirea pentru situații de criză și reziliența.

(17) În plus, pentru a spori reziliența altor componente critice, cum ar fi sistemul de rutare, și pentru a asigura funcționalitatea acestora în timpul crizelor cibernetice majore, este esențial să se pună în aplicare în timp util cele mai bune practici corespunzătoare și cele mai recente standarde disponibile. În consecință, Regulamentul de punere în aplicare (UE) 2024/2690 prevede instituirea unui forum multipartit pentru identificarea celor mai bune standarde și tehnici de implementare disponibile pentru elementele esențiale de securitate cibernetică și încurajează participarea entităților relevante.

(18) Pentru a detecta în mod eficace activitățile răuvoitoare din lanțurile de aprovizionare globale din ce în ce mai complexe care pot avea un impact la nivelul întregii Uniuni, este necesară o abordare coordonată. Acest lucru este deosebit de relevant pentru domeniile în care Uniunea se bazează pe tehnologii provenite de la furnizori cu grad ridicat de risc aflați sub jurisdicția unei țări terțe care impune raportarea către autoritățile sale a informațiilor privind vulnerabilitățile legate de software sau de hardware înainte ca acestea să fie cunoscute cu scopul de a fi exploatate. Este posibil, de asemenea, ca actori sponsorizați de state să se prepoziționeze în infrastructurile critice cu intenția de a provoca perturbări ulterior, de exemplu în timpul unui conflict. Acest lucru este dificil de detectat prin metode tradiționale, deoarece actorii care generează amenințări își ascund activitățile combinându-le cu traficul legitim și

fuzionând tehnici de tip „living off the land”, care se bazează pe instrumente și procese legitime pentru a ascunde activitățile răuvoitoare. Același lucru este valabil și pentru țările terțe în care, potrivit declarațiilor publice ale Uniunii sau ale statelor sale membre, actori care generează amenințări și care acționează de pe teritoriul țărilor respective au desfășurat activități cibernetice răuvoitoare împotriva Uniunii. Lanțurile de aprovizionare ar trebui să devină mai reziliente și mai diversificate, menținând în același timp un nivel de referință comun în materie de pregătire.

(19) La nivel tehnic, echipele CSIRT, autoritățile de aplicare a legii, precum și centrele cibernetice naționale și transfrontaliere (centre cibernetice) care urmează să fie instituite în temeiul Regulamentului (UE) 2025/38 joacă un rol esențial în detectarea incidentelor, a amenințărilor cibernetice și a vulnerabilităților, în sprijinirea atribuțiilor tehnice și în redresarea în urma atacurilor cibernetice. Este esențial să se aplice modalitățile procedurale eficace pentru cooperarea dintre rețeaua CSIRT și EU-CyCLONe, astfel cum se prevede în Directiva (UE) 2022/2555. Mecanismul european de alertă în materie de securitate cibernetică urmărește să sprijine dezvoltarea unor capacități avansate pentru ca Uniunea să consolideze capacitățile de detectare, analiză și prelucrare a datelor în legătură cu amenințările cibernetice și prevenirea incidentelor în Uniune.

(20) În ceea ce privește răspunsul imediat, mecanismele aflate la dispoziția statelor membre includ rezerva UE pentru securitate cibernetică și acțiunile de sprijinire a asistenței reciproce instituite în temeiul Regulamentului (UE) 2025/38, echipele de răspuns rapid în caz de amenințări hibride și echipele de răspuns rapid în domeniul cibernetic (CRRT) din cadrul cooperării structurate permanente (PESCO), precum și mecanismele prevăzute pentru aliații NATO. În plus, Protocolul UE privind răspunsul în situații de urgență al autorităților de aplicare a legii (LEERP) sprijină autoritățile de aplicare a legii din UE 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, inclusiv prin armonizarea intervențiilor la nivelul autorităților de aplicare a legii și coordonarea cu partenerii din alte sectoare de activitate. Obținerea unei imagini clare a opțiunilor de răspuns disponibile în cazul incidentelor cibernetice și al activităților hibride și a modului în care acestea sunt utilizate poate asigura o alocare eficientă a resurselor și poate evita duplicarea acestora. În consecință, în temeiul Regulamentului (UE) 2025/38, statele membre au obligația de a informa rețeaua CSIRT și EU-CyCLONe atunci când solicită servicii ale rezervei UE pentru securitate cibernetică.

(21) Combaterea eficace a criminalității informatice este esențială pentru securitatea cibernetică. Descurajarea nu poate fi realizată exclusiv prin reziliență, este nevoie și ca infractorii să fie identificați, urmăriți penal și să li se riposteze. Cooperarea prin intermediul unor sisteme și platforme tehnice adaptate și schimbul de informații relevante între actorii din domeniul securității cibernetice, entitățile care desfășoară activități de diplomație cibernetică și autoritățile de aplicare a legii sunt, prin urmare, esențiale pentru a asigura o înțelegere cuprinzătoare a peisajului amenințărilor și pentru a putea răspunde în mod coerent și coordonat.

(22) Crizele generează incertitudine, pe care adversarii o pot exploata cu ușurință pentru a răspândi dezinformarea și a sădi neîncredere. Pentru a contracara acest lucru, este esențială o comunicare publică clară și coerentă cu privire la situație și la măsurile luate pentru remedierea acesteia. O comunicare strategică coordonată poate sprijini, de asemenea, acțiunile diplomatice față de actorii care generează amenințări persistente și

elaborarea unui narativ privind amenințările la adresa Uniunii, acțiunile de descurajare ale acesteia și necesitatea de a promova un comportament responsabil al statelor în spațiul cibernetic.

(23) Pentru o gestionare eficace a crizelor, este necesar să se identifice soluții comune de comunicare securizată pentru domeniul cibernetic și acestea să fie puse în aplicare în întreaga Uniune, inclusiv, dacă este necesar, pentru schimbul de informații clasificate ale UE. În urma solicitării Consiliului, Comisia și alte entități relevante ale Uniunii au cartografiat instrumentele de comunicare securizate existente și au prezentat rezultatele în decembrie 2022. Există mai multe eforturi separate din partea entităților Uniunii pentru consolidarea capacităților de comunicații securizate în caz de criză care necesită o mai bună coordonare și mobilizare. Printre acestea se numără instituirea unui sistem de comunicații critice al UE (EUCCS) pentru a spori reziliența infrastructurii de comunicații publice împotriva interferențelor răuvoitoare și pentru a îmbunătăți cooperarea operațională zilnică, inclusiv la nivel transfrontalier.

(24) Mediul de securitate al Uniunii necesită o abordare care să ia în considerare toate riscurile, la nivelul întregii administrații și la nivelul întregii societăți, în ceea ce privește pregătirea civilă și militară. Organismele militare se bazează pe infrastructuri critice civile, de exemplu în domeniul comunicațiilor, al energiei, al sănătății, al transporturilor și al logisticii. În consecință și astfel cum s-a subliniat în politica UE în domeniul apărării cibernetice[18], securitatea cibernetică a UE necesită o mai mare cooperare și sinergii între capacitățile de pregătire și răspuns ale rețelelor civile și militare, inclusiv în cazul unui atac armat. Actorii din domeniul securității cibernetice ar trebui să lucreze împreună, dincolo de compartimentările instituționale și operaționale, pentru a anticipa și a aborda amenințarea pe care o reprezintă perturbările multisectoriale și multidimensionale, în conformitate cu principiile care [urmează să fie incluse] în Strategia privind o uniune a pregătirii pentru situații de criză. În plus, activitățile cibernetice răuvoitoare joacă un rol din ce în ce mai important în campaniile hibride mai ample desfășurate împotriva Uniunii, a statelor sale membre și a partenerilor strategici. Prin urmare, este necesară o cooperare mai strânsă între Uniune și NATO.

(25) În cadrul comunității militare, viitorul Centru al UE de coordonare a apărării cibernetice și Capacitatea unică de analiză a informațiilor (SIAC) din cadrul Serviciului European de Acțiune Externă, Rețeaua operațională a echipelor militare de intervenție în caz de incidente de securitate informatică (MICNET) și Conferința comandanților Comandamentului Apărării Cibernetice ai UE facilitată de Agenția Europeană de Apărare (AEA), precum și proiectele relevante din cadrul cooperării structurate permanente (PESCO) reprezintă actori și inițiative importante de coordonare și cooperare în ceea ce privește pregătirea pentru detectarea, descurajarea și apărarea împotriva amenințărilor cibernetice care afectează Uniunea și statele membre, precum și redresarea în urma acestora. Prin urmare, ar trebui încurajată cooperarea dintre actorii civili și militari, cum ar fi cooperarea dintre EU-CyCLONe și Conferința comandanților Comandamentului Apărării Cibernetice ai UE, precum și potențiala colaborare dintre MICNET și rețeaua CSIRT.

(26) Cooperarea cu țările și organizațiile care sunt parteneri strategici internaționali din afara Uniunii consolidează capacitățile Uniunii în materie de securitate cibernetică. Prin promovarea cooperării internaționale, Uniunea și partenerii săi pot asigura

[18] Politica UE în domeniul apărării cibernetice; JOIN/2022/49 final.

conștientizarea comună a situației, coerența în gestionarea crizelor cibernetice și o postură de securitate cibernetică solidă, contribuind la un spațiu cibernetic global deschis, stabil, sigur și rezilient. Această colaborare ar trebui să se bazeze pe încredere și pe obiectivul comun de a proteja infrastructura critică și serviciile esențiale împotriva amenințărilor cibernetice, inclusiv prin promovarea unui comportament responsabil al statelor în spațiul cibernetic, bazat pe cadrul Organizației Națiunilor Unite (ONU) și prin tragerea la răspundere a actorilor care generează amenințări pentru comportamentul lor iresponsabil și ilegal în spațiul cibernetic. Măsurile de diplomație cibernetică contribuie la descurajarea activităților cibernetice răuvoitoare și la răspunsul la acestea și asigură coordonarea și cooperarea cu țările care sunt parteneri strategici internaționali.

ADOPTĂ PREZENTA RECOMANDARE:

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

(1) Prezenta recomandare stabilește cadrul Uniunii pentru gestionarea crizelor de securitate cibernetică în contextul pregătirii generale a UE pentru amenințările hibride multidimensionale. Modul în care un incident poate escalada într-un incident de mare amploare și apoi într-o criză la nivelul UE este ilustrat și sintetizat în anexa 1, inclusiv în cazul în care un astfel de incident coincide cu alte amenințări hibride care necesită interacțiunea dintre răspunsurile necesare. Cadrul de gestionare a crizelor cibernetice ar trebui să permită actorilor relevanți de la nivelul Uniunii, inclusiv entităților și rețelelor, să înțeleagă cum trebuie să interacționeze și să utilizeze în mod optim mecanismele existente enumerate în anexa II pe parcursul întregului ciclu de viață al gestionării crizelor. În plus, acesta recomandă actorilor respectivi de la nivelul Uniunii cum poate fi îmbunătățită eficacitatea mecanismelor existente.

(2) Uniunea și statele sale membre ar trebui să urmeze Planul de acțiune în materie de securitate cibernetică în ceea ce privește gestionarea unei crize generate de un incident de securitate cibernetică de mare amploare, astfel cum este definit la articolul 6 punctul 7 din Directiva (UE) 2022/2555, care afectează buna funcționare a pieței interne sau prezintă riscuri grave în materie de securitate și siguranță publică pentru entitățile sau cetățenii din mai multe state membre sau din Uniune în ansamblu („criză cibernetică”).

(3) Atunci când un incident de securitate cibernetică, detectat la nivel tehnic de o echipă CSIRT sau de un centru cibernetic, duce la escaladare conform procedurilor interne ale rețelei CSIRT, a trebui să fie partajate informațiile adecvate, în conformitate cu modalitățile procedurale relevante, cu EU-CyCLONe, care, la rândul său, ar trebui să analizeze dacă respectivul incident este un incident de mare amploare potențial sau în desfășurare, astfel cum este definit la articolul 6 punctul 7 din Directiva (UE) 2022/2555. Ar trebui să se determine dacă există o criză cibernetice ca urmare a acestui incident de mare amploare sau dacă aceasta a luat sfârșit în conformitate cu Decizia de punere în aplicare (UE) 2018/1993, în special cu articolele 4 și 5.

(4) În conformitate cu principiile proporționalității, subsidiarității, complementarității și confidențialității informațiilor prevăzute în anexa III, statele membre și entitățile Uniunii ar trebui să își aprofundeze cooperarea în ceea ce privește gestionarea crizelor cibernetice, promovând încrederea reciprocă și bazându-se pe rețelele și mecanismele existente. Deși Planul de acțiune în materie de securitate cibernetică nu

interferează cu modul în care entitățile își definesc procedurile interne, fiecare entitate ar trebui să definească în mod clar interfețele utilizate pentru colaborarea cu alte entități. Aceste interfețe ar trebui să fie stabilite de comun acord între entitățile în cauză și să fie documentate în mod clar.

(5) Planul de acțiune în materie de securitate cibernetică ar trebui aplicat asigurându-se coerența sa cu Planul de acțiune pentru infrastructura critică, în special în cazul incidentelor care afectează atât reziliența fizică, cât și securitatea cibernetică a infrastructurii critice[19]. În cazul în care există măsuri sectoriale de gestionare a crizelor care vizează incidentele de securitate cibernetică, măsurile respective ar trebui să fie puse în aplicare în mod coerent cu prezenta recomandare.

II: Pregătirea pentru o criză cibernetică la nivelul Uniunii

(a) Conștientizarea situației și schimbul de informații

(6) Datele verificate și fiabile, inclusiv tendințele în materie de incidente, tactici, tehnici și proceduri, precum și vulnerabilitățile exploatate activ ar trebui să stea la baza unei conștientizări comune a situației în rândul statelor membre și al entităților Uniunii cu privire la peisajul amenințărilor cibernetice. Aceste cunoștințe partajate ar trebui utilizate de statele membre și de entitățile Uniunii pentru a anticipa, a se pregăti și a detecta atacurile cibernetice, conform domeniilor lor de responsabilitate. Această conștientizare comună a situației ar trebui:

(a) să se aplice tuturor sectoarelor critice enumerate în Directiva (UE) 2022/2555, în special comunicațiilor, infrastructurii digitale, energiei, transporturilor, finanțelor, spațiului și sănătății, și ar trebui să se aplice, de asemenea, prin intermediul CERT-UE, rețelelor și sistemelor entităților Uniunii în conformitate cu Regulamentul (UE, Euratom) 2023/2841;

(b) să se bazeze pe seturi de date diversificate și integrate de înaltă calitate care sunt colectate, prelucrate și partajate în timp real;

(c) să fie luate în considerare în raportul comun de evaluare a securității cibernetice (JCAR) și în alte produse relevante;

(d) să ia în considerare amenințările hibride conexe, inclusiv acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI) și dezinformarea;

(e) să sprijine acțiunile și măsurile de răspuns pe termen scurt, precum și să contribuie la planificarea pe termen lung a politicilor în contextul pregătirii și al descurajării;

(f) [link către alte evaluări ale riscurilor și amenințărilor realizate în mod regulat și consolidate de Strategia privind o uniune a pregătirii pentru situații de criză cu scopul de a asigura sinergii și simplificare în ceea ce privește obligațiile de raportare ale statelor membre.]

(7) 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 membri;

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

(c) să utilizeze pe deplin instrumentele disponibile pentru schimbul de informații.

(8) Statele membre și entitățile relevante ale Uniunii ar trebui să îmbunătățească modalitățile de coordonare și de parteneriat cu sectorul privat, inclusiv cu comunitățile și producătorii de software cu sursă deschisă, pentru a îmbunătăți schimbul de informații, bazându-se pe centrele de schimb de informații și de analiză a informațiilor existente la nivelul UE și la nivel național, pentru a consolida capacitatea de securitate cibernetică și pentru a răspunde la incidentele de securitate cibernetică, inclusiv prin mese rotunde cu EU-CyCLONe și cu rețeaua CSIRT.

(9) Statele membre și entitățile relevante ale Uniunii ar putea alege, în scopul promovării cooperării și al consolidării încrederii, precum și pe baza acordurilor privind schimbul de informații în materie de securitate cibernetică prevăzute în Directiva (UE) 2022/2555 și a dispozițiilor Regulamentului (UE) 2025/38 privind centrele cibernetice, să creeze clustere de colaborare voluntară pe baza principiului necesității de a cunoaște, în cazul în care există preocupări comune, cum ar fi descurajarea, detectarea sau răspunsul la un anumit tip de amenințare cu care se confruntă în mod unic. Orice astfel de clustere ar trebui să respecte mandatul actorilor relevanți, precum și structurile deja stabilite. Aceste clustere de colaborare ar putea apela la entitățile Uniunii să le faciliteze colaborarea, inclusiv prin intermediul unei infrastructuri adecvate.

(10) Statele membre, prin intermediul Grupului de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui, în termen de 12 luni de la adoptarea Planului de acțiune în materie de securitate cibernetică, să elaboreze o taxonomie comună cu privire la gestionarea crizelor cibernetice și să ofere un ghid privind gestionarea securizată și schimbul securizat de informații legate de incidentele și crizele de securitate cibernetică, care să includă o secțiune dedicată stabilirii nivelului de confidențialitate al acestor informații (clasificare).

(11) Atunci când stabilesc nivelul de confidențialitate pentru informațiile disponibile, statele membre și entitățile relevante ale Uniunii ar trebui să ia în considerare impactul potențial pe care îl poate avea atribuirea unu nivel superior de clasificare asupra schimbului voluntar de informații și asupra realizării unei conștientizări comune a situației. Atunci când fac schimb de informații neclasificate, 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.

(b) Exerciții comune

(12) Statele membre și entitățile relevante ale Uniunii ar trebui să dezvolte un ciclu continuu eficient de exerciții de securitate cibernetică pentru a se pregăti pentru crizele cibernetice și pentru a spori eficiența organizațională. Aceste exerciții ar trebui să se bazeze pe scenariile elaborate pe baza evaluărilor de risc coordonate la nivelul UE, inclusiv a celor privind crizele multisectoriale. Ciclul continuu al exercițiilor de securitate cibernetică ar trebui să țină seama de UCPM și de alte mecanisme de răspuns în caz de criză de la nivelul Uniunii. Acesta ar trebui să asigure faptul că lecțiile învățate din exerciții sunt puse în aplicare în mod eficace.

(13) Actorii relevanți ai Uniunii ar putea efectua exerciții la scară mai mică pentru a-și testa interacțiunile și interfețele în cazul escaladării incidentelor cibernetice.

(14) Serviciile Comisiei, SEAE și ENISA sunt invitate să organizeze un exercițiu de testare a Planului de acțiune în materie de securitate cibernetică în termen de 18 luni de la adoptarea acestuia, implicând toți actorii relevanți, inclusiv sectorul privat.

(c) Capacități de rezoluție a DNS

(15) Statele membre, entitățile relevante ale Uniunii, precum și entitățile private, cum ar fi operatorii de infrastructură critică, ar trebui să își consolideze strategia de diversificare a rezoluției sistemelor de nume de domenii (DNS), inclusiv utilizarea a cel puțin unei infrastructuri DNS cu sediul în Uniune, cum ar fi DNS4EU, pentru a asigura o rezoluția fiabilă a DNS în timpul crizelor majore. ENISA și EU-CyCLONe ar trebui să elaboreze și să pună la dispoziție orientări referitoare la comutarea automată către sisteme de siguranță (*failover*) în situații de urgență, care să prezinte etapele care trebuie parcurse pentru a asigura preluarea funcțiilor de către o infrastructură DNS cu sediul în Uniune în cazul în care alte servicii DNS nu funcționează, asigurând continuitatea serviciilor critice în timpul unei crize.

(16) În plus, centrele cibernetice naționale și centrele cibernetice transfrontaliere ar trebui să facă schimb de informații relevante privind amenințările cu astfel de infrastructuri DNS cu sediul în Uniune, pentru a le sprijini să ofere un nivel ridicat de protecție împotriva amenințărilor specifice Uniunii și, prin urmare, să sporească și mai mult capacitățile de detectare și atenuare a amenințărilor specifice Uniunii.

(17) Pentru a consolida, în general, securitatea și disponibilitatea infrastructurii critice de internet, inclusiv în timpul crizelor, statele membre ar trebui să promoveze în mod activ participarea tuturor părților interesate relevante, inclusiv a celor care nu sunt vizate în mod direct de Regulamentul de punere în aplicare a NIS 2, la forumul multipartit însărcinat cu identificarea celor mai bune standarde și tehnici de implementare disponibile pentru măsuri esențiale de securitate a rețelei. În plus, statele membre ar trebui să ia în considerare implicarea în cadrul forumului și să adopte ele însele orientările recomandate.

(d) Resurse

(18) Statele membre ar trebui să utilizeze pe deplin resursele financiare disponibile pentru securitatea cibernetică furnizate de programele relevante ale Uniunii.

III: Detectarea unui incident care ar putea escalada într-o criză cibernetică

(19) Pentru a face față complexității în creștere a incidentelor cibernetice și provocărilor tot mai mari în ceea ce privește detectarea acestora, atât entitățile publice, cât și cele private ar trebui să pună în aplicare strategii de detectare bazate pe amenințări în toate infrastructurile lor digitale, pentru a identifica eventuale prepoziționări care pot fi exploatate ulterior cu scopul de a produce perturbări. Atunci când sunt identificate operațiuni sub acoperire, entitățile ar trebui să facă schimb proactiv de informații relevante cu partenerii lor cu mult înainte ca situațiile să se transforme în situații de criză.

(20) 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 o potențială criză cibernetică.

(21) Rețeaua CSIRT și EU-CyCLONe ar trebui să stabilească 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.

(22) Rețeaua CSIRT ar trebui să consilieze EU-CyCLONe cu privire la posibilitatea ca un incident de securitate cibernetică observat să fie considerat un incident de mare amploare potențial sau în desfășurare.

(23) Centrele cibernetice transfrontaliere, deja instituite sau care urmează să fie instituite în temeiul Regulamentului (UE) 2025/38, ar trebui să contribuie cu informații relevante la mecanismele de la nivelul Uniunii în cazul unui incident de securitate cibernetică de mare amploare potențial sau în desfășurare pe baza unei abordări care ține seama toate riscurile, inclusiv daunele fizice aduse infrastructurii critice care compromit disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor care sunt oferite de rețele și sisteme informatice sau care sunt accesibile prin intermediul acestora.

(24) În cazul în care se detectează un incident de securitate cibernetică potențial sau de mare amploare cu impact multisectorial:

(a) Comisia ar trebui să faciliteze fluxul de informații necesare între punctele de contact pentru mecanismele de criză orizontale și sectoriale relevante la nivelul Uniunii enumerate în anexa II și EU-CyCLONe;

(b) entitățile relevante ale Uniunii ar trebui să sprijine EU-CyCLONe în evaluarea consecințelor pentru diferitele sectoare și populație.

IV: Răspunsul la o criză cibernetică la nivelul Uniunii

(25) În cazul unei crize cibernetice stabilite în temeiul IPCR, toți actorii ar trebui să răspundă în strânsă coordonare cu alte entități care răspund la amenințări hibride mai ample în cadrul unei abordări care ține seama de toate nivelurile de guvernare, după cum urmează:

(a) statul membru (statele membre) afectat(e) și rețeaua CSIRT ar trebui să coopereze pentru a restabili rapid sistemele compromise, asigurând perturbări operaționale minime;

(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 raportul privind analiza și conștientizarea integrată a situației (ISAA) din cadrul mecanismului IPCR;

(c) Comisia, în cooperare cu Înaltul Reprezentant, după caz, ar trebui să asigure coerența și coordonarea între răspunsurile la criză și acțiunile conexe de răspuns de la nivelul Uniunii, în special mecanismele sectoriale relevante de gestionare a crizelor de la nivelul Uniunii enumerate în anexa 2, precum și în ceea ce privește solicitarea de asistență prin intermediul UCPM;

(d) președinția Consiliului ar trebui să ia în considerare invitarea președintelui EU-CyCLONe la mese rotunde informale și la alte reuniuni relevante ale Consiliului în cadrul mecanismului IPCR;

(e) Consiliul, sprijinit de EU-CyCLONe și de entitățile relevante ale Uniunii, ar trebui să coordoneze eforturile de comunicare publică, inclusiv pentru a se asigura că situația de criză nu este utilizată pentru a răspândi informații inexacte;

(f) Înaltul Reprezentant, în strânsă cooperare cu Comisia și cu alte entități relevante ale Uniunii, ar trebui să sprijine, inclusiv prin analize și rapoarte,

procesul decizional din cadrul Consiliului cu privire la utilizarea unor posibile măsuri ca parte a setului de instrumente 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;

(g) Comisia, Înaltul Reprezentant și statele membre ar trebui, de asemenea, să utilizeze mai eficient instrumente economice precum interdicțiile comerciale pentru a preveni, a descuraja și a răspunde mai bine la activitățile cibernetice răuvoitoare persistente ale actorilor statali.

(26) În cazul în care un utilizator al serviciilor furnizate de rezerva UE pentru securitate cibernetică[20] solicită servicii din partea rezervei în conformitate cu articolul 15 din Regulamentul (UE) 2025/38 și fără a aduce atingere niciunui act viitor de punere în aplicare în temeiul regulamentului respectiv:

(a) serviciile ar trebui să fie implementate în termen de 24 de ore de la solicitare;

(b) Comisia și Înaltul Reprezentant ar trebui să asigure coordonarea cu măsuri suplimentare, în conformitate cu setul de instrumente pentru contracararea amenințărilor hibride[21] în cazul unor activități cibernetice răuvoitoare care fac parte dintr-o campanie hibridă mai amplă;

(c) în cazul unor activități cibernetice răuvoitoare cu o dimensiune militară, statul membru solicitant ar trebui să informeze Conferința comandanților Comandamentului Apărării Cibernetice ai Uniunii cu privire la cererea sa.

(27) În cazul unui incident de securitate cibernetică de mare amploare care afectează buna funcționare a serviciilor spațiale esențiale pentru securitatea Uniunii sau a statelor sale membre, EU-CyCLONe ar trebui să informeze Înaltul Reprezentant în vederea coordonării unui posibil răspuns cu arhitectura de răspuns la amenințările spațiale instituită în conformitate cu Decizia (PESC) 2021/698 a Consiliului.

V: Redresarea în urma unei crize cibernetice

(28) Statele membre, entitățile și rețelele relevante ale Uniunii ar trebui să colaboreze în etapa de redresare, valorificând lecțiile învățate din exercițiile desfășurate, 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.

VI: Comunicații securizate

---

[20] Rezerva UE pentru securitate cibernetică este un mecanism care constă în servicii furnizate, la cerere, de furnizori de încredere de servicii de securitate gestionate pentru a sprijini răspunsul și a iniția acțiuni de redresare în cazul unor incidente de securitate cibernetică semnificative, al unor incidente de securitate cibernetică de mare amploare sau al unor incidente de securitate cibernetică echivalente cu cele de mare amploare care afectează statele membre, instituțiile, organele, oficiile sau agențiile Uniunii sau țările terțe asociate la DEP.

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

(29) Pe baza cartografierii instrumentelor de comunicații securizate existente[22], Comisia, Înaltul Reprezentant, EU-CyCLONe, rețeaua CSIRT și entitățile relevante ale Uniunii ar trebui să convină, până la sfârșitul anului 2026, asupra unui set interoperabil de soluții de comunicare securizată pentru actorii relevanți din Uniune. Aceste soluții ar trebui să acopere întreaga gamă de moduri de comunicare necesare [voce, date, video-teleconferință (VTC), mesagerie, colaborare și schimb de documente și consultare]. Soluțiile ar trebui să reflecte principii-cheie precum interesele Uniunii în materie de securitate, suveranitatea tehnologică și confidențialitatea, precum și caracteristici precum utilizabilitatea, securitatea de la stadiul conceperii, certificarea de către organismele europene de securitate a informațiilor, criptarea de la un capăt la altul, autentificarea, disponibilitatea și criptografia post-cuantică. Soluțiile ar trebui să îndeplinească cerințe definite în comun pentru protecția informațiilor sensibile neclasificate și să includă instrumente pentru schimbul de informații RESTREINT UE/EU RESTRICTED.

(30) Pe această bază, actorii de la nivelul Uniunii ar trebui să utilizeze soluții bazate pe protocolul Matrix pentru comunicarea în timp real. Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) instituit în temeiul Regulamentului (UE) 2021/887, fără a aduce atingere viitorului cadru financiar multianual, ar trebui să ia în considerare finanțarea prin intermediul programului „Europa digitală” pentru a sprijini statele membre în implementarea acestor instrumente.

(31) În special, entitățile UE și statele membre ar trebui să elaboreze planuri de contingență pentru crize grave în care canalele normale de comunicații care se bazează pe internet sau pe rețele de telecomunicații ar fi perturbate sau indisponibile.

(32) Pe termen mediu, ar trebui instituite mecanisme de comunicare și de schimb de informații între autoritățile de aplicare a legii și rețelele de securitate cibernetică, în special la nivel tehnic, pentru un răspuns eficace în situații de criză. Aceste mecanisme ar trebui să respecte rolul fiecărei părți și să evite interferența cu operațiunile în curs. Comisia colaborează cu statele membre în vederea instituirii Sistemului european de comunicații critice (EUCCS), care ar trebui să conecteze până în 2030 rețelele de comunicații ale autorităților de aplicare a legii și ale protecției civile din întregul spațiu Schengen, astfel încât echipamentele critice de comunicații să poată fi utilizate și pe teritoriul altor state membre. Prin urmare, EUCCS poate aduce beneficii și răspunsului comun cu comunitățile cibernetice relevante. Acest sistem ar trebui să includă comunicații de rezervă, de exemplu prin comunicații prin satelit.

VII: Coordonarea crizelor cibernetice cu actorii militari

(33) EU-CyCLONe și Conferința comandanților Comandamentului Apărării Cibernetice ai UE, MICNET și rețeaua CSIRT, precum și viitorul Centru de coordonare a apărării cibernetice al UE și omologii săi civili din Uniune ar trebui să coopereze pentru a dezvolta conștientizarea comună a situației între actorii civili și militari.

(34) Ținând seama de acordurile existente, cum ar fi acordul tehnic CERT-UE/NATO din 2016, Uniunea ar trebui să depună eforturi pentru a stabili puncte de contact pentru coordonarea cu NATO pentru ca în cazul unei crize cibernetice să facă schimb de informațiile necesare cu privire la situație și la utilizarea mecanismelor de răspuns în

[22] HWPCI WK 862/23.

situații de criză. În acest scop, Uniunea ar trebui să exploreze cum ar putea îmbunătăți capacitățile de schimb de informații cu NATO, inclusiv prin posibile interconexiuni între sistemele informatice și de comunicații ale celor două entități.

(35) În cazul în care, în contextul unui incident de securitate cibernetică, un stat membru utilizează inițiative relevante în domeniul apărării, cum ar fi echipele de răspuns rapid în domeniul cibernetic și asistența reciprocă în ceea ce privește securitatea cibernetică (CRRT) din cadrul PESCO sau alte inițiative relevante, cum ar fi echipele Uniunii de răspuns rapid în caz de amenințări hibride (HRRT), acesta ar trebui să informeze EU-CyCLONe, precum și Conferința comandanților Comandamentului Apărării Cibernetice ai UE.

VIII: Cooperarea cu partenerii strategici

(36) Înaltul Reprezentant, în strânsă cooperare cu Comisia și cu alte entități relevante ale Uniunii, ar trebui:

(a) în cazul în care se identifică un incident relevant, să faciliteze fluxul de informații necesare cu partenerii strategici;

(b) să consolideze coordonarea cu partenerii strategici în ceea ce privește răspunsul la activitățile cibernetice răuvoitoare susținute inițiate de actori care generează amenințări persistente, în special atunci când se utilizează setul de instrumente pentru diplomația cibernetică, în conformitate cu orientările sale de punere în aplicare.

(37) Statele membre, Înaltul Reprezentant, Comisia și alte entități relevante ale Uniunii ar trebui să colaboreze cu partenerii strategici și cu organizațiile internaționale pentru a promova bunele practici și comportamentul responsabil al statelor în spațiul cibernetic și pentru a asigura o reacție rapidă și coordonată în cazul unor incidente cibernetice potențiale sau de mare amploare.

(38) Ca parte a ciclului continuu de exerciții menționat în secțiunea II de mai sus, serviciile Comisiei și SEAE ar trebui să ia în considerare organizarea unui exercițiu comun al personalului pentru a testa cooperarea dintre componenta civilă și cea militară în cazul unui incident cibernetic de mare amploare care ar afecta statele membre ale Uniunii și aliații NATO, inclusiv în cazul în care este activat sau este posibil să fie activat articolul 4 sau 5 din Tratatul NATO.

(39) Având în vedere expunerea țărilor candidate și potențialul ca incidente cibernetice să aibă loc în vecinătatea Uniunii, ar trebui avute în vedere exerciții comune care să implice țările candidate.

Adoptată la Bruxelles,

Pentru Consiliu,

Președintele