Consiliul
Uniunii Europene

Bruxelles, 18 noiembrie 2024
(OR. en)

15644/24

Dosar interinstituțional:
2023/0109(COD)

CODEC 2118
CYBER 326
TELECOM 335
CADREFIN 188
FIN 1009
BUDGET 63
IND 514
JAI 1656
MI 926
DATAPROTECT 318
RELEX 1429
PE 252

NOTĂ DE INFORMARE

Sursă:	Secretariatul General al Consiliului
Destinatar:	Comitetul Reprezentanților Permanenți / Consiliul
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor - Rezultatul primei lecturi a Parlamentului European și procedura de rectificare (Strasbourg, 24 aprilie 2024 și Bruxelles, 14 noiembrie 2024)

I. INTRODUCERE

În conformitate cu dispozițiile articolului 294 din TFUE și cu Declarația comună privind aspectele practice în cadrul procedurii de codecizie[1], între Consiliu, Parlamentul European și Comisie au avut loc o serie de contacte informale în vederea obținerii unui acord în primă lectură cu privire la acest dosar legislativ.

[1] JO C 145, 30.6.2007, p. 5.

Era prevăzut ca acest dosar[2] să facă obiectul procedurii de rectificare[3] în cadrul Parlamentului European, după adoptarea de către Parlamentul European precedent a poziției sale în primă lectură.

II. VOTURI

În ședința sa din 24 aprilie 2024, Parlamentul European a adoptat amendamentul 2 (fără revizuirea de către experții juriști-lingviști) la propunerea Comisiei, amendamentul 3 care conține o declarație a Comisiei și o rezoluție legislativă, constituind poziția Parlamentului European în primă lectură. Aceasta reflectă acordul provizoriu la care s-a ajuns între instituții.

După finalizarea de către experții juriști-lingviști a textului adoptat, Parlamentul European a aprobat, la 14 noiembrie 2024, o rectificare la poziția adoptată în primă lectură.

Cu această rectificare, Consiliul ar trebui să fie în măsură să aprobe poziția Parlamentului European, astfel cum figurează în anexa[4] la prezenta notă, încheind astfel prima lectură pentru ambele instituții.

Actul ar urma apoi să fie adoptat cu formularea care corespunde poziției Parlamentului European.

---

[2] Doc. 10819/24 + COR 1.

[3] Articolul 251 din Regulamentul de procedură al PE.

[4] Textul rectificării figurează în anexă. Aceasta se prezintă sub forma unui text consolidat, în care modificările la propunerea Comisiei sunt evidențiate prin caractere aldine cursive. Simbolul „▌” indică părți eliminate din text.

ANEXĂ
(14.11.2024)

P9_TA(2024)0355

Regulamentul privind solidaritatea cibernetică

Rezoluția legislativă a Parlamentului European din 24 aprilie 2024 referitoare la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Procedura legislativă ordinară: prima lectură)

Parlamentul European,

– având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2023)0209),

– având în vedere articolul 294 alineatul (2), articolul 173 alineatul (3) și articolul 322 alineatul (1) litera (a) din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată de către Comisie (C9-0136/2023),

– având în vedere articolul 294 alineatul (3) din Tratatul privind funcționarea Uniunii Europene,

– având în vedere avizul Curții de Conturi din 18 aprilie 2023[1],

– având în vedere avizul Comitetului Economic și Social European din 13 iulie 2023[2],

– având în vedere avizul Comitetului Regiunilor din 30 noiembrie 2023[3],

– având în vedere acordul provizoriu aprobat de comisia competentă în temeiul articolului 74 alineatul (4) din Regulamentul său de procedură și angajamentul reprezentantului Consiliului, exprimat în scrisoarea din 21 martie 2024, de a aproba poziția Parlamentului în conformitate cu articolul 294 alineatul (4) din Tratatul privind funcționarea Uniunii Europene,

– având în vedere articolul 59 din Regulamentul său de procedură,

– având în vedere avizul Comisiei pentru afaceri externe și cel al Comisiei pentru transport și turism,

– având în vedere raportul Comisiei pentru industrie, cercetare și energie (A9-0426/2023),

---

1 Nepublicat încă în Jurnalul Oficial.
2 JO C 349, 29.9.2023, p. 167.
3 JO C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.

1. adoptă poziția sa în primă lectură prezentată în continuare;

2. ia act de declarația Comisiei anexată la prezenta rezoluție, care va fi publicată în seria C a *Jurnalului Oficial al Uniunii Europene*;

3. solicită Comisiei să îl sesizeze din nou în cazul în care își înlocuiește, își modifică în mod substanțial sau intenționează să-și modifice în mod substanțial propunerea;

4. încredințează Președintei sarcina de a transmite Consiliului și Comisiei, precum și parlamentelor naționale poziția Parlamentului.

P9_TC1-COD(2023)0109

Poziția Parlamentului European adoptată în primă lectură la 24 aprilie 2024 în vederea adoptării Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului 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)*

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 173 alineatul (3) și articolul 322 alineatul (1) litera (a),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Curții de Conturi[1],

având în vedere avizul Comitetului Economic și Social European[2],

având în vedere avizul Comitetului Regiunilor[3],

hotărând în conformitate cu procedura legislativă ordinară[4],

---

1 ***Avizul din 18 aprilie 2023 (nepublicat încă în Jurnalul Oficial).***
2 ***JO C 349, 29.9.2023, p. 167.***
3 ***JO C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.***
4 ***Poziția Parlamentului European din 24 aprilie 2024.***

întrucât:

(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică ***și în societate***, ***având în vedere interconectarea și interdependența tot mai mari*** ale administrațiilor publice ale statelor membre, ale întreprinderilor și ale cetățenilor la nivel transsectorial și transfrontalier***, ceea ce creează totodată posibile vulnerabilități***.

(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică, inclusiv numărul atacurilor asupra lanțului de aprovizionare în scopul spionajului cibernetic, al ransomware-ului sau al perturbării, sunt în creștere ***la nivelul Uniunii și la nivel mondial***. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unor posibile incidente de securitate cibernetică de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită ***a cadrului*** de securitate cibernetică al Uniunii. Această amenințare depășește ***războiul de agresiune al Rusiei împotriva*** Ucrainei și este susceptibilă să persiste, având în vedere multitudinea de actori ▌ implicați în tensiunile geopolitice actuale. Astfel de incidente pot împiedica furnizarea serviciilor publice***, deoarece atacurile cibernetice vizează frecvent serviciile și infrastructurile publice locale, regionale sau naționale, autoritățile locale fiind deosebit de vulnerabile, inclusiv din cauza resurselor lor limitate. Incidentele pot să împiedice*** și desfășurarea activităților economice, inclusiv în sectoarele ***cu o importanță critică ridicată sau alte sectoare de importanță critică***, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei ***și sistemelor democratice ale*** Uniunii și ar putea avea chiar consecințe asupra sănătății sau asupra vieții.

În plus, incidentele de securitate cibernetică sunt imprevizibile, deoarece adesea apar și evoluează rapid, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări. ***Este așadar necesară o cooperare strânsă între sectorul public, sectorul privat, mediul academic, societatea civilă și mass-media.***

(3) Este necesară consolidarea poziției competitive a industriei și a serviciilor din Uniune în cadrul economiei digitale și sprijinirea transformării digitale a acestora, prin consolidarea nivelului de securitate cibernetică pe piața unică digitală***,*** astfel cum se recomandă în trei propuneri diferite ale Conferinței privind viitorul Europei. Este necesar să se sporească reziliența cetățenilor, a întreprinderilor***, în special a microîntreprinderilor, a întreprinderilor mici și mijlocii și a întreprinderilor nou-înființate***, precum și a entităților care operează infrastructuri critice***,*** împotriva amenințărilor cibernetice tot mai mari, care pot avea un impact societal și economic devastator. Prin urmare, sunt necesare investiții în infrastructuri și servicii ***și consolidarea capacităților pentru a dezvolta competențe în materie de securitate cibernetică*** care vor sprijini o detectare mai rapidă a amenințărilor cibernetice și a incidentelor și răspunsul mai rapid la acestea. În plus, statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare și pentru a răspunde mai bine la acestea, precum ***și de asistență în etapa inițială de redresare*** în urma unor astfel de incidente. ***Dezvoltând structurile deja existente și în strânsă cooperare cu acestea***, Uniunea ar trebui să își sporească capacitățile în domeniile respective, în special în ceea ce privește colectarea și analiza datelor privind amenințările cibernetice și incidentele.

(4) Uniunea a luat deja o serie de măsuri pentru a reduce vulnerabilitățile și a spori reziliența infrastructurilor și a entităților critice împotriva riscurilor, în special Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[5], Directivele 2013/40/UE[6] și (UE) 2022/2555[7] ale Parlamentului European și ale Consiliului și Recomandarea (UE) 2017/1584 a Comisiei[8]. În plus, Recomandarea Consiliului din 8 decembrie 2022 privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri și să coopereze între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile vizate, pentru a spori reziliența infrastructurii critice utilizate pentru a furniza servicii esențiale pe piața internă.

5 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).

6 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).

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

8 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).

(5) Riscurile tot mai mari în materie de securitate cibernetică și un peisaj general complex al amenințărilor, cu un risc clar de propagare rapidă a incidentelor de la un stat membru la altul și de la o țară terță la Uniune, necesită ***consolidarea*** solidarității la nivelul Uniunii pentru o mai bună detectare a amenințărilor cibernetice și a incidentelor, o mai bună pregătire legată de acestea, ***un răspuns mai bun la acestea și o mai bună redresare în urma lor, mai ales prin întărirea capacităților structurilor deja disponibile.*** În plus, Concluziile Consiliului din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene au invitat Comisia să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică.

(6) Comunicarea comună a Comisiei și a Înaltului Reprezentant pentru politica externă și de securitate comună din 10 noiembrie 2022 către Parlamentul European și Consiliu privind politica UE în domeniul apărării cibernetice a anunțat o inițiativă a UE privind solidaritatea cibernetică cu obiectivele de a consolida capacitățile comune de detectare, de conștientizare a situației și de răspuns la nivelul UE prin promovarea implementării unei infrastructuri a UE de centre de operațiuni de securitate (SOC), de a sprijini crearea treptată a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și de a testa entitățile critice în vederea identificării vulnerabilităților potențiale pe baza evaluărilor riscurilor la nivelul UE.

(7) Este necesar să se consolideze detectarea și conștientizarea situației privind amenințările cibernetice și incidentele în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capacităților statelor membre și ale Uniunii de ***a preveni*** incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare ***și de a răspunde la acestea***. Prin urmare, ar trebui să fie ***creată*** o ***rețea*** paneuropeană de ***centre cibernetice*** (denumită în continuare „***sistemul european de alertă în materie de securitate cibernetică”***) pentru a crea capacități de detectare ***coordonată și de conștientizare a situației, întărind totodată capacitățile Uniunii de detectare a amenințărilor și de partajare de informații***; ar trebui să fie instituit un mecanism pentru situații de urgență în materie de securitate cibernetică pentru a sprijini statele membre***, la cererea acestora,*** să se pregătească pentru incidente de securitate cibernetică semnificative și incidente de securitate cibernetică de mare amploare, să răspundă la acestea, să atenueze impactul acestora și să inițieze redresarea în urma lor, precum și să sprijine alți utilizatori ***să răspundă la*** incidentele de securitate cibernetică semnificative și la incidentele de securitate cibernetică ***echivalente cu*** cele de mare amploare; ar trebui să fie instituit un mecanism european de analiză a incidentelor de securitate cibernetică pentru a analiza și a evalua incidentele de securitate cibernetică semnificative sau incidentele de securitate cibernetică de mare amploare specifice***. Acțiunile întreprinse în temeiul prezentului regulament ar trebui să se desfășoare cu respectarea competențelor statelor membre și ar trebui să completeze activitățile desfășurate de rețeaua CSIRT, de Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) sau de Grupul de cooperare (denumit în continuare „Grupul de cooperare NIS”), instituite în temeiul Directivei (UE) 2022/2555***, ***evitând paralelismele.*** Acțiunile respective nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene (TFUE).

(8) Pentru a realiza obiectivele respective, este necesar să se modifice Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului[9] în anumite domenii. În special, prezentul regulament ar trebui să modifice Regulamentul (UE) 2021/694 în ceea ce privește adăugarea unor noi obiective operaționale legate de ***sistemul european de alertă în materie de securitate cibernetică*** și de mecanismul pentru situații de urgență în materie de securitate cibernetică în cadrul obiectivului specific nr. 3 ***din programul „Europa digitală" (DEP)***, care vizează garantarea rezilienței, a integrității și credibilității pieței unice digitale, consolidarea capacităților de monitorizare a atacurilor cibernetice și a amenințărilor cibernetice și de răspuns la acestea, precum și consolidarea cooperării ***și coordonării*** transfrontaliere în materie de securitate cibernetică. ***Sistemul european de alertă în materie de securitate cibernetică ar putea avea un rol important în sprijinirea statelor membre în anticiparea amenințărilor cibernetice și în protejarea împotriva acestora, iar rezerva UE pentru securitate cibernetică ar putea juca un rol important în sprijinirea statelor membre, a instituțiilor, organelor, oficiilor și agențiilor Uniunii și a țărilor terțe asociate la DEP în răspunsul la incidentele de securitate cibernetică semnificative, incidentele de securitate cibernetică de mare amploare și incidentele de securitate cibernetică echivalente cu cele de mare amploare și în atenuarea impactului acestora.***

[9] ***Regulamentul*** (UE) 2021/694 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a programului „Europa digitală" și de abrogare a Deciziei (UE) 2015/2240 (JO L 166, 11.5.2021, p. 1).

Impactul respectiv ar putea include prejudicii materiale sau morale considerabile și riscuri grave în materie de securitate și siguranță publică. Având în vedere rolurile specifice pe care le-ar putea avea sistemul european de alertă în materie de securitate cibernetică și rezerva UE pentru securitate cibernetică, prezentul regulament ar trebui să modifice Regulamentul (UE) 2021/694 în ceea ce privește participarea entităților juridice care sunt stabilite în Uniune, dar sunt controlate din țări terțe, în cazul în care există un risc real ca instrumentele, infrastructurile sau serviciile necesare și suficiente sau tehnologia, cunoștințele de specialitate și capacitatea să nu fie disponibile în Uniune, iar beneficiile includerii unor astfel de entități să depășească riscul de securitate. Ar trebui să fie stabilite condițiile specifice în care se poate acorda sprijin financiar pentru acțiunile ***de punere în aplicare a sistemului european de alertă în materie de securitate cibernetică și a rezervei UE pentru securitate cibernetică*** și ar trebui să fie definite mecanismele de guvernanță și coordonare necesare pentru atingerea obiectivelor preconizate. Alte modificări ale Regulamentului (UE) 2021/694 ar trebui să includă descrieri ale acțiunilor propuse în cadrul noilor obiective operaționale, precum și indicatori măsurabili pentru monitorizarea punerii în aplicare a respectivelor noi obiective operaționale.

(9) Pentru a consolida răspunsul Uniunii la amenințările cibernetice și la incidente, este vitală cooperarea cu organizațiile internaționale, precum și cu partenerii internaționali de încredere cu valori comune. În acest context, prin „parteneri internaționali de încredere și cu valori comune" ar trebui să se înțeleagă țările care împărtășesc principiile pe care se întemeiază Uniunea, și anume democrația, statul de drept, universalitatea și indivizibilitatea drepturilor omului și a libertăților fundamentale, respectarea demnității umane, principiile egalității și solidarității, precum și respectarea principiilor Cartei Organizației Națiunilor Unite și a dreptului internațional și care nu subminează interesele esențiale de securitate ale Uniunii sau ale statelor sale membre.

O astfel de cooperare ar putea fi benefică și în ceea ce privește acțiunile întreprinse în temeiul prezentul regulament, în special sistemul european de alertă în materie de securitate cibernetică și rezerva UE pentru securitate cibernetică. Regulamentul (UE) 2021/694 ar trebui să prevadă, dacă sunt îndeplinite anumite condiții de disponibilitate și de securitate, ca licitațiile pentru sistemul european de alertă în materie de securitate cibernetică și rezerva UE pentru securitate cibernetică să fie deschise entităților juridice controlate din țări terțe, sub rezerva cerințelor de securitate. Atunci când se evaluează riscul de securitate al deschiderii achizițiilor publice în acest mod, este important să se țină seama de principiile și valorile pe care Uniunea le împărtășește cu parteneri internaționali cu valori comune, în cazul în care principiile și valorile respective sunt legate de interesele esențiale de securitate ale Uniunii. În plus, în cazul în care astfel de cerințe de securitate sunt în curs de examinare în temeiul Regulamentului (UE) 2021/694, ar putea fi luate în considerare mai multe elemente, cum ar fi structura corporativă și procesul decizional al unei entități, securitatea datelor și a informațiilor clasificate sau sensibile și asigurarea faptului că rezultatele acțiunii nu fac obiectul unui control sau al unor restricții din partea unor țări terțe neeligibile.

(10) Finanțarea acțiunilor în temeiul prezentului regulament ar trebui să fie prevăzută în Regulamentul (UE) 2021/694, care ar trebui să rămână actul de bază relevant pentru acțiunile consacrate în cadrul obiectivului specific nr. 3 al DEP. În programele de lucru relevante urmează să fie prevăzute condiții specifice de participare pentru fiecare acțiune, în conformitate cu Regulamentul (UE) 2021/694.

(11) Prezentului regulament i se aplică normele financiare orizontale adoptate de Parlamentul European și de Consiliu în temeiul articolului 322 din TFUE. Respectivele norme sunt prevăzute în ***Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului***[10] și determină, în special, procedura de stabilire și execuție a bugetului Uniunii și prevăd controale privind responsabilitatea actorilor financiari. Normele adoptate în temeiul articolului 322 din TFUE includ, de asemenea, un regim general de condiționalitate pentru protecția bugetului Uniunii, astfel cum este stabilit în Regulamentul (UE, Euratom) 2020/2092 al Parlamentului European și al Consiliului[11].

---

10 ***Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului din 23 septembrie 2024 privind normele financiare aplicabile bugetului general al Uniunii (JO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).***

11 ***Regulamentul (UE, Euratom) 2020/2092 al Parlamentului European și al Consiliului din 16 decembrie 2020 privind un regim general de condiționalitate pentru protecția bugetului Uniunii (JO L 433 I, 22.12.2020, p. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

(12) Deși măsurile de prevenire și de pregătire sunt esențiale pentru o mai bună reziliență a Uniunii pentru a putea reacționa la incidentele de securitate cibernetică semnificative, la incidentele de securitate cibernetică de mare amploare și la incidentele de securitate cibernetică echivalente cu cele de mare amploare, frecvența, momentul la care survin și amploarea unor astfel de incidente sunt, prin natura lor, imprevizibile. Resursele financiare necesare pentru un răspuns adecvat pot varia mult de la un an la altul și ar trebui să fie disponibile de urgență. Prin urmare, reconcilierea principiului bugetar al previzibilității cu necesitatea de a reacționa rapid la noile necesități presupune nevoia de adaptare a execuției financiare a programelor de lucru. Prin urmare, este oportun să se autorizeze reportarea creditelor neutilizate, dar numai în exercițiul următor și doar pentru rezerva UE pentru securitate cibernetică și pentru acțiunile de asistență reciprocă, în plus față de reportarea creditelor autorizată în temeiul articolului 12 alineatul (4) din Regulamentul (UE, Euratom) 2024/2509.

(13) Pentru a preveni și a evalua într-un mod mai eficace amenințările cibernetice și incidentele, a răspunde mai eficace la acestea ***și a asigura redresarea mai eficace în urma lor,*** este necesar să se dezvolte cunoștințe mai cuprinzătoare cu privire la amenințările la adresa activelor și infrastructurilor critice de pe teritoriul Uniunii, inclusiv cu privire la distribuția geografică, interconectarea și efectele potențiale ale acestora în cazul atacurilor cibernetice care afectează infrastructurile respective. ***O abordare proactivă la identificarea, atenuarea și prevenirea amenințărilor cibernetice presupune o capacitate sporită în ceea ce privește capacitățile avansate de detectare. Sistemul european de alertă în materie de securitate cibernetică ar trebui să fie format din mai multe centre cibernetice transfrontaliere interoperaționale, fiecare grupând trei sau mai multe centre cibernetice naționale.*** Infrastructura respectivă ar trebui să servească intereselor și nevoilor naționale și ale Uniunii în materie de securitate cibernetică, valorificând ***tehnologia de ultimă generație pentru instrumente avansate de colectare a datelor și informațiilor relevante, anonimizate dacă este cazul,*** și de analiză a datelor, consolidând ***în mod coordonat*** capacitățile de detectare și gestionare a incidentelor de securitate cibernetică și asigurând conștientizarea în timp real a situației. Infrastructura respectivă ar trebui să servească ***la îmbunătățirea poziției în materie de securitate cibernetică, prin creșterea gradului de detectare, agregare și analiză a datelor și informațiilor, cu scopul de a preveni*** amenințările cibernetice și incidentele și, prin urmare, să completeze și să sprijine entitățile și rețelele Uniunii responsabile de gestionarea crizelor cibernetice în Uniune, în special EU-CyCLONe .

(14) ***Statele membre participă voluntar la sistemul european de alertă în materie de securitate cibernetică.*** Fiecare stat membru ar trebui să desemneze un organism ***unic*** la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. Respectivele ***centre cibernetice*** naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea la ***sistemul european de alertă în materie de securitate cibernetică*** și ar trebui să se asigure că informațiile privind amenințările cibernetice provenite de la entități publice și private sunt partajate și colectate la nivel național într-un mod eficace și raționalizat. ***Centrele cibernetice naționale ar putea întări cooperarea și partajarea de informații între entitățile publice și private și ar putea sprijini, de asemenea, schimbul de date și informații relevante cu comunitățile sectoriale și transsectoriale relevante, inclusiv cu centrele relevante de partajare de informații și analiză din industrie (ISAC). Cooperarea strânsă și coordonată între entitățile publice și private este esențială pentru consolidarea rezilienței cibernetice a Uniunii. O astfel de cooperare este deosebit de valoroasă în contextul partajării de informații privind amenințările cibernetice pentru a îmbunătăți protecția cibernetică activă. În cadrul acestei cooperări și al partajării de informații, centrele cibernetice naționale ar putea solicita și primi informații specifice.***

Respectivele centre cibernetice naționale nu sunt nici obligate, nici împuternicite prin prezentul regulament să asigure îndeplinirea unor astfel de cereri. După caz și în conformitate cu dreptul Uniunii și cu dreptul intern, informațiile solicitate sau primite ar putea include date de telemetrie, de senzori și de intrare de la diverse entități, cum ar fi furnizorii de servicii de securitate, care își desfășoară activitatea în sectoare cu o importanță critică ridicată sau în alte sectoare de importanță critică din statul membru respectiv, pentru a îmbunătăți detectarea rapidă și timpurie a potențialelor amenințări cibernetice și incidente, pentru o mai bună conștientizare a situației. Dacă centrul cibernetic național nu este totodată și autoritatea competentă desemnată sau instituită de statul membru relevant în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, este esențial ca centrul respectiv să se coordoneze cu autoritatea competentă respectivă pentru cererile care privesc astfel de date și primirea unor astfel de date.

(15) ***Ca parte a sistemului european de alertă în materie de securitate cibernetică,*** ar trebui să fie înființate o serie de centre ***cibernetice transfrontaliere***. Respectivele centre cibernetice transfrontaliere ar trebui să reunească ***centre cibernetice*** naționale din cel puțin trei state membre, pentru a asigura că beneficiile detectării amenințărilor transfrontaliere și ale partajării și gestionării informațiilor pot fi realizate pe deplin. Obiectivul general al ***centrelor cibernetice*** transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor cibernetice și sprijinirea producerii de informații de înaltă calitate privind amenințările cibernetice, în special prin partajarea de ***informații relevante, anonimizate dacă este cazul, într-un mediu sigur și fiabil,*** din diferite surse, publice sau private, precum și prin partajarea și utilizarea în comun a instrumentelor de ultimă generație și prin dezvoltarea în comun a capacităților de detectare, analiză și prevenire într-un mediu ***sigur și*** de încredere. ***Centrele cibernetice*** transfrontaliere ar trebui să ofere noi capacități suplimentare, pe baza și în completarea SOC-urilor ***și a echipelor CSIRT*** existente și a altor actori relevanți***, printre care rețeaua CSIRT***.

(16) Un stat membru selectat de Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) instituit prin Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului[12] în urma unei cereri de exprimare a interesului pentru a înființa un centru cibernetic național sau pentru a consolida capacitățile unui astfel de centru ar trebui să achiziționeze instrumente, infrastructuri sau servicii relevante în comun cu ECCC. Un astfel de stat membru ar trebui să fie eligibil pentru un grant pentru exploatarea instrumentelor, infrastructurilor sau serviciilor. Un consorțiu-gazdă format din cel puțin trei state membre, care a fost selectat de ECCC în urma unei cereri de exprimare a interesului pentru înființarea unui centru cibernetic transfrontalier sau pentru consolidarea capacităților unui astfel de centru ar trebui să achiziționeze instrumente, infrastructuri sau servicii relevante în comun cu ECCC. Consorțiul-gazdă ar trebui să fie eligibil pentru a primi un grant pentru exploatarea instrumentelor, infrastructurilor sau serviciilor. Procedura de achiziții pentru achiziționarea instrumentelor, infrastructurilor sau serviciilor relevante ar trebui să fie efectuată în comun de ECCC și de autoritățile contractante relevante din statele membre selectate în urma unor astfel de cereri de exprimare a interesului.

---

[12] ***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).***

O astfel de achiziție ar trebui să respecte prevederile de la articolul 168 alineatul (2) din Regulamentul (UE) 2024/2509 și normele financiare aplicabile ECCC. Prin urmare, entitățile private nu ar trebui să fie eligibile pentru a participa la cererile de exprimare a interesului de a achiziționa instrumente, infrastructuri sau servicii în comun cu ECCC sau de a primi granturi pentru exploatarea instrumentelor, infrastructurilor sau serviciilor. Cu toate acestea, statele membre ar trebui să aibă posibilitatea de a implica entități private în crearea, consolidarea și funcționarea centrelor lor cibernetice naționale și a centrelor cibernetice transfrontaliere în alte moduri pe care le consideră adecvate, în conformitate cu dreptul Uniunii și cu dreptul intern. Entitățile private ar putea fi totodată eligibile pentru a primi finanțare din partea Uniunii în temeiul Regulamentului (UE) 2021/887 pentru a oferi sprijin centrelor cibernetice naționale.

(17) Pentru a îmbunătăți detectarea amenințărilor cibernetice și conștientizarea situației în Uniune, un stat membru care este selectat în urma unei cereri de exprimare a interesului să înființeze un centru cibernetic național sau să consolideze capacitățile unui astfel de centru ar trebui să se angajeze să solicite participarea la un centru cibernetic transfrontalier. Dacă un stat membru nu participă la un centru cibernetic transfrontalier în termen de doi ani de la data la care sunt achiziționate instrumentele, infrastructurile sau serviciile sau de la data la care primește finanțare sub formă de granturi, luându-se în considerare data care survine mai întâi, acesta nu ar trebui să fie eligibil să participe la alte acțiuni de sprijin ale Uniunii în cadrul sistemului european de alertă în materie de securitate cibernetică pentru a consolida capacitățile centrului său cibernetic național. În astfel de cazuri, entitățile din statele membre ar putea participa în continuare la cereri de propuneri pe alte teme în cadrul DEP sau al altor programe de finanțare ale Uniunii, inclusiv la cereri de propuneri privind capacitățile de detectare cibernetică și de partajare de informații, cu condiția ca entitățile respective să îndeplinească criteriile de eligibilitate stabilite în programele respective.

(18) ▌ Echipele CSIRT fac schimb de informații în cadrul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. ***Sistemul european de alertă în materie de securitate cibernetică*** ar trebui să constituie o nouă capacitate care să fie complementară rețelei CSIRT, ***contribuind la mai buna conștientizare a situației la nivelul Uniunii, permițând consolidarea capacităților*** rețelei CSIRT***. Centrele cibernetice transfrontaliere ar trebui să se coordoneze și să coopereze îndeaproape cu rețeaua CSIRT. Acestea ar trebui să acționeze prin punerea în comun a datelor și prin partajarea de informații relevante, anonimizate dacă este cazul, privind*** amenințările cibernetice care provin de la entități publice și private, sporind valoarea acestor date și informații prin analize de specialitate și infrastructuri achiziționate în comun și ***instrumente de ultimă generație și contribuind la suveranitatea tehnologică a Uniunii, la autonomia sa strategică deschisă, la competitivitatea și reziliența sa, precum și la dezvoltarea capacităților Uniunii.***

(19) ***Centrele cibernetice transfrontaliere*** ar trebui să acționeze ca puncte centrale care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind amenințările cibernetice și să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de ***părți interesate, precum*** echipele de intervenție în caz de urgență informatică (CERT), echipele CSIRT, centrele de schimb de informații și de analiză (ISAC) și operatorii de infrastructuri critice. ***Membrii unui consorțiu-gazdă ar trebui să specifice în acordul de consorțiu informațiile relevante care urmează să fie partajate între participanții la centrul cibernetic transfrontalier în cauză.*** Informațiile care fac obiectul unui schimb între participanții la un ***centru cibernetic*** transfrontalier ar putea include, ***de exemplu***, date provenite de la rețele și senzori, fluxuri de informații privind amenințările, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări cibernetice, ***incidente evitate la limită, vulnerabilități, tehnici și proceduri, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurarea instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice***. În plus, ***centrele cibernetice*** transfrontaliere ar trebui să încheie acorduri de cooperare între ele.

Astfel de acorduri de cooperare ar trebui, în special, să specifice principiile partajării de informații și interoperabilitatea. Clauzele lor privind interoperabilitatea, în special formatele și protocoalele pentru partajarea de informații, ar trebui să fie ghidate de orientările de interoperabilitate emise de Agenția Uniunii Europene pentru Securitate Cibernetică instituită prin Regulamentul (UE) 2019/881 (ENISA) și, prin urmare, să aibă ca punct de plecare orientările respective. Orientările respective ar trebui să fie emise rapid pentru a se asigura că pot fi luate în considerare de centrele cibernetice transfrontaliere într-un stadiu incipient. Acestea ar trebui să țină seama de standardele internaționale, de cele mai bune practici și de funcționarea existentă a centrelor cibernetice transfrontaliere existente.

(20) Centrele cibernetice transfrontaliere și rețeaua CSIRT ar trebui să coopereze îndeaproape pentru a asigura sinergiile și complementaritatea activităților. În acest scop, acestea ar trebui să convină asupra unor acorduri procedurale privind cooperarea și partajarea de informații relevante. Aceasta ar putea include partajarea de informații relevante privind amenințările cibernetice și incidentele de securitate cibernetică semnificative și asigurarea faptului că se partajează cu rețeaua CSIRT experiența cu instrumente de ultimă generație, în special inteligența artificială și tehnologia de analiză a datelor, utilizate în cadrul centrelor cibernetice transfrontaliere.

(21) Conștientizarea comună a situației în rândul autorităților relevante reprezintă o condiție prealabilă indispensabilă pentru pregătirea și coordonarea la nivelul Uniunii în ceea ce privește incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare. Directiva (UE) 2022/2555 a instituit EU-CyCLONe pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele, ***oficiile*** și agențiile Uniunii. ***Directiva (UE) 2022/2555 a instituit și rețeaua CSIRT, pentru a asigura rapiditatea și eficacitatea cooperării operaționale dintre statele membre. Pentru a asigura conștientizarea situației și pentru a consolida solidaritatea, în situațiile în care centrele cibernetice transfrontaliere obțin informații legate de un incident de securitate cibernetică de mare amploare potențial sau aflat în curs, acestea ar trebui să furnizeze informații relevante rețelei CSIRT și să informeze, ca alertă timpurie, EU-CyCLONe. În funcție de situație, informațiile care urmează să fie partajate ar putea include în special informații tehnice, informații cu privire la natura și motivele atacatorului sau ale atacatorului potențial, precum și informații fără caracter tehnic de nivel superior cu privire la un incident de securitate cibernetică de mare amploare potențial sau aflat în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.***

Directiva (UE) 2022/2555 reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii (UCPM) instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului[13], precum și responsabilitatea acesteia de a furniza rapoarte analitice pentru mecanismul integrat al ***Uniunii*** pentru un răspuns politic la crize (denumit în continuare „mecanismul IPCR") în temeiul Deciziei de punere în aplicare (UE) 2018/1993 a Consiliului[14]. ***În cazul în care centrele cibernetice transfrontaliere partajează informații relevante și avertismente timpurii*** în ceea ce privește un incident de securitate cibernetică ***de mare amploare potențial sau aflat în curs cu EU-CyCLONe și cu rețeaua CSIRT, este imperativ ca informațiile respective să fie partajate prin intermediul rețelelor respective cu autoritățile statelor membre, precum și cu Comisia. În acest sens,*** Directiva (UE) 2022/2555 ***prevede că scopul EU-CyCLONe este de a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele, oficiile și agențiile Uniunii. Printre sarcinile EU-CyCLONe se numără conștientizarea comună a situației în cazul unor astfel de incidente și crize. Este extrem de important ca EU-CyCLONe să se asigure, în conformitate cu acest scop și cu sarcinile sale, că astfel de informații se transmit imediat reprezentanților relevanți ai statelor membre și Comisiei. În acest scop, este esențial ca Regulamentul de procedură al EU-CyCLONe să includă dispoziții adecvate.***

---

13 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, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Decizia de punere în aplicare (UE) 2018/1993 a Consiliului din 11 decembrie 2018 privind mecanismul integrat al Uniunii pentru un răspuns politic la crize (JO L 320, 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(22) Entitățile care participă la ***sistemul european de alertă în materie de securitate cibernetică*** ar trebui să asigure un nivel ridicat de interoperabilitate între ele, inclusiv, după caz, în ceea ce privește formatele de date, taxonomia și instrumentele de manipulare și de analiză a datelor. Acestea ar trebui să asigure, de asemenea, canale de comunicații securizate, un nivel minim de securitate a nivelului de aplicație, un tablou de bord al conștientizării situației și indicatori. Adoptarea unei taxonomii comune și elaborarea unui model pentru rapoartele situaționale în vederea descrierii ***cauzelor amenințărilor cibernetice detectate*** și ***a riscurilor detectate*** ar trebui să țină seama de ***rezultatele obținute în*** notificarea incidentelor în contextul punerii în aplicare a Directivei (UE) 2022/2555.

(23) Pentru a permite schimbul de date ***și informații relevante*** privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere ***și sigur***, entitățile care participă la ***sistemul european de alertă în materie de securitate cibernetică*** ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate ***și ar trebui să dispună de personal calificat***. Acest lucru ar trebui să permită îmbunătățirea capacităților de detectare colectivă și avertizarea în timp util a autorităților și a entităților relevante, în special prin utilizarea celor mai recente tehnologii de inteligență artificială și de analiză a datelor.

(24) Prin colectarea, ***analizarea,*** partajarea și schimbul de date ***și informații relevante***, ***sistemul european de alertă în materie de securitate cibernetică*** ar trebui să consolideze suveranitatea tehnologică a Uniunii, ***și să inaugureze autonomia în materie de securitate cibernetică, competitivitate și reziliență***. Punerea în comun a datelor actualizate de înaltă calitate ***ar putea*** să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. ***Supravegherea de către factorul uman și, în acest scop, o forță de muncă calificată rămân esențiale pentru punerea în comun eficace a unor date de înaltă calitate.***

(25) Deși ***sistemul european de alertă în materie de securitate cibernetică*** este un proiect civil, comunitatea de apărare cibernetică ar putea beneficia de capacități civile mai puternice de detectare și de conștientizare a situației dezvoltate pentru protecția infrastructurii critice. ▌

(26) Partajarea de informații între participanții la ***sistemul european de alertă în materie de securitate cibernetică*** ar trebui să respecte cerințele juridice existente și, în special, dreptul Uniunii și dreptul intern privind protecția datelor, precum și normele Uniunii privind concurența care reglementează schimbul de informații. Destinatarul informațiilor ar trebui să pună în aplicare, în măsura în care prelucrarea datelor cu caracter personal este necesară, măsuri tehnice și organizatorice care să protejeze drepturile și libertățile persoanelor vizate și să distrugă datele de îndată ce acestea nu mai sunt necesare pentru scopul declarat și să informeze entitatea care pune la dispoziție datele că datele au fost distruse.

(27) ***Păstrarea confidențialității și a securității informațiilor este de o importanță capitală pentru toți cei trei piloni ai prezentului regulament, fie pentru încurajarea partajării sau schimbului de informații în contextul sistemului european de alertă în materie de securitate cibernetică, pentru protejarea intereselor entităților care solicită sprijin prin mecanismul pentru situații de urgență în materie de securitate cibernetică, fie pentru asigurarea faptului că rapoartele din cadrul mecanismului european de analiză a incidentelor de securitate cibernetică pot genera învățăminte utile, fără a avea un impact negativ asupra entităților afectate de incidente. Participarea statelor membre și a entităților la mecanismele respective depinde de relațiile de încredere dintre toți participanții lor. Dacă informațiile sunt confidențiale în temeiul normelor Uniunii sau al normelor naționale, partajarea sau schimbul informațiilor respective în temeiul prezentului regulament ar trebui să se limiteze la ceea ce este relevant și proporțional cu scopul partajării sau schimbului de informații. De asemenea, partajarea sau schimbul de informații ar trebui să păstreze confidențialitatea respectivelor informații, inclusiv să protejeze securitatea și interesele comerciale ale entităților în cauză. Partajarea sau schimbul de informații în temeiul prezentului regulament s-ar putea face prin încheierea de acorduri de nedivulgare sau orientări privind distribuția informațiilor, cum ar fi un protocol de tip semafor (TLP). TLP trebuie înțeles drept mijloc de a furniza informații despre orice limitări în ceea ce privește răspândirea ulterioară a informațiilor. Acesta este utilizat în aproape toate echipele CSIRT și în unele echipe ISAC. Pe lângă aceste cerințe generale, în ceea ce privește sistemul european de alertă în materie de securitate cibernetică, acordurile consorțiilor-gazdă ar trebui să stabilească norme specifice privind condițiile pentru partajarea de informații în cadrul centrului cibernetic transfrontalier în cauză. Acordurile respective ar putea impune, în special, ca informațiile să fie partajate numai în conformitate cu dreptul Uniunii și cu dreptul intern.***

(28) În ceea ce privește implementarea rezervei UE pentru securitate cibernetică, sunt necesare norme specifice de confidențialitate. Sprijinul va fi solicitat, evaluat și acordat într-un context de criză și în ceea ce privește entitățile care își desfășoară activitatea în sectoare sensibile. Pentru ca rezerva UE pentru securitate cibernetică să funcționeze în mod eficace, este esențial ca utilizatorii și entitățile să poată partaja și oferi acces fără întârziere la toate informațiile necesare pentru ca fiecare entitate să își îndeplinească rolul în evaluarea cererilor și în implementarea sprijinului. În consecință, prezentul regulament ar trebui să prevadă că toate aceste informații trebuie să fie utilizate sau partajate numai dacă este necesar pentru funcționarea rezervei UE pentru securitate cibernetică și că informațiile care sunt confidențiale sau clasificate în temeiul dreptului Uniunii și al dreptului intern trebuie să fie utilizate și partajate numai în conformitate cu dreptul respectiv. În plus, utilizatorii ar trebui să fie în măsură, după caz, să utilizeze protocoale de partajare de informații, cum ar fi TLP, pentru a specifica în detaliu limitările ce se impun. Deși utilizatorii dispun de o marjă de apreciere în această privință, este important ca, atunci când aplică astfel de limitări, aceștia să ia în considerare posibilele consecințe, în special în ceea ce privește evaluarea sau livrarea întârziată a serviciilor solicitate. Pentru a dispune de o rezervă UE pentru securitate cibernetică eficientă, este important ca autoritatea contractantă să clarifice consecințele respective pentru utilizator înainte de a depune o cerere. Garanțiile respective se limitează la solicitarea și furnizarea de servicii aferente rezervei UE pentru securitate cibernetică și nu afectează schimbul de informații în alte contexte, cum ar fi achizițiile legate de rezerva UE pentru securitate cibernetică.

▌

(29) Având în vedere riscurile tot mai mari și numărul tot mai mare de incidente care afectează statele membre, este necesar să se instituie un instrument de sprijin în caz de criză, și ***anume mecanismul pentru situații de urgență în materie de securitate cibernetică,*** pentru a îmbunătăți reziliența Uniunii la incidentele de securitate cibernetică semnificative, incidentele de securitate cibernetică de mare amploare ***și*** incidentele de securitate cibernetică ***echivalente cu cele de mare amploare*** și pentru a completa acțiunile statelor membre prin sprijin financiar de urgență pentru pregătire, răspunsul la incidente și redresarea ***inițială*** în ceea ce privește serviciile esențiale. ***Întrucât redresarea completă în urma unui incident este un proces complex de restabilire a funcționării entității afectate de incident la stadiul anterior incidentului și ar putea fi un proces îndelungat cu costuri importante, sprijinul din rezerva UE pentru securitate cibernetică ar trebui să se limiteze la etapa inițială a procesului de redresare, care conduce la restabilirea funcționalităților de bază ale sistemelor.*** Mecanismul pentru situații de urgență ***în materie de securitate cibernetică*** ar trebui să permită mobilizarea rapidă ***și eficientă*** a asistenței în circumstanțe definite și în condiții clare, precum și o monitorizare și o evaluare atente ale modului în care au fost utilizate resursele. Deși responsabilitatea principală pentru prevenirea incidentelor și a crizelor, pregătirea pentru acestea și răspunsul la acestea le revine statelor membre, mecanismul pentru situații de urgență ***în materie de securitate cibernetică*** promovează solidaritatea între statele membre în conformitate cu articolul 3 alineatul (3) din Tratatul privind Uniunea Europeană (TUE).

(30) Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să ofere sprijin statelor membre în completarea propriilor măsuri și resurse, precum și a altor opțiuni de sprijin existente în cazul răspunsului la incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare și al redresării ***inițiale*** în urma acestora, cum ar fi serviciile furnizate de ENISA în conformitate cu mandatul său, răspunsul coordonat și asistența din partea rețelei CSIRT, sprijinul pentru atenuare din partea EU-CyCLONe, precum și asistența reciprocă între statele membre, inclusiv, în contextul articolului 42 alineatul (7) din TUE, echipele de răspuns rapid în domeniul cibernetic din cadrul cooperării structurate permanente (PESCO)instituite în temeiul Deciziei (PESC) 2017/2315 a Consiliului[15] ▌. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea unor astfel de incidente în întreaga Uniune și în țările terțe ***asociate la DEP, răspunsul la astfel de incidente și redresarea în urma acestora***.

[15] Decizia (PESC) 2017/2315 a Consiliului din 11 decembrie 2017 de stabilire a cooperării structurate permanente (PESCO) și de adoptare a listei statelor membre participante (JO L 331, 14.12.2017, p. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Prezentul regulament nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special Directivei (UE) 2022/2555, ***mecanismului de protecție civilă al Uniunii instituit prin Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului[16], mecanismului IPCR și Recomandării (UE) 2017/1584 a Comisiei[17]. Sprijinul acordat prin mecanismul pentru situații de urgență în materie de securitate cibernetică poate completa asistența acordată în contextul politicii externe și de securitate comune și al politicii de securitate și apărare comune, inclusiv prin intermediul echipelor de răspuns rapid în domeniul cibernetic, respectând natura civilă a mecanismului pentru situații de urgență în materie de securitate cibernetică. Sprijinul acordat prin mecanismul pentru situații de urgență în materie de securitate cibernetică*** poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE, ***inclusiv asistența acordată de un stat membru unui alt stat membru, sau poate face parte din răspunsul comun al Uniunii și al statelor membre sau în situațiile menționate*** la articolul 222 din TFUE. ***Punerea în aplicare a prezentului regulament*** ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, după caz.

---

16 ***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).***

17 ***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).***

(32) Asistența acordată în temeiul prezentului regulament ar trebui să sprijine și să completeze acțiunile întreprinse de statele membre la nivel național. În acest scop, ar trebui să se asigure o cooperare și o consultare strânse între Comisie, ***ENISA, statele membre și, dacă este cazul, ECCC***. Atunci când solicită sprijin în cadrul mecanismului pentru situații de urgență ***în materie de securitate cibernetică***, statele membre ar trebui să furnizeze informații relevante care să justifice necesitatea sprijinului.

(33) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să instituie una sau mai multe autorități de gestionare a crizelor cibernetice și să se asigure că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace și eficient. De asemenea, aceasta impune statelor membre să identifice capacitățile, activele și procedurile care pot fi utilizate în cazul unei crize, precum și să adopte un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Statele membre au, de asemenea, obligația de a institui una sau mai multe echipe CSIRT însărcinate cu responsabilități de administrare a incidentelor în conformitate cu un proces bine definit și care să acopere cel puțin sectoarele, subsectoarele și tipurile de entități care intră în domeniul de aplicare al directivei respective, precum și de a se asigura că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace. Prezentul regulament nu aduce atingere rolului Comisiei în asigurarea respectării de către statele membre a obligațiilor prevăzute în Directiva (UE) 2022/2555. Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să ofere asistență pentru acțiunile menite să consolideze pregătirea, precum și pentru acțiunile de răspuns la incidente pentru a atenua impactul incidentelor de securitate cibernetică semnificative și al incidentelor de securitate cibernetică de mare amploare, pentru a sprijini redresarea ***inițială sau pentru a restabili funcțiile de bază ale serviciilor asigurate de entități*** care își desfășoară activitatea în ***sectoare cu o importanță critică ridicată sau de entități*** care își desfășoară activitatea în ***alte sectoare de importanță critică***.

(34) În cadrul acțiunilor de pregătire, pentru a promova o abordare coerentă și a consolida securitatea în întreaga Uniune și pe piața sa internă, ar trebui să se acorde sprijin pentru testarea și evaluarea în mod coordonat a securității cibernetice a entităților care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată*** identificate în temeiul Directivei (UE) 2022/2555***, inclusiv prin exerciții și formare***. În acest scop, Comisia, ***după consultarea*** ENISA***, a Grupului*** de cooperare NIS ***și a EU-CyCLONe***, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată a pregătirii la nivelul Uniunii. Sectoarele sau subsectoarele ar trebui să fie selectate dintre sectoarele cu o importanță critică ridicată prevăzute în anexa I la Directiva (UE) 2022/2555. Testarea coordonată a pregătirii ar trebui să se bazeze pe scenarii și metodologii de risc comune. Selectarea sectoarelor și elaborarea scenariilor de risc ar trebui să țină seama de evaluările riscurilor și de scenariile de risc relevante la nivelul Uniunii, inclusiv de necesitatea de a evita suprapunerile, cum ar fi evaluarea riscurilor și scenariile de risc solicitate în Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene ▌ efectuate de Comisie, de Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (denumit în continuare „Înaltul Reprezentant”) și de Grupul de cooperare NIS, în coordonare cu organismele și agențiile civile și militare relevante și cu rețelele instituite, inclusiv EU-CyCLONe, precum și de evaluarea riscurilor pentru rețelele și infrastructurile de comunicații, solicitată prin Apelul ministerial comun de la Nevers și realizată de Grupul de cooperare NIS, cu sprijinul Comisiei și al ENISA și în cooperare cu Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice instituit prin Regulamentul (UE) 2018/1971 al Parlamentului European și al Consiliului[18], de evaluările coordonate la nivelul Uniunii ale riscurilor de securitate în ceea ce privește lanțurile de aprovizionare critice, care urmează să fie efectuate în temeiul articolului 22 din Directiva (UE) 2022/2555 și de testarea rezilienței operaționale digitale, astfel cum se prevede în Regulamentul (UE)

18 Regulamentul (UE) 2018/1971 al Parlamentului European și al Consiliului din 11 decembrie 2018 de instituire a Organismului Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC) și a Agenției de sprijin pentru OAREC (Oficiul OAREC) și de modificare a Regulamentului (UE) 2015/2120 și de abrogare a Regulamentului (CE) nr. 1211/2009 (JO L 321, 17.12.2018, p. 1).

2022/2554 al Parlamentului European și al Consiliului[19]. Selectarea sectoarelor ar trebui, de asemenea, să țină seama de Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice.

[19] 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).

(35) În plus, mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să asigure sprijin pentru alte acțiuni de pregătire și să sprijine pregătirea în alte sectoare, care nu sunt acoperite de testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată sau a*** entităților care își desfășoară activitatea în sectoare ***în alte sectoare*** de importanță critică. Aceste acțiuni ar putea include diferite tipuri de activități de pregătire la nivel național.

(36) Atunci când statele membre primesc granturi pentru a sprijini acțiunile de pregătire, entitățile din sectoare cu o importanță critică ridicată pot participa la acțiunile respective în mod voluntar. Este o bună practică ca, în urma unor astfel de acțiuni, entitățile participante să elaboreze un plan de remediere pentru a pune în aplicare orice recomandări rezultate privind măsuri specifice, astfel încât să beneficieze pe deplin de pe urma acțiunii de pregătire. Deși este important ca statele membre să solicite, în cadrul acțiunilor, ca entitățile participante să elaboreze și să pună în aplicare astfel de planuri de remediere, statele membre nu sunt nici obligate, nici împuternicite prin prezentul regulament să asigure respectarea unor astfel de solicitări. Astfel de solicitări nu aduc atingere cerințelor impuse entităților și competențelor de supraveghere ale autorităților competente, în conformitate cu Directiva (UE) 2022/2555.

(37) Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui, de asemenea, să ofere sprijin pentru acțiunile de răspuns la incidente menite să atenueze impactul incidentelor de securitate cibernetică semnificative, al incidentelor de securitate cibernetică de mare amploare și al incidentelor de securitate cibernetică echivalente cu cele de mare amploare, să sprijine redresarea ***inițială*** sau să restabilească funcționarea serviciilor esențiale. După caz, acesta ar trebui să completeze UCPM pentru a asigura o abordare cuprinzătoare pentru a răspunde impactului incidentelor asupra cetățenilor.

(38) Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să sprijine asistența ***tehnică*** acordată de ***un stat membru altui stat membru*** care este afectat de un incident de securitate cibernetică semnificativ sau de un incident de securitate cibernetică de mare amploare, ***inclusiv de echipele CSIRT, astfel cum se menționează la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555***. Statele membre care acordă ***astfel de*** asistență ar trebui să aibă posibilitatea de a depune cereri pentru a acoperi costurile legate de trimiterea echipelor de experți în cadrul asistenței reciproce. Costurile eligibile ar putea include cheltuielile de deplasare, cazare și diurnă ale experților în securitate cibernetică.

(39) ***Având în vedere rolul esențial pe care îl joacă întreprinderile private în detectarea incidentelor de securitate cibernetică de mare amploare*** și a ***incidentelor de securitate cibernetică echivalente cu cele de mare amploare, în pregătirea legată de acestea și în răspunsul la acestea, este important să se recunoască valoarea cooperării voluntare pro bono cu astfel de întreprinderi, prin care acestea oferă servicii fără remunerație în cazul incidentelor și crizelor de securitate cibernetică de mare amploare și al incidentelor și crizelor de securitate cibernetică echivalente cu cele de mare amploare. ENISA, în cooperare cu EU-CyCLONe, ar putea monitoriza evoluția unor astfel de inițiative pro bono și ar putea promova conformitatea acestora cu criteriile aplicabile furnizorilor de încredere de servicii de securitate gestionate în temeiul prezentului regulament, inclusiv în ceea ce privește fiabilitatea întreprinderilor private, experiența acestora, precum și capacitatea de a gestiona informațiile sensibile în mod securizat.***

(40) Ca parte a mecanismului pentru situații de urgență în materie de securitate cibernetică, ar trebui instituită treptat o rezervă UE pentru securitate cibernetică care să constea în servicii furnizate 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***. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor. ***Prin urmare, aceasta ar trebui să includă servicii care sunt angajate în prealabil, inclusiv, de exemplu, capacități care se află în așteptare și care pot fi desfășurate rapid.*** Serviciile din rezerva UE pentru securitate cibernetică ar trebui să servească la sprijinirea autorităților naționale în ceea ce privește furnizarea de asistență entităților afectate care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată sau*** entităților afectate care își desfășoară activitatea ***în alte sectoare de importanță critică***, în completarea propriilor acțiuni la nivel național. ***Serviciile din rezerva UE pentru securitate cibernetică ar trebui să aibă capacitatea de a servi, de asemenea, la sprijinirea instituțiilor, a organelor, a oficiilor și a agențiilor Uniunii, în condiții similare. Rezerva UE pentru securitate cibernetică ar putea contribui și la consolidarea poziției concurențiale a industriei și a serviciilor din Uniune în întreaga economie digitală, inclusiv a microîntreprinderilor și a întreprinderilor mici și mijlocii, precum și a întreprinderilor nou-înființate, inclusiv prin furnizarea de stimulente pentru investiții în cercetare și inovare. Este important să se țină seama de Cadrul european de competențe în materie de securitate cibernetică al ENISA atunci când se achiziționează serviciile pentru rezerva UE pentru securitate cibernetică.*** Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, ***utilizatorii ar trebui să includă în cererea lor informații adecvate cu privire la entitatea afectată și la impactul potențial, informații privind serviciul solicitat din rezerva UE pentru securitate cibernetică*** și sprijinul acordat entității afectate la nivel național, care ar trebui să fie luat în considerare atunci când se evaluează cererea ***din partea solicitantului***. ***Pentru a asigura complementaritatea cu alte forme de sprijin***

disponibile pentru entitatea afectată, cererea ar trebui să includă, dacă sunt disponibile, și informații privind acorduri contractuale aflate în vigoare pentru răspunsul la incidente și servicii de redresare inițială, precum și contracte de asigurare care ar putea acoperi un astfel de tip de incident.

(41) Pentru a asigura folosirea eficace a fondurilor din partea Uniunii din cadrul rezervei UE pentru securitate cibernetică, serviciile angajate în prealabil ar trebui să poată fi transformate, în conformitate cu contractul relevant, în servicii de pregătire legate de prevenirea incidentelor și de răspunsul la acestea, în cazul în care respectivele servicii angajate în prealabil nu sunt folosite pentru răspunsul la incidente în perioada în care sunt angajate în prealabil. Serviciile respective ar trebui să fie complementare acțiunilor de pregătire care urmează să fie gestionate de ECCC și să nu se suprapună cu acestea.

(42) Cererile de sprijin din rezerva UE pentru securitate cibernetică din partea autorităților statelor membre de gestionare a crizelor cibernetice și a echipelor CSIRT sau CERT-UE, în numele instituțiilor, organelor, oficiilor și agențiilor Uniunii, ar trebui să fie evaluate de autoritatea contractantă. În cazurile în care administrarea și operarea rezervei UE pentru securitate cibernetică au fost încredințate către ENISA, autoritatea contractantă este ENISA. Cererile de sprijin din partea țărilor terțe asociate la DEP ar trebui să fie evaluate de Comisie. Pentru a facilita transmiterea și evaluarea cererilor de sprijin, ENISA ar putea crea o platformă securizată.

(43) Atunci când se primesc concomitent mai multe cereri, ordinea de prioritate a cererilor respective ar trebui să fie stabilită în conformitate cu criteriile prevăzute în prezentul regulament. Având în vedere obiectivele generale ale prezentului regulament, criteriile respective ar trebui să includă amploarea și gravitatea incidentului, tipul entității afectate, impactul potențial al incidentului asupra statelor membre afectate și asupra utilizatorilor afectați, natura transfrontalieră potențială a incidentului și riscul de propagare, precum și măsurile luate deja de utilizator pentru a sprijini răspunsul și redresarea inițială. Având în vedere aceste obiective și având în vedere că cererile din partea utilizatorilor din statele membre sunt destinate exclusiv sprijinirii, în întreaga Uniune, a entităților care își desfășoară activitatea în sectoare cu o importanță critică ridicată sau a entităților care își desfășoară activitatea în alte sectoare de importanță critică, este oportun să se acorde o prioritate mai mare cererilor utilizatorilor din statele membre atunci când criteriile respective conduc la evaluarea a două sau mai multe cereri ca fiind de același rang. Acest lucru nu aduce atingere niciunei obligații pe care statele membre ar putea să o aibă, în temeiul acordurilor de găzduire relevante, de a lua măsuri pentru a proteja instituțiile, organele, oficiile și agențiile Uniunii și a le acorda asistență.

(44) Comisia ar trebui să aibă responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Având în vedere experiența vastă dobândită de ENISA în ceea ce privește acțiunea de sprijin în materie de securitate cibernetică, ENISA este agenția cea mai adecvată pentru a implementa rezerva UE pentru securitate cibernetică. Prin urmare, Comisia ar trebui să încredințeze ENISA, parțial sau, în cazul în care Comisia consideră că este oportun, în întregime, operarea și administrarea rezervei UE pentru securitate cibernetică. Încredințarea ar trebui să aibă loc în conformitate cu normele aplicabile în temeiul Regulamentului (UE, Euratom) 2024/2509 și, în special, ar trebui să fie condiționată de îndeplinirea condițiilor relevante pentru semnarea unui acord de contribuție. Orice aspecte legate de operarea și administrarea rezervei UE pentru securitate cibernetică care nu au fost încredințate ENISA ar trebui să facă obiectul gestionării directe de către Comisie, inclusiv înainte de semnarea acordului de contribuție.

(45) Statele membre ar trebui să aibă un rol esențial în constituirea, implementarea și etapa de după implementare a rezervei UE pentru securitate cibernetică. Întrucât Regulamentul (UE) 2021/694 este actul de bază relevant pentru acțiunile de implementare a rezervei UE pentru securitate cibernetică, acțiunile din cadrul rezervei UE pentru securitate cibernetică ar trebui să fie prevăzute în programele de lucru menționate la articolul 24 din Regulamentul (UE) 2021/694. În temeiul alineatului (6) de la articolul menționat, programele de lucru respective ar trebui să fie adoptate de Comisie prin intermediul unor acte de punere în aplicare, în conformitate cu procedura de examinare. În plus, Comisia, în coordonare cu Grupul de cooperare NIS, ar trebui să stabilească prioritățile și evoluția rezervei UE pentru securitate cibernetică.

(46) Contractele încheiate în contextul rezervei UE pentru securitate cibernetică nu ar trebui să afecteze relația dintre întreprinderi și obligațiile existente între entitatea afectată sau utilizatori și furnizorul de servicii.

(47) În scopul selectării furnizorilor privați de servicii care să furnizeze servicii în contextul rezervei UE pentru securitate cibernetică, este necesar să se stabilească un set de criterii minime și cerințe care ar trebui incluse în cererea de oferte pentru selectarea furnizorilor respectivi, astfel încât să se asigure că sunt îndeplinite nevoile autorităților statelor membre, ale entităților care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată și ale entităților care își desfășoară activitatea în alte sectoare*** de importanță critică. ***Pentru a răspunde nevoilor specifice ale statelor membre, atunci când achiziționează servicii pentru rezerva UE pentru securitate cibernetică, autoritatea contractantă ar trebui, după caz, să formuleze criterii de selecție și cerințe suplimentare față de cele prevăzute în prezentul regulament. Este important să se încurajeze participarea furnizorilor mai mici, activi la nivel regional și local.***

(48) Atunci când selectează furnizorii pentru a fi incluși în rezerva UE pentru securitate cibernetică, autoritatea contractantă ar trebui să urmărească să se asigure că rezerva UE pentru securitate cibernetică, privită în ansamblu, conține furnizori care pot răspunde cerințelor lingvistice ale utilizatorilor. În acest scop, înainte de a pregăti caietul de sarcini, autoritatea contractantă ar trebui să verifice dacă potențialii utilizatori ai rezervei UE pentru securitate cibernetică au cerințe lingvistice specifice, astfel încât serviciile de asistență oferite în cadrul rezervei UE pentru securitate cibernetică să poată fi furnizate într-una din limbile oficiale ale instituțiilor Uniunii sau ale statelor membre, care să poată fi înțeleasă de utilizator sau de entitatea afectată. În cazul în care un utilizator solicită mai multe limbi pentru furnizarea de servicii de asistență oferite în cadrul rezervei UE pentru securitate cibernetică, iar serviciile respective au fost achiziționate în limbile respective pentru utilizatorul respectiv, utilizatorul ar trebui să poată preciza în cererea de sprijin din rezerva UE pentru securitate cibernetică în care dintre aceste limbi ar trebui să fie furnizate serviciile în legătură cu incidentul specific care a generat cererea.

(49) Pentru a sprijini instituirea rezervei UE pentru securitate cibernetică, ***este important ca*** Comisia ***să solicite*** ENISA să pregătească o propunere de sistem de certificare ***în materie de securitate cibernetică*** pentru serviciile de securitate gestionate în temeiul Regulamentului (UE) 2019/881 în domeniile acoperite de mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică.

(50) Pentru a sprijini obiectivele prezentului regulament de promovare a conștientizării comune a situației, de consolidare a rezilienței Uniunii și de facilitare a unui răspuns eficace la incidentele de securitate cibernetică semnificative și la incidentele de securitate cibernetică de mare amploare, ***Comisia sau*** EU-CyCLONe ar trebui să poată solicita ENISA, ***cu sprijinul rețelei CSIRT și cu aprobarea statelor membre în cauză,*** să revizuiască și să evalueze amenințările cibernetice, vulnerabilitățile ***exploatabile cunoscute*** și acțiunile de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau un anumit incident de securitate cibernetică de mare amploare. În urma finalizării unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de analiză a incidentelor, în colaborare cu ***statul membru în cauză și cu*** părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ▌ai Comisiei și ai altor instituții, organe, ***oficii*** și agenții relevante ale Uniunii. Pe baza colaborării cu părțile interesate, inclusiv din sectorul privat, raportul de analiză privind incidentele specifice ar trebui să vizeze evaluarea cauzelor, a impactului și a atenuării unui incident, după producerea acestuia. Ar trebui să se acorde o atenție deosebită contribuțiilor și învățămintelor împărtășite de furnizorii de servicii de securitate gestionate care îndeplinesc condițiile de maximă integritate profesională, imparțialitate și cunoștințe tehnice necesare, astfel cum se prevede în prezentul regulament. Raportul ar trebui să fie prezentat ▌EU-CyCLONe, ***rețelei*** CSIRT și Comisiei și ***ar trebui să fie utilizat pentru a contribui*** la activitatea acestora***, precum și la activitatea ENISA***. În cazul în care incidentul se referă la o țară terță ***asociată la DEP***, Comisia ***ar trebui să transmită raportul și*** Înaltului Reprezentant.

(51) Având în vedere caracterul imprevizibil al atacurilor cibernetice și faptul că, adesea, acestea nu sunt limitate la o anumită zonă geografică și prezintă un risc ridicat de propagare, consolidarea rezilienței țărilor învecinate și a capacității lor de a răspunde în mod eficace la incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică echivalente cu cele de mare amploare contribuie la protecția Uniunii în ansamblu***, în special a pieței sale interne și a industriei sale***. ***Astfel de activități ar putea, în plus, contribui la diplomația cibernetică a Uniunii.*** Prin urmare, țările terțe asociate la DEP ar trebui să aibă posibilitatea de a solicita sprijin din rezerva UE pentru securitate cibernetică***, pe întreg teritoriul lor sau pe o parte a acestuia***, în cazul în care acest lucru este prevăzut în acordul ***prin care țara terță este asociată*** la DEP. Finanțarea pentru țările terțe asociate ***la DEP*** ar trebui să fie sprijinită de Uniune în cadrul parteneriatelor și al instrumentelor de finanțare relevante pentru țările respective. Sprijinul ar trebui să acopere serviciile din domeniul răspunsului la incidentele de securitate cibernetică semnificative sau incidentele de securitate cibernetică echivalente cu cele de mare amploare și al redresării ***inițiale*** în urma acestora.

(52) Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere de servicii de securitate gestionate în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP. Țările terțe asociate la DEP ar trebui să poată solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care entitățile vizate și pentru care solicită sprijin din rezerva UE pentru securitate cibernetică sunt entități care își desfășoară activitatea în sectoare cu o importanță critică ridicată sau entități care își desfășoară activitatea în alte sectoare de importanță critică și în cazul în care incidentele detectate conduc la perturbări operaționale semnificative sau ar putea avea efecte de propagare în Uniune. Țările terțe asociate la DEP ar trebui să fie eligibile pentru a primi sprijin numai dacă acordul prin care sunt asociate la DEP prevede în mod specific un astfel de sprijin. În plus, aceste țări terțe ar trebui să rămână eligibile numai atât timp cât sunt îndeplinite trei criterii. În primul rând, țara terță ar trebui să respecte pe deplin clauzele relevante din acordul respectiv. În al doilea rând, având în vedere caracterul complementar al rezervei UE pentru securitate cibernetică, țara terță ar trebui să fi luat măsuri adecvate pentru a se pregăti pentru incidente de securitate cibernetică semnificative sau incidente de securitate cibernetică echivalente cu cele de mare amploare. În al treilea rând, acordarea de sprijin din rezerva UE pentru securitate cibernetică ar trebui să fie în concordanță cu politica Uniunii față de țara respectivă și cu relațiile generale cu aceasta și cu alte politici ale Uniunii în domeniul securității. În contextul evaluării sale privind respectarea acestui al treilea criteriu, Comisia ar trebui să consulte Înaltul Reprezentant în vederea alinierii acordării unui astfel de sprijin la politica externă și de securitate comună.

(53) ***Acordarea de sprijin țărilor terțe asociate la DEP poate afecta relațiile cu țările terțe și politica de securitate a Uniunii, inclusiv în contextul politicii externe și de securitate comune și al politicii de securitate și apărare comune. În consecință, este oportun să se acorde Consiliului competențe de executare pentru a autoriza și a preciza perioada în care poate fi acordat un astfel de sprijin. Consiliul ar trebui să acționeze pe baza unei propuneri a Comisiei, ținând seama în mod corespunzător de evaluarea Comisiei în legătură cu cele trei criterii. Acest lucru ar trebui să fie valabil și în cazul reînnoirilor și al propunerilor de modificare sau de abrogare a unor astfel de acte. Atunci când, în circumstanțe excepționale, consideră că a avut loc o modificare semnificativă a circumstanțelor în ceea ce privește al treilea criteriu, Consiliul ar trebui să poată acționa din proprie inițiativă pentru a modifica sau a abroga un act de punere în aplicare, fără a aștepta o propunere a Comisiei. Este probabil ca astfel de schimbări semnificative să necesite acțiuni urgente, să aibă implicații deosebit de importante pentru relațiile cu țările terțe și să nu necesite o evaluare detaliată prealabilă din partea Comisiei. În plus, Comisia ar trebui să coopereze cu Înaltul Reprezentant în ceea ce privește cererile de sprijin din partea țărilor terțe asociate la DEP și punerea în aplicare a sprijinului acordat unor astfel de țări terțe. Comisia ar trebui, de asemenea, să țină seama de orice opinie exprimată de ENISA în legătură cu astfel de cereri și sprijin. Comisia ar trebui să informeze Consiliul cu privire la rezultatul evaluării cererilor, inclusiv cu privire la orice observații relevante formulate în această privință, și cu privire la serviciile care sunt implementate.***

(54) Comunicarea Comisiei din 18 aprilie 2023 privind Academia de competențe în domeniul cibernetic a recunoscut deficitul de profesioniști calificați. Este nevoie de astfel de competențe pentru realizarea obiectivelor prezentului regulament. Uniunea are urgent nevoie de profesioniști cu aptitudini și competențe pentru a preveni, a detecta și a descuraja atacurile cibernetice și pentru a apăra Uniunea, inclusiv infrastructurile sale cele mai critice, împotriva unor astfel de atacuri, și pentru a-i asigura reziliența. În acest scop, este important să se încurajeze cooperarea între părțile interesate, inclusiv din sectorul privat, din mediul academic și din sectorul public. Este la fel de important să se creeze sinergii, în toate teritoriile Uniunii, pentru investițiile în educație și formare pentru a promova crearea de garanții în vederea evitării exodului creierelor sau a accentuării lacunelor în materie de competențe într-o mai mare măsură în unele regiuni decât în altele. Trebuie să se elimine urgent lacunele în materie de competențe în domeniul securității cibernetice, cu un accent deosebit pe reducerea disparității de gen în cadrul forței de muncă din acest sector, pentru a promova prezența și participarea femeilor la conceperea guvernanței digitale.

(55) Pentru a stimula inovarea pe piața unică digitală, este important să se consolideze cercetarea și inovarea în domeniul securității cibernetice, în scopul de a contribui la creșterea rezilienței statelor membre și a autonomiei strategice deschise a Uniunii, ambele fiind obiective ale prezentului regulament. Sinergiile sunt esențiale pentru a consolida cooperarea și coordonarea între diferitele părți interesate, inclusiv din sectorul privat, societatea civilă și mediul academic.

(56) Prezentul regulament ar trebui să țină seama de angajamentul asumat în Declarația comună a Parlamentului European, a Consiliului și a Comisiei din 26 ianuarie 2022 intitulată „Declarația europeană privind drepturile și principiile digitale pentru deceniul digital", de a proteja interesele democrațiilor, cetățenilor, întreprinderilor și instituțiilor publice ale Uniunii împotriva riscurilor de securitate cibernetică și a criminalității informatice, inclusiv împotriva încălcării securității datelor și a furtului sau manipulării identității.

(57) ***În vederea completării anumitor elemente neesențiale ale prezentului regulament, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui delegată Comisiei în ceea ce privește precizarea tipurilor și numărului de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[20]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.***

(58) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei pentru a ***preciza modalitățile procedurale detaliate de alocare a serviciilor de sprijin din rezerva UE pentru securitate cibernetică***. ***Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[21].***

---

20 *JO L 123, 12.5.2016, p. 1,*
ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

21 ***Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(59) Fără a aduce atingere normelor referitoare la bugetul anual al Uniunii în temeiul tratatelor, Comisia ar trebui să țină seama de obligațiile care decurg din prezentul regulament atunci când evaluează nevoile în materie de buget și de personal ale ENISA.

(60) Comisia ar trebui să efectueze periodic o evaluare a măsurilor prevăzute în prezentul regulament. Prima astfel de evaluare ar trebui să aibă loc în primii doi ani de la data intrării în vigoare a prezentului regulament și, ulterior, evaluările ar trebui să se efectueze cel puțin o dată la patru ani, ținând seama de calendarul revizuirii cadrului financiar multianual instituit în temeiul articolului 312 din TFUE. Comisia ar trebui să prezinte Parlamentului European și Consiliului un raport privind progresele înregistrate. Pentru a evalua diferitele elemente necesare, inclusiv amploarea informațiilor partajate în cadrul sistemului european de alertă în materie de securitate cibernetică, Comisia ar trebui să se bazeze exclusiv pe informații care sunt ușor accesibile sau furnizate în mod voluntar. Având în vedere evoluțiile geopolitice și pentru a asigura continuitatea și dezvoltarea în continuare a măsurilor prevăzute în prezentul regulament după 2027, este important ca Comisia să evalueze necesitatea de a aloca un buget adecvat în cadrul financiar multianual pentru perioada 2028-2034.

(61) ***Întrucât obiectivele prezentului regulament, și anume consolidarea poziției competitive a industriei și a serviciilor din Uniune în cadrul economiei digitale și contribuirea la suveranitatea tehnologică a Uniunii și la autonomia strategică deschisă în domeniul securității cibernetice, nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere amploarea sau efectele acțiunii, acestea pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivelor respective.***

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I

DISPOZIȚII GENERALE

Articolul 1

Obiect și obiective

(1) Prezentul regulament stabilește măsuri de consolidare a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea, în special prin instituirea:

(a) ***unei rețele*** paneuropene de centre ***cibernetice (denumită în continuare „sistemul european de alertă în materie de securitate cibernetică”),*** pentru a construi și a consolida capacitățile ***coordonate*** de detectare și ***capacitățile comune*** de conștientizare a situației;

(b) unui mecanism pentru situații de urgență în materie de securitate cibernetică, pentru a sprijini statele membre să se pregătească pentru incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare, să răspundă la acestea***, să le atenueze impactul*** și să ***inițieze redresarea*** în urma lor, ***precum și pentru a sprijini alți utilizatori să răspundă la*** incidentele de securitate cibernetică semnificative și la incidentele de securitate cibernetică ***echivalente cu*** cele de mare amploare;

(c) unui mecanism european de analiză a incidentelor de securitate cibernetică pentru a analiza și a evalua incidentele de securitate cibernetică semnificative sau incidentele de securitate cibernetică de mare amploare.

(2) Prezentul regulament urmărește ***obiectivele generale*** de consolidare ***a poziției concurențiale a industriei și a serviciilor din Uniune în întreaga economie digitală, inclusiv a microîntreprinderilor și a întreprinderilor mici și mijlocii, precum și a întreprinderilor nou-înființate, și de a contribui la suveranitatea tehnologică a Uniunii și la autonomia strategică deschisă în domeniul securității cibernetice, inclusiv prin stimularea inovării pe piața unică digitală. Acesta urmărește obiectivele respective prin consolidarea*** solidarității la nivelul Uniunii***, întărirea ecosistemului de securitate cibernetică, sporirea rezilienței cibernetice a statelor membre și dezvoltarea aptitudinilor, a know-how-ului, a abilităților și a competențelor forței de muncă în ceea ce privește securitatea cibernetică***.

(3) Îndeplinirea obiectivelor generale menționate la alineatul (2) este urmărită prin intermediul următoarelor obiective specifice:

(a) de a consolida ***capacitățile comune coordonate de detectare*** și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările cibernetice și incidente ;

(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată sau al entităților care își desfășoară activitatea în alte sectoare*** de importanță critică din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități ***de testare coordonată a pregătirii și*** de răspuns ***și redresare consolidate pentru a gestiona incidente*** de securitate cibernetică semnificative***, incidente de securitate cibernetică de mare amploare*** sau ***incidente de securitate cibernetică echivalente cu cele*** de mare amploare, inclusiv ***posibilitatea punerii*** la dispoziția țărilor terțe asociate la ***programul „Europa digitală” (DEP)*** a sprijinului din partea Uniunii pentru răspunsul la incidentele de securitate cibernetică;

(c) de a spori reziliența Uniunii și de a contribui la un răspuns eficace la incidente prin analizarea și evaluarea incidentelor de securitate cibernetică semnificative sau a incidentelor de securitate cibernetică de mare amploare, inclusiv prin valorificarea lecțiilor învățate și, după caz, prin recomandări.

(4) ***Acțiunile întreprinse în temeiul prezentului regulament se desfășoară cu respectarea adecvată a competențelor statelor membre și sunt complementare activităților desfășurate de rețeaua CSIRT, de EU-CyCLONe și de Grupul de cooperare NIS.***

(5) Prezentul regulament nu aduce atingere ***funcțiilor esențiale ale statelor membre, incluzând asigurarea integrității teritoriale a statului, menținerea ordinii publice și apărarea securității naționale***. ***În special, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru.***

(6) ***Partajarea sau schimbul, în temeiul prezentului regulament, de informații care sunt confidențiale în temeiul normelor Uniunii sau al normelor naționale se limitează la ceea ce este relevant și proporțional cu scopul partajării sau schimbului. Respectiva partajare sau respectivul schimb de informații păstrează confidențialitatea informațiilor și protejează securitatea și interesele comerciale ale entităților în cauză. Partajarea sau schimbul nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.***

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

▌

1. ***„centru cibernetic transfrontalier”*** înseamnă o platformă multinațională ***instituită printr-un acord de consorțiu scris*** care reunește într-o structură coordonată de rețea ***centre 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;

▌

2. „consorțiu-gazdă” înseamnă un consorțiu alcătuit din state ***membre*** participante, ▌ care au convenit să înființeze și să contribuie la achiziționarea de instrumente***,*** ***infrastructuri sau servicii*** pentru un ***centru cibernetic*** transfrontalier și la asigurarea funcționării acestuia;

3. „echipă CSIRT” înseamnă o echipă CSIRT desemnată sau instituită în temeiul articolului 10 din Directiva (UE) 2022/2555;

4. „entitate” înseamnă o entitate în sensul definiției de la articolul 6 punctul 38 din Directiva (UE) 2022/2555;

5. „entități care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată***” înseamnă tipurile de entități enumerate în anexa I la Directiva (UE) 2022/2555;

6. „entități care își desfășoară activitatea în alte sectoare de importanță critică” înseamnă tipurile de entități enumerate în anexa II la Directiva (UE) 2022/2555;

7. „risc” înseamnă risc în sensul definiției de la articolul 6 punctul 9 din Directiva (UE) 2022/2555;

8. „amenințare cibernetică” înseamnă o amenințare cibernetică în sensul definiției de la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

▌

9. „incident” înseamnă un incident în sensul definiției de la articolul 6 punctul 6 din Directiva (UE) 2022/2555;

10. „incident de securitate cibernetică semnificativ” înseamnă un incident care îndeplinește criteriile prevăzute la articolul 23 alineatul (3) din Directiva (UE) 2022/2555;

11. „incident major” înseamnă un incident major în sensul definiției de la articolul 3 punctul 8 din Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului[22];

12. „incident de securitate cibernetică de mare amploare” înseamnă un incident de securitate cibernetică de mare amploare în sensul definiției de la articolul 6 punctul 7 din Directiva (UE) 2022/2555;

13. „incident de securitate cibernetică echivalent cu cele de mare amploare” înseamnă, în cazul instituțiilor, organelor, oficiilor și agențiilor Uniunii, un incident major și, în cazul țărilor terțe asociate la DEP, un incident care cauzează un nivel de perturbare care depășește capacitatea țării terțe asociate la DEP în cauză de a răspunde;

14. „țară terță asociată la DEP” înseamnă o țară terță care este parte la un acord cu Uniunea care permite participarea sa la programul „Europa digitală” în temeiul articolului 10 din Regulamentul (UE) 2021/694;

---

[22] ***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).***

15. „autoritate contractantă” înseamnă Comisia sau, în cazul în care operarea și administrarea rezervei UE pentru securitate cibernetică a fost încredințată ENISA în temeiul articolului 14 alineatul (5), ENISA;

▌

16. „furnizor de servicii de securitate gestionate” înseamnă un furnizor de servicii de securitate gestionate în sensul definiției de la articolul 6 punctul 40 din Directiva (UE) 2022/2555;

17. „furnizori de încredere ***de servicii de securitate gestionate***” înseamnă furnizori de servicii de securitate gestionate ▌ selectați ***pentru a fi incluși în rezerva UE pentru securitate cibernetică*** în conformitate cu articolul 17.

Capitolul II

SISTEMUL EUROPEAN ***DE ALERTĂ ÎN MATERIE DE SECURITATE CIBERNETICĂ***

Articolul 3

Instituirea ***sistemului*** european ***de alertă în materie de securitate cibernetică***

(1) ***Se instituie sistemul european de alertă în materie de securitate cibernetică,*** o ***rețea*** paneuropeană ***de infrastructură formată din centre cibernetice naționale și centre cibernetice transfrontaliere care aderă în mod voluntar, pentru a sprijini dezvoltarea de capacități avansate care să permită Uniunii să consolideze capacitățile de detectare, analiză și prelucrare a datelor în raport cu amenințările cibernetice și prevenirea incidentelor în Uniune***.

(2) ***Sistemul*** european ***de alertă în materie de securitate cibernetică***:

(a) contribuie la o mai bună protecție împotriva amenințărilor cibernetice și la un răspuns mai bun la acestea, sprijinind entitățile relevante, în special echipele CSIRT, rețeaua CSIRT, EU-CyCLONe și autoritățile competente desemnate sau instituite în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cooperând cu acestea și consolidându-le capacitățile;

(b) pune în comun ***date și informații relevante*** privind amenințările cibernetice și incidente din diferite surse ***în cadrul centrelor cibernetice transfrontaliere și partajează informații analizate sau agregate*** prin intermediul ***centrelor cibernetice transfrontaliere, după caz, cu rețeaua CSIRT***;

(c) ***colectează și sprijină producția*** de informații operative de înaltă calitate și de informații privind amenințările cibernetice, prin utilizarea unor instrumente de ultimă generație ***și a unor tehnologii avansate și partajează informațiile respective și informațiile privind amenințările cibernetice***;

▌

(d) contribuie la ***o mai bună detectare coordonată*** a amenințărilor cibernetice și la conștientizarea ***comună a*** situației în întreaga Uniune***, precum și la emiterea de semnalări, inclusiv, după caz, furnizând recomandări concrete entităților***;

(e) furnizează servicii și activități pentru comunitatea securității cibernetice din Uniune, contribuind inclusiv la dezvoltarea unor instrumente ***și tehnologii*** avansate***, cum ar fi instrumentele*** de inteligență artificială și de analiză a datelor.

▌

(3) Acțiunile de punere în aplicare a sistemului european de alertă în materie de securitate cibernetică sunt sprijinite prin finanțare din DEP și sunt puse în aplicare în conformitate cu Regulamentul (UE) 2021/694, în special cu obiectivul specific nr. 3 din regulamentul menționat.

Articolul 4

Centrele ***cibernetice*** naționale

(1) ***În cazul în care un stat membru decide să participe la sistemul*** european ***de alertă în materie de securitate cibernetică, acesta*** desemnează ***sau, după caz, instituie un centru cibernetic național în sensul prezentului regulament.***

(2) ***Un centru cibernetic național este o entitate unică care acționează sub autoritatea unui stat membru. Acesta poate fi o echipă CSIRT sau, după caz, o autoritate națională de gestionare a crizelor cibernetice sau o altă autoritate competentă desemnată sau instituită în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555 sau o altă entitate. Centrul cibernetic național:***

(a) ***are capacitatea de a acționa ca punct de referință și punct de acces către alte organizații publice și private de la nivel național pentru colectarea și analizarea informațiilor privind amenințările cibernetice și incidente și de a contribui la un centru cibernetic transfrontalier, astfel cum se menționează la articolul 5; și***

(b) ***este capabil să detecteze, să agrege și să analizeze date și informații relevante pentru amenințările cibernetice și incidente, cum ar fi informațiile privind amenințările cibernetice, utilizând în special tehnologii de ultimă generație, cu scopul de a preveni incidentele.***

I

(3) ***Ca parte a funcțiilor menționate la alineatul (2) din prezentul articol, centrele cibernetice naționale pot coopera cu entități din sectorul privat pentru a face schimb de date și informații relevante în scopul de a detecta și preveni amenințările cibernetice și incidentele, inclusiv cu comunități sectoriale și transsectoriale de entități esențiale și importante, astfel cum sunt menționate la articolul 3 din Directiva (UE) 2022/2555. După caz și în conformitate cu dreptul Uniunii și cu dreptul intern, informațiile solicitate sau primite de centrele cibernetice naționale pot include date obținute prin telemetrie, senzori sau jurnalizare.***

(4) Un ***stat membru*** selectat în temeiul ***articolului 9 alineatul (1)*** se angajează să solicite ***ca centrul său cibernetic*** național ***să participe la un centru cibernetic transfrontalier***.

Articolul 5

Centre ***cibernetice*** transfrontaliere

(1) ***În cazul în care*** cel puțin trei state membre ***se angajează să garanteze că centrele lor cibernetice naționale colaborează*** pentru a-și coordona activitățile de detectare cibernetică și de monitorizare a amenințărilor***, statele membre respective pot crea un consorțiu-gazdă în sensul prezentului regulament***.

(2) Un consorțiu-gazdă este alcătuit din cel puțin trei state participante care au convenit să înființeze un centru cibernetic transfrontalier și să contribuie la achiziționarea de instrumente, infrastructuri sau servicii pentru un astfel de centru, precum și la funcționarea sa, în conformitate cu alineatul (4).

(3) ***În cazul în care un consorțiu-gazdă este selectat în conformitate cu articolul 9 alineatul (3), membrii săi*** încheie un acord de consorțiu scris care***:***

(a) stabilește procedurile interne pentru punerea în aplicare a acordului de găzduire și de utilizare ***menționat la articolul 9 alineatul (3);***

(b) înființează centrul cibernetic transfrontalier al consorțiului-gazdă; și

(c) include clauzele specifice necesare în temeiul articolului 6 alineatele (1) și (2).

(4) Un centru cibernetic transfrontalier este o platformă multinațională instituită printr-un acord de consorțiu scris, astfel cum este menționat la alineatul (3). Acesta reunește într-o structură de rețea coordonată centrele cibernetice naționale ale statelor membre ale consorțiului-gazdă. Acesta este conceput pentru a îmbunătăți monitorizarea, detectarea și analiza amenințărilor cibernetice, pentru a preveni incidentele și a sprijini producerea de informații privind amenințările cibernetice, în special prin schimbul de date și informații relevante, anonimizate dacă este cazul, precum și prin partajarea instrumentelor de ultimă generație și prin dezvoltarea în comun a capacităților de detectare, analiză și prevenire și protecție în domeniul cibernetic într-un mediu de încredere.

(5) Un ***centru cibernetic*** transfrontalier este reprezentat din punct de vedere juridic de un ***membru al consorțiului-gazdă corespunzător*** care acționează în calitate de coordonator sau de consorțiul-gazdă, ***dacă acesta are personalitate juridică. Responsabilitatea pentru conformitatea centrului cibernetic transfrontalier cu prezentul regulament și*** cu acordul de găzduire și de utilizare ***se stabilește în acordul de consorțiu scris menționat la alineatul (3)***.

(6) Un stat membru se poate alătura unui consorțiu-gazdă existent cu acordul membrilor consorțiului-gazdă. Acordul de consorțiu scris menționat la alineatul (3) și acordul de găzduire și de utilizare se modifică în consecință. Acest lucru nu afectează drepturile de proprietate ale Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC) asupra instrumentelor, infrastructurilor sau serviciilor deja achiziționate în comun cu consorțiul-gazdă respectiv.

Articolul 6

Cooperarea și partajarea de informații în cadrul ***centrelor cibernetice*** transfrontaliere și între acestea

(1) Membrii unui consorțiu-gazdă ***se asigură că centrele lor cibernetice naționale partajează între ele în cadrul centrului cibernetic transfrontalier, în conformitate cu acordul de consorțiu scris menționat la articolul 5 alineatul (3), informații relevante, anonimizate dacă este cazul, cum ar fi*** informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromis, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurarea instrumentelor de securitate cibernetică pentru a detecta atacurile cibernetice, în cazul în care o astfel de partajare de informații:

(a) ***promovează și îmbunătățește detectarea amenințărilor cibernetice și consolidează capacitățile rețelei CSIRT de a preveni incidentele și de a răspunde la acestea sau de a le atenua impactul***;

(b) sporește nivelul de securitate cibernetică, ***de exemplu*** prin creșterea gradului de conștientizare cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea unei game de capacități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare, etapele proceselor de răspuns și de recuperare sau promovarea colaborării dintre entitățile publice și private în domeniul cercetării amenințărilor.

(2) Acordul de consorțiu scris menționat la articolul 5 alineatul (3) stabilește:

(a) un angajament de a partaja ***în rândul membrilor consorțiului-gazdă informațiile*** menționate la alineatul (1) și condițiile în care urmează să fie partajate informațiile respective;

(b) un cadru de guvernanță care să ***precizeze și să*** stimuleze partajarea între toți participanții de informații ***relevante, anonimizate dacă este cazul, menționate la alineatul (1)***;

(c) ținte privind contribuția la dezvoltarea unor instrumente ***și tehnologii*** avansate***, cum ar fi instrumentele*** de inteligență artificială și de analiză a datelor.

Acordul de consorțiu scris poate preciza că informațiile menționate la alineatul (1) trebuie să fie partajate în conformitate cu dreptul Uniunii și cu dreptul intern.

(3) Centrele cibernetice transfrontaliere încheie acorduri de cooperare între ele, specificând principiile de interoperabilitate și de partajare de informații între centrele cibernetice transfrontaliere. Centrele cibernetice transfrontaliere informează Comisia cu privire la acordurile de cooperare încheiate.

(4) ▌ Partajarea de informații ***menționată la alineatul (1)*** între ***centrele cibernetice transfrontaliere este asigurată printr-un*** nivel ridicat de interoperabilitate. ***Pentru a sprijini o astfel de interoperabilitate, ENISA, în strânsă consultare cu Comisia, fără întârzieri nejustificate și, în orice caz, până la ... [12 luni de la data intrării în vigoare a prezentului regulament], emite orientări privind interoperabilitatea care specifică în special formatele și protocoalele de partajare de informații, ținând seama de standardele internaționale și de cele mai bune practici, precum și de funcționarea oricăror centre cibernetice transfrontaliere existente. Cerințele de interoperabilitate prevăzute în acordurile de cooperare dintre centrele cibernetice transfrontaliere se bazează pe orientările emise de ENISA***.

▌

Articolul 7

Cooperarea și partajarea de informații cu ***rețelele de la nivelul*** Uniunii

(1) ***Centrele cibernetice transfrontaliere și rețeaua CSIRT cooperează îndeaproape, în special cu scopul de a partaja informații. În acest sens, ele convin asupra unor modalități procedurale privind cooperarea și partajarea de informații relevante și, fără a aduce atingere alineatului (2), privind tipurile de informații care urmează să fie partajate.***

(2) În cazul în care ***centrele cibernetice*** transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau aflat în curs, acestea ***se asigură, în scopul conștientizării comune a situației, că sunt furnizate informații relevante, precum și alerte timpurii autorităților statelor membre și Comisiei prin intermediul EU-CyCLONe și al rețelei CSIRT,*** fără întârzieri nejustificate.

I

Articolul 8

Securitate

(1) Statele membre care participă la ***sistemul*** european ***de alertă în materie de securitate cibernetică*** asigură un nivel ridicat ***de securitate cibernetică, inclusiv de confidențialitate și*** de securitate a datelor***, precum*** și de securitate fizică a rețelei ***sistemului*** european ***de alertă în materie de securitate cibernetică*** și se asigură că ***rețeaua*** este gestionată și controlată în mod adecvat, astfel încât să fie protejată de amenințări și să se garanteze securitatea sa și a sistemelor, inclusiv a datelor și ***informațiilor partajate*** prin intermediul ***rețelei***.

(2) Statele membre care participă la ***sistemul*** european ***de alertă în materie de securitate cibernetică*** se asigură că partajarea de informații ***menționată la articolul 6 alineatul (1)*** în cadrul ***sistemului*** european ***de alertă în materie de securitate cibernetică*** cu ***orice entitate, alta decât o autoritate sau un organism public al unui stat membru,*** nu afectează interesele în materie de securitate ale Uniunii ***sau ale statelor membre***.

Articolul 9

Finanțarea sistemului european de alertă în materie de securitate cibernetică

(1) În urma unei cereri de exprimare a interesului adresată statelor membre care intenționează să participe la sistemul european de alertă în materie de securitate cibernetică, ECCC selectează statele membre care urmează să participe în comun cu ECCC la achiziția publică de instrumente, infrastructuri sau servicii, pentru a pregăti funcționarea centrelor cibernetice naționale desemnate sau înființate în temeiul articolului 4 alineatul (1) sau pentru a consolida capacitățile unor astfel de centre. ECCC poate acorda granturi statelor membre selectate pentru a finanța funcționarea unor astfel de instrumente, infrastructuri sau servicii. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor, infrastructurilor sau serviciilor și până la 50 % din costurile de funcționare. Statele membre suportă restul costurilor. Înainte de lansarea procedurii de achiziție a instrumentelor, infrastructurilor sau serviciilor, ECCC și statele membre selectate încheie un acord de găzduire și de utilizare care reglementează utilizarea instrumentelor, infrastructurilor sau serviciilor.

(2) În cazul în care un centru cibernetic național al unui stat membru nu participă la un centru cibernetic transfrontalier în termen de doi ani de la data la care au fost achiziționate instrumentele, infrastructurile sau serviciile sau de la data la care a beneficiat de finanțare sub formă de granturi, luându-se în considerare data care survine mai întâi, statul membru nu este eligibil pentru sprijin suplimentar din partea Uniunii în temeiul prezentului capitol până nu se alătură unui centru cibernetic transfrontalier.

(3) În urma unei cereri de exprimare a interesului, un consorțiu-gazdă este selectat de către ECCC pentru a participa la o achiziție de instrumente, infrastructuri sau servicii în comun cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor, infrastructurilor sau serviciilor. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor, infrastructurilor sau serviciilor și până la 50 % din costurile de funcționare. Consorțiul-gazdă acoperă restul costurilor. Înainte de lansarea procedurii de achiziție a instrumentelor, infrastructurilor sau serviciilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și de utilizare care reglementează utilizarea instrumentelor, infrastructurilor sau serviciilor.

(4) ECCC pregătește, cel puțin o dată la doi ani, o cartografiere a instrumentelor, infrastructurilor sau serviciilor care sunt necesare și de o calitate adecvată pentru înființarea sau consolidarea capacităților centrelor cibernetice naționale și a centrelor cibernetice transfrontaliere, precum și a disponibilității acestora, inclusiv din partea entităților juridice stabilite sau considerate a fi stabilite în statele membre și controlate de statele membre sau de resortisanți ai statelor membre. Atunci când pregătește cartografierea, ECCC consultă rețeaua CSIRT, orice centru cibernetic transfrontalier existent, ENISA și Comisia.

Capitolul III

MECANISMUL PENTRU SITUAȚII DE URGENȚĂ ÎN MATERIE DE SECURITATE CIBERNETICĂ

Articolul 10

Instituirea mecanismului pentru situații de urgență în materie de securitate cibernetică

(1) Se instituie un mecanism pentru situații de urgență ***în materie de securitate cibernetică*** pentru a sprijini ***îmbunătățirea rezilienței*** Uniunii la amenințările cibernetice și pregătirea, în spiritul solidarității, pentru impactul pe termen scurt al incidentelor de securitate cibernetică semnificative***,*** al incidentelor de securitate cibernetică ***de mare amploare și*** al incidentelor de securitate cibernetică ***echivalente cu cele de mare amploare*** și pentru a atenua acest impact.

(2) În cazul statelor membre, acțiunile din cadrul mecanismului pentru situații de urgență în materie de securitate cibernetică sunt furnizate la cerere și sunt complementare eforturilor și acțiunilor statelor membre de pregătire legată de incidentele de securitate cibernetică, de răspuns la acestea și de redresare în urma lor.

(3) Acțiunile de punere în aplicare a ***mecanismului pentru situații de urgență în materie de securitate cibernetică*** sunt sprijinite prin finanțare din programul ***DEP*** și sunt puse în aplicare în conformitate cu Regulamentul (UE) 2021/694, în special cu obiectivul specific nr. 3 din regulamentul menționat.

(4) Acțiunile din cadrul mecanismului pentru situații de urgență în materie de securitate cibernetică sunt puse în aplicare cu precădere prin intermediul ECCC în conformitate cu Regulamentul (UE) 2021/887. Cu toate acestea, acțiunile de punere în aplicare a rezervei UE pentru securitate cibernetică, astfel cum sunt menționate la articolul 11 litera (b) din prezentul regulament, sunt implementate de către Comisie și ENISA.

Articolul 11

Tipuri de acțiuni

Mecanismul ***pentru situații de urgență în materie de securitate cibernetică*** sprijină următoarele tipuri de acțiuni:

(a) acțiuni de pregătire, ***și anume:***

(i) testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare cu o importanță critică ridicată în întreaga Uniune, astfel cum se specifică la articolul 12;

(ii) alte acțiuni de pregătire pentru entitățile care își desfășoară activitatea în sectoare cu o importanță critică ridicată sau pentru entitățile care își desfășoară activitatea în alte sectoare de importanță critică, astfel cum se specifică la articolul 13;

(b) acțiuni ▌ care sprijină răspunsul la incidentele de securitate cibernetică semnificative***,*** incidentele de securitate cibernetică ***de mare amploare și*** incidentele de securitate cibernetică ***echivalente cu cele de mare amploare*** și ***inițiază*** redresarea ▌ în urma acestora, care urmează să fie furnizate de furnizorii de încredere ***de servicii de securitate gestionate*** care participă la rezerva UE pentru securitate cibernetică instituită în temeiul articolului 14;

(c) acțiuni de sprijinire a asistenței reciproce***, astfel cum sunt menționate*** la articolul ***18***.

Articolul 12

Testarea coordonată a pregătirii entităților

(1) Mecanismul pentru situații de urgență în materie de securitate cibernetică sprijină testarea voluntară coordonată a pregătirii entităților care își desfășoară activitatea în sectoare cu o importanță critică ridicată.

(2) Testarea coordonată a pregătirii poate consta în activități de pregătire, cum ar fi testele de rezistență la intruziuni, și evaluarea amenințărilor.

(3) Sprijinul pentru acțiunile de pregătire în temeiul prezentului articol se acordă statelor membre în principal sub formă de granturi și în condițiile prevăzute în programele de lucru relevante, astfel cum sunt menționate la articolul 24 din Regulamentul (UE) 2021/694.

(4) În scopul de a sprijini testarea coordonată a pregătirii entităților menționate la articolul 11 litera (a) ***punctul (i)*** din prezentul regulament în întreaga Uniune, Comisia identifică, după consultarea Grupului de cooperare NIS***, a EU-CyCLONe*** și a ENISA, sectoarele sau subsectoarele vizate din sectoarele cu o importanță critică ridicată enumerate în anexa I la Directiva (UE) 2022/2555 ***pentru care se poate publica o cerere de propuneri pentru acordarea de granturi. Participarea statelor membre la respectivele cereri de propuneri este voluntară.***

(5) Atunci când identifică sectoarele sau subsectoarele menționate la alineatul (4), Comisia ține seama de evaluările coordonate ale riscurilor și de testele de reziliență de la nivelul Uniunii, precum și de rezultatele acestora.

(6) Grupul de cooperare NIS, în colaborare cu Comisia***, cu Înaltul Reprezentant pentru politica externă și de securitate comună (denumit în continuare „Înaltul Reprezentant”) și cu*** ENISA și***, în limitele mandatului său, cu UE-CyCLONe***, elaborează scenarii de risc și metodologii comune pentru testarea coordonată a pregătirii menționată ***la articolul 11 litera (a) punctul (i) și, după caz, pentru alte acțiuni de pregătire menționate la litera (a) punctul (ii) de la articolul menționat***.

(7) ***În cazul în care o entitate care își desfășoară activitatea într-un sector cu o importanță critică ridicată participă în mod voluntar la testarea coordonată a pregătirii, iar testarea respectivă conduce la recomandări privind măsuri specifice pe care entitatea participantă le-ar putea integra într-un plan de remediere, autoritatea statului membru responsabilă de testarea coordonată a pregătirii examinează, după caz, cursul dat măsurilor respective de către entitățile participante cu scopul de a consolida pregătirea.***

Articolul 13

Alte acțiuni de pregătire

(1) Mecanismul pentru situații de urgență în materie de securitate cibernetică sprijină acțiunile de pregătire care nu intră sub incidența articolului 12. Aceste acțiuni includ acțiuni de pregătire pentru entitățile din sectoarele care nu au fost identificate în vederea testării coordonate a pregătirii în temeiul articolului 12. Aceste acțiuni pot sprijini monitorizarea vulnerabilității, monitorizarea riscurilor, exercițiile și formarea.

(2) Sprijinul pentru acțiunile de pregătire în temeiul prezentului articol se acordă statelor membre la cerere și în principal sub formă de granturi și în condițiile prevăzute în programele de lucru relevante, astfel cum sunt menționate la articolul 24 din Regulamentul (UE) 2021/694.

Articolul 14

Instituirea rezervei UE pentru securitate cibernetică

(1) Se instituie o rezervă UE pentru securitate cibernetică pentru a sprijini***, la cerere,*** utilizatorii menționați la alineatul (3) să răspundă sau să ofere sprijin pentru răspunsul la incidentele de securitate cibernetică semnificative***,*** incidentele de securitate cibernetică ***de mare amploare sau*** incidentele de securitate cibernetică ***echivalente cu cele de mare amploare*** și pentru ***a inițial*** redresarea ▌ în urma unor astfel de incidente.

(2) Rezerva UE pentru securitate cibernetică constă în servicii de răspuns ▌ furnizate de furnizori de încredere ***de servicii de securitate gestionate*** selectați în conformitate cu criteriile prevăzute la articolul 17 alineatul (2). Rezerva UE pentru securitate cibernetică ***poate*** include servicii angajate în prealabil. Serviciile ***angajate în prealabil ale unui furnizor de încredere de servicii de securitate gestionate pot fi transformate în servicii de pregătire legate de prevenirea incidentelor și de răspunsul la incidente, în cazul în care respectivele servicii angajate în prealabil nu sunt utilizate pentru răspunsul la incidente în perioada în care sunt angajate în prealabil. Rezerva*** UE pentru securitate cibernetică poate fi desfășurată***, la cerere,*** în toate statele membre***, în instituțiile, organele, oficiile și agențiile Uniunii, precum și în țările terțe asociate la DEP, astfel cum sunt menționate la articolul 19 alineatul (1)***.

(3) ***Utilizatorii*** serviciilor furnizate de rezerva UE pentru securitate cibernetică ***sunt următorii***:

(a) autoritățile de gestionare a crizelor cibernetice și echipele CSIRT din statele membre, astfel cum sunt menționate la articolul 9 alineatele (1) și (2) și, respectiv, la articolul 10 din Directiva (UE) 2022/2555;

(b) ***CERT-UE, în conformitate cu articolul 13 din Regulamentul (UE, Euratom) 2023/2841***;

(c) autoritățile competente, cum ar fi echipele de răspuns la incidente de securitate cibernetică și autoritățile de gestionare a crizelor cibernetice din țările terțe asociate la DEP, în conformitate cu articolul 19 alineatul (8).

(4) Comisia are responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Comisia stabilește prioritățile și evoluția rezervei UE pentru securitate cibernetică ***în coordonare cu Grupul de cooperare NIS și***, în conformitate cu cerințele utilizatorilor menționați la alineatul (3), supraveghează punerea sa în aplicare și asigură complementaritatea, coerența, sinergiile și legăturile cu alte acțiuni de sprijin în temeiul prezentului regulament, precum și cu alte acțiuni și programe ale Uniunii. ***Prioritățile respective sunt analizate și, dacă este cazul, sunt revizuite o dată la doi ani. Comisia informează Parlamentul European și Consiliul cu privire la prioritățile respective și la orice revizuire a acestora.***

(5) ***Fără a aduce atingere responsabilității generale a Comisiei pentru punerea în aplicare a rezervei UE pentru securitate cibernetică menționată la alineatul (4) de la prezentul articol și sub rezerva acordului de contribuție definit la articolul 2 punctul 19 din Regulamentul (UE, Euratom) 2024/2509, Comisia încredințează ENISA, integral sau parțial, operarea și administrarea rezervei UE pentru securitate cibernetică. Aspectele care nu sunt încredințate ENISA fac în continuare obiectul gestiunii directe de către Comisie.***

(6) ***ENISA pregătește, cel puțin o dată la doi ani, o cartografiere a serviciilor de care au nevoie utilizatorii menționați la alineatul (3) literele (a) și (b) din prezentul articol. Cartografierea include și disponibilitatea unor astfel de servicii, inclusiv din partea entităților juridice stabilite sau considerate a fi stabilite în statele membre și controlate de statele membre sau de resortisanți ai statelor membre. Atunci când cartografiază această disponibilitate,*** ENISA ***evaluează competențele și capacitatea forței de muncă din Uniune în domeniul securității cibernetice care sunt pertinente pentru a realiza obiectivele rezervei UE pentru securitate cibernetică. Pentru a pregăti cartografierea, ENISA consultă Grupul de cooperare NIS, EU-CyCLONe, Comisia și, după caz, Consiliul interinstituțional pentru securitate cibernetică instituit în temeiul articolului 10 din Regulamentul (UE, Euratom) 2023/2841 (IICB). Atunci când cartografiază disponibilitatea serviciilor, ENISA consultă, de asemenea, părțile interesate relevante din sectorul securității cibernetice, inclusiv furnizorii de servicii de securitate gestionate. ENISA elaborează o cartografiere similară, după ce informează Consiliul și după ce consultă EU-CyCLONe,*** Comisia ***și***, după caz, ▌Înaltul Reprezentant***, pentru a identifica nevoile utilizatorilor menționați la alineatul (3) litera (c) din prezentul articol***.

(7) Comisia ***este împuternicită să adopte acte delegate în conformitate cu articolul 23 pentru a completa prezentul regulament prin specificarea*** tipurilor și a numărului de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică. ***Atunci când pregătește respectivele acte delegate, Comisia ține seama de cartografierea menționată la alineatul (6) de la prezentul articol și poate face schimb de opinii și coopera cu Grupul de cooperare NIS și cu ENISA.***

Articolul 15

Cereri de sprijin din rezerva UE pentru securitate cibernetică

(1) Utilizatorii menționați la articolul 14 alineatul (3) pot solicita servicii din rezerva UE pentru securitate cibernetică pentru a sprijini răspunsul la incidentele de securitate cibernetică semnificative***,*** incidentele de securitate cibernetică ***de mare amploare sau*** incidentele de securitate cibernetică ***echivalente cu cele de mare amploare*** și ***a inițial*** redresarea în urma acestora.

(2) Pentru a primi sprijin din rezerva UE pentru securitate cibernetică, utilizatorii menționați la articolul 14 alineatul (3) ***iau toate măsurile corespunzătoare*** cu scopul de a atenua efectele incidentului pentru care se solicită sprijin, inclusiv***, dacă este cazul,*** furnizarea de asistență tehnică directă și de alte resurse pentru a sprijini răspunsul la incident, precum și eforturile ▌ de redresare.

(3) Cererile de sprijin ▌ se transmit ***autorității contractante după cum urmează:***

(a) în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (a) din prezentul regulament, prin intermediul punctului unic de contact desemnat sau instituit temeiul articolului 8 alineatul (3) din Directiva (UE) 2022/2555;

(b) în cazul utilizatorului menționat la articolul 14 alineatul (3) litera (b), de către utilizatorul respectiv;

(c) în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (c), prin intermediul punctului unic de contact menționat la articolul 19 alineatul (9).

(4) ***În cazul cererilor utilizatorilor menționați la articolul 14 alineatul (3) litera (a),*** Statele membre informează rețeaua CSIRT și, după caz, EU-CyCLONe cu privire la cererile ***utilizatorilor*** lor de răspuns la incidente și de sprijin ***inițial*** pentru redresare în temeiul prezentului articol.

(5) Cererile de răspuns la incidente și de sprijin ***inițial*** pentru redresare includ:

(a) informații adecvate privind entitatea afectată și impactul potențial al incidentului***:***

(i) în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (a), asupra statelor membre și utilizatorilor afectați, inclusiv riscul de propagare către un alt stat membru;

(ii) în cazul utilizatorului menționat la articolul 14 alineatul (3) litera (b), asupra instituțiilor, organelor, oficiilor sau agențiilor Uniunii afectate;

(iii) în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (c), asupra țărilor asociate la DEP afectate;

(b) informații privind serviciul solicitat, precum și privind utilizarea prevăzută a sprijinului solicitat, inclusiv o indicație a nevoilor estimate;

(c) informații ***adecvate*** cu privire la măsurile luate pentru a atenua incidentul pentru care se solicită sprijin, astfel cum se menționează la alineatul (2);

(d) ***după caz,*** informații ***disponibile*** cu privire la alte forme de sprijin aflate la dispoziția entității afectate ▌.

(6) ENISA, în cooperare cu Comisia și cu ***EU-CyCLONe***, elaborează un model pentru a facilita transmiterea cererilor de sprijin din rezerva UE pentru securitate cibernetică.

(7) Comisia poate, prin intermediul unor acte de punere în aplicare, să precizeze modalitățile ***procedurale*** detaliate ***privind modul de a solicita serviciile*** de sprijin din rezerva UE pentru securitate cibernetică ***și modul de a răspunde la astfel de cereri în temeiul prezentului articol, al articolului 16 alineatul (1) și al articolului 19 alineatul (10), inclusiv modalitățile de depunere a unor astfel de cereri și de transmitere a răspunsurilor și modele pentru rapoartele menționate la articolul 16 alineatul (9)***. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 24 alineatul (2).

Articolul 16

Punerea în aplicare a sprijinului din rezerva UE pentru securitate cibernetică

(1) ***În cazul cererilor din partea utilizatorilor menționați la articolul 14 alineatul (3) literele (a) și (b),*** cererile de sprijin din rezerva UE pentru securitate cibernetică sunt evaluate de ***autoritatea contractantă***. ***Se transmite un răspuns utilizatorilor menționați la articolul 14 alineatul (3) literele (a) și (b) fără întârziere și, în orice caz, nu mai târziu de 48 de ore de la depunerea cererii, pentru a se asigura eficacitatea sprijinului. Autoritatea contractantă informează Consiliul și Comisia cu privire la rezultatele procedurii.***

(2) ***În ceea ce privește informațiile partajate în cursul solicitării și furnizării serviciilor din rezerva UE pentru securitate cibernetică, toate părțile implicate în aplicarea prezentului regulament:***

(a) ***limitează utilizarea și partajarea informațiilor respective la ceea ce este necesar pentru îndeplinirea obligațiilor sau funcțiilor care le revin în temeiul prezentului regulament;***

(b) ***utilizează și partajează informațiile confidențiale sau clasificate în temeiul dreptului Uniunii și al dreptului intern numai în conformitate cu dreptul respectiv; și***

(c) ***asigură un schimb de informații eficace, eficient și securizat, după caz, utilizând și respectând protocoalele relevante de partajare de informații, inclusiv protocolul de tip semafor.***

(3) ***La evaluarea cererilor individuale în temeiul articolului 16 alineatul (1) și al articolului 19 alineatul (10), autoritatea contractantă sau Comisia, după caz, evaluează mai întâi dacă sunt îndeplinite criteriile menționate la articolul 15 alineatele (1) și (2). În acest caz, autoritatea contractantă sau Comisia evaluează durata și natura corespunzătoare ale sprijinului, având în vedere obiectivul menționat la articolul 1 alineatul (3) litera (b) și următoarele criterii, după caz:***

(a) ***amploarea și*** gravitatea incidentului;

(b) tipul de entitate afectată, acordându-se o prioritate mai mare incidentelor care afectează entitățile esențiale, astfel cum sunt menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555;

(c) impactul potențial al incidentului asupra statelor membre afectate***, asupra instituțiilor, organelor, oficiilor sau agențiilor Uniunii sau asupra țărilor terțe asociate la DEP***;

(d) caracterul transfrontalier potențial al incidentului și riscul de propagare către alte state membre***, către instituțiile, organele, oficiile sau agențiile Uniunii sau către țările terțe asociate la DEP***;

(e) măsurile luate de utilizator pentru a sprijini răspunsul și eforturile ***inițiale*** de redresare, astfel cum se menționează la articolul 15 alineatul (2).

(4) Pentru a stabili ordinea de prioritate a cererilor, în cazul cererilor concurente din partea utilizatorilor menționați la articolul 14 alineatul (3), se iau în considerare criteriile menționate la alineatul (3) de la prezentul articol, după caz, fără a aduce atingere principiului cooperării loiale dintre statele membre și instituțiile, organele, oficiile și agențiile Uniunii. În cazul în care două sau mai multe cereri sunt evaluate ca fiind egale în temeiul criteriilor respective, se acordă o prioritate mai mare cererilor din partea utilizatorilor din statele membre. În cazul în care funcționarea și administrarea rezervei UE pentru securitate cibernetică au fost încredințate, integral sau parțial, ENISA în temeiul articolului 14 alineatul (5), ENISA și Comisia cooperează îndeaproape pentru a stabili ordinea de prioritate a cererilor în conformitate cu prezentul alineat.

(5) Serviciile din rezerva UE pentru securitate cibernetică sunt furnizate în conformitate cu acordurile specifice dintre furnizorul de ***încredere de servicii de securitate gestionate*** și utilizatorul căruia i se acordă sprijin din cadrul rezervei UE pentru securitate cibernetică. ***Serviciile respective pot fi furnizate în conformitate cu acordurile specifice dintre furnizorul de încredere de servicii de securitate gestionate, utilizator și entitatea afectată. Toate acordurile menționate la prezentul alineat*** includ***, printre altele,*** condiții de răspundere.

(6) Acordurile menționate la alineatul (5) se ***bazează*** pe modele elaborate de ENISA, după consultarea statelor membre ***și, după caz, a altor utilizatori ai rezervei UE pentru securitate cibernetică***.

(7) Comisia***, ENISA și utilizatorii rezervei*** UE pentru securitate cibernetică nu își asumă răspunderea contractuală pentru daunele cauzate terților de serviciile furnizate în cadrul punerii în aplicare a rezervei UE pentru securitate cibernetică.

(8) Utilizatorii pot utiliza serviciile rezervei UE pentru securitate cibernetică furnizate ca răspuns la o cerere formulată în temeiul articolului 15 alineatul (1) numai pentru a sprijini răspunsul la incidentele de securitate cibernetică semnificative, la incidentele de securitate cibernetică de mare amploare sau la incidentele de securitate cibernetică echivalente cu cele de mare amploare și pentru a iniția redresarea în urma acestora. Aceștia pot utiliza serviciile respective numai în ceea ce privește:

(a) entitățile care își desfășoară activitatea în sectoare cu o importanță critică ridicată sau entitățile care își desfășoară activitatea în alte sectoare de importanță critică, în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (a), și entitățile echivalente în cazul utilizatorilor menționați la articolul 15 alineatul (3) litera (c); și

(b) instituțiile, organele, oficiile și agențiile Uniunii, în cazul utilizatorului menționat la articolul 14 alineatul (3) litera (b).

(9) În termen de ***două luni*** de la încheierea sprijinului, ***utilizatorii care au beneficiat de sprijin*** prezintă ▌ un raport de sinteză privind serviciul furnizat, rezultatele obținute și învățămintele desprinse***:***

(a) Comisiei, ENISA, rețelei CSIRT și EU-CyCLONe, în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (a);

(b) Comisiei, ENISA și IICB, în cazul utilizatorului menționat la articolul 14 alineatul (3) litera (b);

(c) Comisiei, în cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (c).

Comisia transmite Consiliului și Înaltului Reprezentant orice raport de sinteză primit de la utilizatorii menționați la articolul 14 alineatul (3) în temeiul primului paragraf litera (c) de la prezentul alineat.

(10) În cazul în care funcționarea și administrarea rezervei UE pentru securitate cibernetică au fost încredințate, integral sau parțial, ENISA în temeiul articolului 14 alineatul (5) din prezentul regulament, ENISA informează și consultă periodic Comisia în acest sens. În acest context, ENISA transmite imediat Comisiei cererile pe care le primește de la utilizatorii menționați la articolul 14 alineatul (3) litera (c) din prezentul regulament și, atunci când acest lucru este necesar cu scopul de a stabili ordinea de prioritate în temeiul prezentului articol, cererile pe care le-a primit din partea utilizatorilor menționați la articolul 14 alineatul (3) litera (a) sau (b) din prezentul regulament. Obligațiile prevăzute la prezentul alineat nu aduc atingere articolului 14 din Regulamentul (UE) 2019/881.

(11) ***În cazul utilizatorilor menționați la articolul 14 alineatul (3) literele (a) și (b), autoritatea contractantă*** raportează periodic Grupului de cooperare NIS cu privire la utilizarea şi rezultatele sprijinului.

(12) În cazul utilizatorilor menționați la articolul 14 alineatul (3) litera (c), Comisia raportează Consiliului și informează Înaltul Reprezentant periodic și cel puțin de două ori pe an cu privire la utilizarea și rezultatele sprijinului.

I

Articolul 17

Furnizori de încredere de servicii de securitate gestionate

(1) În cadrul procedurilor de achiziții publice în scopul instituirii rezervei UE pentru securitate cibernetică, autoritatea contractantă acționează în conformitate cu principiile prevăzute în Regulamentul (UE, Euratom) 2024/2509 și cu următoarele principii:

(a) se asigură că ***serviciile cuprinse în*** rezerva UE pentru securitate cibernetică***, când sunt considerate ca un tot unitar, sunt de așa natură încât rezerva*** UE pentru securitate cibernetică să includă servicii care pot fi implementate în toate statele membre, ținând seama în special de cerințele naționale pentru furnizarea unor astfel de servicii, inclusiv în ceea ce privește limba, certificarea sau acreditarea;

(b) asigură protecția intereselor esențiale de securitate ale Uniunii și ale statelor sale membre;

(c) se asigură că rezerva UE pentru securitate cibernetică aduce valoare adăugată pentru Uniune, contribuind la obiectivele prevăzute la articolul 3 din Regulamentul (UE) 2021/694, inclusiv prin promovarea dezvoltării competențelor în materie de securitate cibernetică în Uniune.

(2) Atunci când achiziționează servicii pentru rezerva UE pentru securitate cibernetică, autoritatea contractantă include în documentele achiziției următoarele criterii și cerințe:

(a) furnizorul demonstrează că personalul său are cel mai înalt grad de integritate profesională, independență, responsabilitate și competență tehnică necesară pentru a desfășura activitățile în domeniul său specific și asigură permanența și continuitatea cunoștințelor de specialitate, precum și resursele tehnice necesare;

(b) furnizorul, ***precum și orice filiale și subcontractanți relevanți respectă normele aplicabile privind protecția informațiilor clasificate și*** instituie ***măsuri adecvate, inclusiv, după caz, acorduri între ei,*** pentru protecția informațiilor ***confidențiale*** referitoare la serviciu, în special a dovezilor, a constatărilor și a rapoartelor ▌ ;

(c) furnizorul pune la dispoziție dovezi suficiente că structura sa de conducere este transparentă și nu este susceptibilă de a compromite imparțialitatea și calitatea serviciilor sale sau de a cauza conflicte de interese;

(d) furnizorul deține o autorizare de securitate adecvată, cel puțin pentru personalul destinat implementării serviciilor***, dacă o astfel de cerință este impusă de un stat membru***;

(e) furnizorul dispune de nivelul relevant de securitate pentru sistemele sale informatice;

(f) furnizorul este dotat cu echipamentele ▌ hardware și software necesare pentru a sprijini serviciul solicitat***, care nu au vulnerabilități exploatabile cunoscute, are instalate ultimele actualizări de securitate și în orice caz respectă toate dispozițiile aplicabile din Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului***[23+]***;***

(g) furnizorul este în măsură să demonstreze că are experiență în furnizarea de servicii similare autorităților naționale relevante, entităților care își desfășoară activitatea în sectoare ***cu o importanță critică ridicată sau entităților care își desfășoară activitatea în alte sectoare de importanță critică***;

---

[23] ***Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... (JO L, …, ELI: …).***

[+] ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 100/23 [2022/0272(COD)] și a se introduce numărul, data, titlul și referința de publicare în JO și referința ELI a regulamentului respectiv în nota de subsol aferentă.***

(h) furnizorul este în măsură să furnizeze serviciul într-un termen scurt în statele membre în care poate furniza serviciul;

(i) furnizorul este în măsură să furnizeze serviciul ***în una sau mai multe limbi oficiale ale instituțiilor Uniunii sau ale unui stat membru, după cum solicită, eventual, statele membre sau utilizatorii menționați la articolul 14 alineatul (3) literele (b) și (c), în cazul*** în care ***furnizorul*** poate furniza serviciul;

(j) odată ce se instituie ▌ un sistem ***european*** de certificare ***a securității cibernetice*** pentru ***serviciile*** de securitate ***gestionate*** în conformitate cu Regulamentul (UE) 2019/881, furnizorul este certificat în conformitate cu sistemul respectiv***, în termen de doi ani de la data la care se aplică sistemul***;

(k) furnizorul include în ofertă condițiile de conversie pentru orice serviciu neutilizat de răspuns la incidente care ar putea fi transformat în servicii de pregătire strâns legate de răspunsul la incidente, de exemplu exerciții sau cursuri de formare.

(3) În scopul achiziționării de servicii pentru rezerva UE pentru securitate cibernetică, autoritatea contractantă poate, după caz, să precizeze criterii și cerințe suplimentare față de cele menționate la alineatul (2), în strânsă cooperare cu statele membre.

Articolul 18

Acțiuni de sprijinire a asistenței reciproce

(1) Mecanismul pentru situații de urgență în materie de securitate cibernetică oferă sprijin pentru asistența acordată de un stat membru altui stat membru afectat de un incident de securitate cibernetică semnificativ sau de un incident de securitate cibernetică de mare amploare, inclusiv în cazurile menționate la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555.

(2) Sprijinul pentru asistența tehnică reciprocă menționat la alineatul (1) de la prezentul articol se acordă sub formă de granturi și în condițiile prevăzute în programele de lucru relevante, astfel cum sunt menționate la articolul 24 din Regulamentul (UE) 2021/694.

Articolul 19

Sprijinul acordat țărilor terțe ***asociate la DEP***

(1) ***O țară terță asociată la DEP*** poate solicita sprijin din rezerva UE pentru securitate cibernetică ***în cazul în care acordul prin care este asociată la DEP prevede participarea la rezerva*** UE pentru securitate cibernetică. ***Acordul respectiv conține dispoziții care impun țării terțe asociate la DEP în cauză să respecte obligațiile prevăzute la alineatele (2) și (9) de la prezentul articol. În scopul participării unei țări terțe la rezerva UE pentru securitate cibernetică, asocierea parțială a unei țări terțe la DEP poate include o asociere limitată la obiectivul operațional menționat la articolul 6 alineatul (1) litera (g) din Regulamentul (UE) 2021/694.***

(2) În termen de trei luni de la încheierea acordului menționat la alineatul (1) și în orice caz înainte de a primi orice sprijin din rezerva UE pentru securitate cibernetică, țara terță ***asociată la DEP*** furnizează Comisiei ▌ informații cu privire la reziliența sa cibernetică și la capacitățile sale de gestionare a riscurilor, incluzând cel puțin informații cu privire la măsurile naționale luate în vederea pregătirii legate de incidente de securitate cibernetică semnificative sau incidente de securitate cibernetică ***echivalente cu cele de mare amploare***, precum și informații privind entitățile naționale responsabile, inclusiv ***echipele de răspuns la incidente de securitate cibernetică*** sau entitățile echivalente, capacitățile acestora și resursele care le sunt alocate. ***Țara terță asociată la DEP transmite periodic și cel puțin o dată pe an actualizări ale informațiilor respective. Comisia transmite informațiile respective Înaltului Reprezentant și ENISA în scopul de a facilita aplicarea*** alineatului (11).

(3) Comisia evaluează periodic, cel puțin o dată pe an, următoarele criterii pentru fiecare țară terță asociată la DEP menționată la alineatul (1):

(a) dacă țara respectivă respectă clauzele acordului menționat la alineatul (1), în măsura în care clauzele respective se referă la participarea la rezerva UE pentru securitate cibernetică;

(b) dacă țara respectivă a luat măsuri adecvate pentru pregătirea legată de incidentele de securitate cibernetică semnificative sau incidentele de securitate cibernetică echivalente cu cele de mare amploare, pe baza informațiilor menționate la alineatul (2); și

(c) dacă sprijinul acordat este în concordanță cu politica Uniunii față de țara respectivă și cu relațiile generale cu ea și consecvent cu alte politici ale Uniunii în domeniul securității.

Comisia se consultă cu Înaltul Reprezentant atunci când realizează evaluarea menționată la primul paragraf, în legătură cu criteriul menționat la litera (c) de la paragraful respectiv.

În cazul în care ajunge la concluzia că o țară terță asociată la DEP îndeplinește toate condițiile menționate la primul paragraf, Comisia transmite Consiliului spre adoptare o propunere de act de punere în aplicare în conformitate cu alineatul (4) care autorizează acordarea de sprijin din rezerva UE pentru securitate cibernetică țării respective.

(4) ***Consiliul poate adopta actele de punere în aplicare menționate la alineatul (3). Respectivele acte de punere în aplicare se aplică timp de maximum un an. Acestea pot fi reînnoite. Acestea pot conține o limită de minimum 75 de zile referitoare la numărul de zile în care se poate acorda sprijin ca răspuns la o singură cerere.***

În sensul prezentului articol, Consiliul acționează cu promptitudine și, de regulă, adoptă actele de punere în aplicare menționate la prezentul alineat în termen de opt săptămâni de la adoptarea propunerii relevante a Comisiei în temeiul alineatului (3) al treilea paragraf.

(5) ***Consiliul poate modifica sau abroga în orice moment un act de punere în aplicare adoptat în temeiul alineatului (4), pe baza unei propuneri a Comisiei.***

Dacă consideră că a intervenit o modificare semnificativă a criteriului menționat la alineatul (3) primul paragraf litera (c), Consiliul poate modifica sau abroga un act de punere în aplicare adoptat în temeiul alineatului (4), la inițiativa motivată corespunzător a unuia sau mai multor state membre.

(6) ***În exercitarea competențelor sale de executare în temeiul prezentului articol, Consiliul aplică criteriile menționate la alineatul (3) primul paragraf și explică cum a evaluat criteriile respective. În special, dacă acționează din proprie inițiativă în temeiul alineatului (5) al doilea paragraf, Consiliul explică modificarea semnificativă menționată la paragraful respectiv.***

(7) Sprijinul din rezerva UE pentru securitate cibernetică ***acordat unei țări asociate la DEP*** respectă toate condițiile specifice prevăzute în ***acordul*** menționat la alineatul (1).

(8) Printre utilizatorii din țările terțe asociate ***la DEP*** eligibile pentru a beneficia de servicii din rezerva UE pentru securitate cibernetică se numără autoritățile competente, cum ar fi ***echipele de răspuns la incidentele de securitate cibernetică*** sau entitățile echivalente și autoritățile de gestionare a crizelor cibernetice.

(9) Fiecare țară terță ***asociată la DEP*** eligibilă pentru sprijin din rezerva UE pentru securitate cibernetică desemnează o autoritate care să acționeze ca punct unic de contact în sensul prezentului regulament.

(10) ***Cererile de sprijin din partea rezervei UE pentru securitate cibernetică se evaluează de către Comisie. Autoritatea contractantă poate acorda sprijin unei țări terțe numai dacă și atât timp cât este în vigoare un act de punere în aplicare al Consiliului care autorizează un astfel de sprijin pentru țara respectivă, adoptat în temeiul alineatului (4) din prezentul articol. Utilizatorii menționați la articolul 14 alineatul (3) litera (c) primesc un răspuns fără întârzieri nejustificate.***

(11) ***La primirea unei cereri de sprijin în temeiul prezentului articol, Comisia informează imediat Consiliul. Comisia comunică Consiliului rezultatul evaluării cererii.*** Comisia ***cooperează și*** cu Înaltul Reprezentant cu privire la cererile primite și la mobilizarea sprijinului acordat țărilor terțe ***asociate la DEP*** din rezerva UE pentru securitate cibernetică. ***În plus, Comisia ține seama de orice opinie exprimată de ENISA în legătură cu cererile respective.***

Articolul 20

Coordonarea cu mecanismele Uniunii de gestionare a crizelor

(1) În cazurile în care un incident de securitate cibernetică semnificativ, un incident de securitate cibernetică de mare amploare sau un incident de securitate cibernetică echivalent cu cele de mare amploare se datorează unor dezastre sau produce dezastre în sensul definiției de la articolul 4 punctul 1 din Decizia nr. 1313/2013/UE, sprijinul acordat în temeiul prezentului regulament pentru a răspunde la astfel de incidente completează acțiunile adoptate în temeiul deciziei menționate și nu contravine acestora.

(2) În cazul unui incident de securitate cibernetică de mare amploare sau a unui incident de securitate cibernetică echivalent cu cele de mare amploare în care este activat mecanismul integrat al Uniunii pentru un răspuns politic la crize (mecanismul IPCR) în temeiul Deciziei de punere în aplicare (UE) 2018/1993, sprijinul acordat în temeiul prezentului regulament pentru răspunsul la un astfel de incident este gestionat în conformitate cu protocoalele și procedurile relevante din cadrul mecanismului IPCR.

Capitolul IV

MECANISMUL EUROPEAN DE ANALIZĂ A INCIDENTELOR DE SECURITATE CIBERNETICĂ

Articolul 21

Mecanismul european de analiză a incidentelor de securitate cibernetică

(1) La cererea Comisiei ***sau a EU-CyCLONe, ENISA, susținută de*** rețeaua CSIRT ***și cu aprobarea statelor membre în cauză***, analizează și evaluează amenințările cibernetice, vulnerabilitățile ***exploatabile cunoscute*** și acțiunile de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau un anumit incident de securitate cibernetică de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA***, cu scopul de a trage învățăminte astfel încât să evite sau să atenueze pe viitor incidente,*** transmite ***EU-CyCLONe,*** rețelei CSIRT, ***statelor membre în cauză*** și Comisiei un raport de analiză a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, în special a sarcinilor prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. ***În cazul în care un incident are un impact asupra unei țări terțe asociate la DEP, ENISA transmite raportul Consiliului. În aceste cazuri***, Comisia transmite raportul Înaltului Reprezentant.

(2) Pentru a elabora raportul de analiză a incidentelor menționat la alineatul (1) de la prezentul articol, ENISA cooperează cu toate părțile interesate relevante, inclusiv reprezentanți ai statelor membre, Comisia sau alte instituții, organe***, oficii*** și agenții relevante ale Uniunii, ***reprezentanți ai sectorului, printre care*** furnizori de servicii de securitate gestionate și utilizatori de servicii de securitate cibernetică și colectează feedback de la aceștia. După caz, ENISA***, în cooperare cu echipele CSIRT și, după caz, cu autoritățile competente desemnate sau instituite în temeiul articolului 8 alineatul (1) din Directiva (UE) 2022/2555, cooperează și cu entitățile afectate de incidente de securitate cibernetică semnificative sau de incidente de securitate cibernetică de mare amploare***. Reprezentanții consultați comunică orice potențial conflict de interese.

(3) Raportul de analiză a incidentelor menționat la alineatul (1) de la prezentul articol cuprinde o evaluare și o analiză a respectivului incident de securitate cibernetică semnificativ sau a respectivului incident de securitate cibernetică de mare amploare, incluzând principalele cauze, vulnerabilități ***exploatabile cunoscute*** și învățăminte desprinse. ***ENISA se asigură că raportul respectă*** dreptul Uniunii sau dreptul intern privind protecția informațiilor sensibile sau clasificate. ***Dacă statele membre relevante sau alți utilizatori menționați la articolul 14 alineatul (3) care sunt afectați de incident solicită acest lucru, datele și informațiile din raport se anonimizează. Raportul nu poate conține detalii despre vulnerabilități exploatate activ și care nu sunt încă remediate.***

(4) După caz, raportul de analiză a incidentelor formulează recomandări pentru a îmbunătăți poziția cibernetică a Uniunii ***și poate cuprinde bune practici și lecții învățate de la părțile interesate relevante***.

(5) ***ENISA poate publica*** o versiune a raportului de analiză a incidentelor ***destinată publicului***. ***Versiunea respectivă a raportului cuprinde doar informații publice fiabile sau alte informații fiabile cu consimțământul statelor membre în cauză și, în cazul unor informații referitoare la un utilizator menționat la articolul 14 alineatul (3) litera (b) sau (c), cu consimțământul utilizatorului respectiv.***

Capitolul V

DISPOZIȚII FINALE

Articolul 22

Modificarea Regulamentului (UE) 2021/694

Regulamentul (UE) 2021/694 se modifică după cum urmează:

1. Articolul 6 se modifică după cum urmează:

(a) alineatul (1) se modifică după cum urmează:

(i) se introduce următoarea literă:

„(aa) sprijinirea dezvoltării ***sistemului european de alertă în materie de securitate cibernetică instituit prin articolul 3 din Regulamentul (UE) .../... al Parlamentului European și al Consiliului**+ (denumit în continuare „sistemul european de alertă în materie de securitate cibernetică”)***, inclusiv dezvoltarea, implementarea și operarea ***de platforme cibernetice*** naționale și transfrontaliere care să contribuie la conștientizarea situației în Uniune și la consolidarea capacităților informaționale strategice ale Uniunii privind amenințările cibernetice;

---

* ***Regulamentul (UE) .../... al Parlamentului European și al Consiliului din ... 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***

+ JO: a se introduce în text numărul regulamentului ***conținut în documentul PE-CONS 94/24 [2023/0109(COD)] și a se introduce numărul, data, titlul și referința de publicare în JO și referința ELI a regulamentului respectiv în nota de subsol aferentă.***

modificare a Regulamentului (UE) 2021/694 (Regulamentul privind solidaritatea cibernetică) (JO L, ..., ELI: ...)";

(ii) se adaugă următoarea literă:

„(g) instituirea și operarea mecanismului pentru situații de urgență în materie ***de securitate*** cibernetică instituit prin articolul 10 din Regulamentul (UE) .../...[+], inclusiv a rezervei UE pentru securitate cibernetică ***instituite prin articolul 14 din regulamentul respectiv (denumită în continuare „rezerva UE pentru securitate cibernetică”)***, pentru a sprijini statele membre în pregătirea legată de incidentele de securitate cibernetică semnificative și de incidentele de securitate cibernetică de amploare și pentru răspunsul la acestea, care este complementar resurselor și capacităților naționale și altor forme de sprijin disponibile la nivelul Uniunii, și sprijinirea altor utilizatori pentru a răspunde incidentelor de securitate cibernetică semnificative și incidentelor de securitate cibernetică echivalente cu cele de mare amploare;”;

(b) alineatul (2) se înlocuiește cu următorul text:

„(2) ***Acțiunile din cadrul obiectivului specific nr. 3 sunt implementate cu precădere prin intermediul Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și al Rețelei de centre naționale de coordonare în conformitate cu Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului*. Cu toate acestea, rezerva UE pentru securitate cibernetică este implementată de către Comisie și, în conformitate cu articolul 14 alineatul (6) din Regulamentul (UE) 2024/..., de către ENISA.***

---

* ***Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de***

[+] ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

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).”

2. Articolul 9 se modifică după cum urmează:

(a) la alineatul (2), literele (b), (c) și (d) se înlocuiesc cu următorul text:

„(b) ***1 760 806 000*** EUR pentru obiectivul specific nr. 2 – Inteligența artificială;

(c) ***1 372 020 000*** EUR pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea;

(d) ***482 640 000*** EUR pentru obiectivul specific nr. 4 – Competențele digitale avansate;”;

(b) se adaugă următorul alineat:

„(8) Prin derogare de la articolul 12 alineatul (1) din Regulamentul financiar, creditele de angajament și de plată neutilizate pentru acțiuni care***, în contextul executării rezervei UE pentru securitate cibernetică și a acțiunilor de sprijinire a asistenței reciproce în temeiul Regulamentului .../...+,*** urmăresc obiectivele prevăzute la articolul 6 alineatul (1) litera (g) din prezentul regulament se reportează automat și pot fi angajate și plătite până la data de 31 decembrie a exercițiului financiar următor. ***Comisia informează Parlamentul European și Consiliul cu privire la creditele reportate în temeiul articolului 12 alineatul (6) din Regulamentul financiar.***”

+ ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

3. Articolul 12 se modifică după cum urmează:

(a) se introduc următoarele alineate:

„(5a) Alineatul (5) nu se aplică, în ceea ce privește entitățile juridice stabilite în Uniune, dar care sunt controlate din țări terțe, niciunei acțiuni de declanșare a sistemului european de alertă în materie de securitate cibernetică dacă sunt îndeplinite cumulativ următoarele două condiții în raport cu acțiunea în cauză:

(a) există un risc real, ținând seama de rezultatele cartografierii realizate în temeiul articolului 9 alineatul (4) din Regulamentul (UE) 2024/...[+], ca instrumentele, infrastructurile sau serviciile care sunt necesare și suficiente pentru ca acțiunea respectivă să contribuie în mod adecvat la obiectivul sistemului european de alertă în materie de securitate cibernetică să nu poată fi procurate de la entități juridice stabilite sau considerate a fi stabilite în statele membre și controlate de statele membre sau de resortisanți ai statelor membre;

(b) riscul de securitate pe care îl prezintă achizițiile de la astfel de entități juridice pentru sistemul european de alertă în materie de securitate cibernetică este proporțional cu beneficiile și nu subminează interesele esențiale de securitate ale Uniunii și ale statelor sale membre.

[+] ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

(5b) Alineatul (5) nu se aplică, în ceea ce privește entitățile juridice stabilite în Uniune, dar care sunt controlate din țări terțe, niciunei acțiuni de mobilizare a rezervei UE pentru securitate cibernetică dacă sunt îndeplinite cumulativ următoarele două condiții în raport cu acțiunea în cauză:

(a) există un risc real, ținând seama de rezultatele cartografierii realizate în temeiul articolului 14 alineatul (6) din Regulamentul (UE) 2024/...+, ca tehnologia, cunoștințele de specialitate sau capacitatea care este necesară și suficientă pentru ca rezerva UE pentru securitate cibernetică să își îndeplinească funcțiile în mod adecvat să nu poată fi procurate de la entități juridice stabilite sau considerate a fi stabilite în statele membre și controlate de statele membre sau de resortisanți ai statelor membre;

(b) riscul de securitate pe care îl prezintă cooptarea unor astfel de entități juridice în rezerva UE pentru securitate cibernetică este proporțional cu beneficiile și nu subminează interesele esențiale de securitate ale Uniunii și ale statelor sale membre.”;

(b) alineatul (6) se înlocuiește cu următorul text:

„***(6) Dacă există motive bine justificate de securitate, programul de lucru poate prevedea, de asemenea, că entitățile juridice stabilite în țări asociate și entitățile juridice care sunt stabilite în Uniune, dar sunt controlate din țări terțe pot fi eligibile să participe la toate sau la o parte dintre acțiunile din cadrul obiectivelor specifice nr. 1 și nr. 2 doar dacă respectă cerințele ce trebuie îndeplinite de către entitățile juridice respective pentru a garanta protecția intereselor de securitate esențiale ale Uniunii și ale statelor membre ale acesteia și pentru a asigura protecția informațiilor din documentele clasificate. Respectivele cerințe se stabilesc în programul de lucru.***

Primul paragraf se aplică, în ceea ce privește entitățile juridice stabilite în Uniune, dar care sunt controlate din țări terțe, și acțiunilor din cadrul obiectivului specific nr. 3 care vizează:

(a) declanșarea sistemului european de alertă în materie de securitate cibernetică, în cazurile în care se aplică alineatul (5a); și

(b) mobilizarea rezervei UE pentru securitate cibernetică, în cazurile în care se aplică alineatul (5b)."

4. La articolul 14, alineatul (2) se înlocuiește cu următorul text:

„(2) Programul poate oferi finanțare sub oricare dintre formele prevăzute de Regulamentul financiar, în special sub formă de achiziții publice ca formă primară de finanțare, sau sub formă de granturi și premii.

Atunci când îndeplinirea obiectivului unei acțiuni necesită achiziționarea de bunuri și servicii inovatoare, granturile pot fi acordate doar beneficiarilor care sunt autorități contractante sau entități contractante, astfel cum sunt definite în Directivele 2014/24/UE* și 2014/25/UE** ale Parlamentului European și ale Consiliului.

Atunci când furnizarea de bunuri sau servicii inovatoare care nu sunt încă comercializate pe scară largă este necesară pentru îndeplinirea obiectivelor unei acțiuni, autoritatea contractantă sau entitatea contractantă poate autoriza atribuirea mai multor contracte în cadrul aceleiași proceduri de achiziție.

Din motive bine justificate de siguranță publică, autoritatea contractantă sau entitatea contractantă poate solicita ca locul de desfășurare a contractului să fie pe teritoriul Uniunii.

Atunci când derulează proceduri de achiziții pentru rezerva UE pentru securitate cibernetică, Comisia și ENISA pot acționa ca organism central de achiziție pentru a achiziționa în numele sau în contul țărilor terțe asociate la program, în conformitate cu articolul 10 din prezentul regulament. De asemenea, Comisia și ENISA pot acționa în calitate de angrosiști, prin cumpărarea, stocarea și revânzarea sau donarea de bunuri și servicii, inclusiv închiriate, către țările terțe respective. Prin derogare de la articolul 168 alineatul (3) din Regulamentul (UE, Euratom) 2024/2509 ***al Parlamentului European și al Consiliului****, solicitarea din partea unei singure țări terțe este suficientă pentru a mandata Comisia sau ENISA să acționeze.

Atunci când derulează proceduri de achiziții pentru rezerva UE pentru securitate cibernetică, Comisia și ENISA pot acționa ca organism central de achiziție pentru a achiziționa în numele sau în contul instituțiilor, organelor**,** ***oficiilor*** sau agențiilor Uniunii. De asemenea, Comisia și ENISA pot acționa în calitate de angrosiști, prin cumpărarea, stocarea și revânzarea sau donarea de bunuri și servicii, inclusiv închiriate, către instituțiile, organele***, oficiile*** sau agențiile Uniunii. Prin derogare de la articolul 168 alineatul (3) din Regulamentul (UE, Euratom) 2024/2509, solicitarea din partea unei singure instituții, a unui singur organ sau oficiu ori a unei singure agenții a Uniunii este suficientă pentru a mandata Comisia sau ENISA să acționeze.

Totodată, programul poate furniza finanțare sub formă de instrumente financiare în cadrul operațiunilor de finanțare mixtă.

---

* ***Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 094 28.3.2014, p. 65).***

** ***Directiva 2014/25/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile efectuate de entitățile care își desfășoară activitatea în sectoarele apei, energiei, transporturilor și serviciilor poștale și de abrogare a Directivei 2004/17/CE (JO L 094 28.3.2014, p. 243).***

*** ***Regulamentul (UE, Euratom) 2024/2509 al Parlamentului European și al Consiliului din 23 septembrie 2024 privind normele financiare aplicabile bugetului general al Uniunii (JO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).”***

5. Se introduce următorul articol:

„***Articolul 16a***

Conflictul de norme

În cazul acțiunilor de punere în aplicare a ***sistemului*** european ***de alertă în materie de securitate cibernetică***, normele aplicabile sunt cele prevăzute la articolele 4,5 și 9 din Regulamentul (UE) .../...+. În cazul unui conflict între dispozițiile prezentului regulament și articolele 4, 5 și 9 din Regulamentul (UE) ***2024/...***+, acesta din urmă prevalează și se aplică acțiunilor specifice respective.

În cazul rezervei UE pentru securitate cibernetică, sunt prevăzute norme specifice pentru participarea țărilor terțe asociate la program la articolul 19

\+ ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

din Regulamentul (UE) 2024/...+. În cazul unui conflict între dispozițiile prezentului regulament și articolul 19 din Regulamentul (UE) 2024/...+, acesta din urmă prevalează și se aplică acțiunilor specifice respective.”

6. Articolul 19 se înlocuiește cu următorul text:

„Articolul 19

Granturi

Granturile din cadrul programului sunt acordate și gestionate în conformitate cu titlul VIII din ***Regulamentul financiar*** și pot acoperi până la 100 % din costurile eligibile, fără a aduce atingere principiului cofinanțării prevăzut la articolul 190 din ***Regulamentul financiar***. Astfel de granturi sunt acordate și gestionate astfel cum este specificat pentru fiecare obiectiv specific.

Sprijinul sub formă de granturi poate fi acordat direct de ECCC, fără o cerere de propuneri, ***statelor membre selectate*** în temeiul articolului 9 din Regulamentul ***(UE) 2024/...*** [+] și ***consorțiului***-gazdă menționat la articolul 5 din Regulamentul ***(UE) 2024/...***[+] în conformitate cu articolul 195 alineatul (1) litera (d) din Regulamentul financiar.

Sprijinul sub formă de granturi pentru mecanismul pentru situații de urgență în materie ***de securitate cibernetică***, poate fi acordat direct de ECCC statelor membre fără o cerere de propuneri, în conformitate cu articolul 195 alineatul (1) litera (d) din Regulamentul financiar.

[+] ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

În ceea ce privește acțiunile de sprijinire a asistenței reciproce prevăzute la articolul 18 din Regulamentul ***(UE) 2024/...***[+], ECCC informează Comisia și ENISA cu privire la cererile de granturi directe ale statelor membre fără o cerere de propuneri.

În ceea ce privește acțiunile de sprijinire a asistenței reciproce prevăzute la articolul 18 din Regulamentul ***(UE) 2024/...***[+] și în conformitate cu articolul 193 alineatul (2) al doilea paragraf litera (a) din Regulamentul financiar, în cazuri justificate în mod corespunzător, costurile pot fi considerate eligibile chiar dacă au fost suportate înainte de depunerea cererii de grant.”

7. Anexele I și II se modifică în conformitate cu anexa la prezentul regulament.

[+] ***JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 94/24 [2023/0109(COD)].***

Articolul 23

Exercitarea delegării de competențe

(1) ***Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.***

(2) ***Competența de a adopta acte delegate menționată la articolul 14 alineatul (7) se conferă Comisiei pe o perioadă de 5 ani de la ... [data intrării în vigoare a prezentului regulament]. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.***

(3) Delegarea de competențe menționată la articolul 14 alineatul (7) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) ***Un act delegat adoptat în temeiul articolului 14 alineatul (7) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu, sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor ridica obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.***

Articolul 24

Procedura comitetului

(1) Comisia este asistată de Comitetul de coordonare al programului „Europa digitală” menționat la articolul 31 alineatul (1) din Regulamentul (UE) 2021/694. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 25

Evaluarea ***și revizuirea***

(1) ***Până la ...*** [***doi*** ani de la data intrării în vigoare a prezentului regulament] ***și, ulterior, o dată la patru ani, Comisia evaluează funcționarea măsurilor prevăzute în prezentul regulament și*** prezintă ***un raport*** Parlamentului European și Consiliului ▌ .

(2) ***Evaluarea menționată la alineatul (1) analizează în special următoarele:***

(a) ***numărul de centre cibernetice naționale și de centre cibernetice transfrontaliere înființate, amploarea informațiilor partajate, inclusiv, dacă este posibil, impactul asupra activității rețelei CSIRT, și măsura în care au contribuit la o mai bună detectare și conștientizare a situației comune din Uniune cu privire la amenințările cibernetice și incidente și la dezvoltarea unor tehnologii de ultimă generație; cum au fost utilizate fondurile din cadrul DEP pentru instrumentele, infrastructurile sau serviciile de securitate cibernetică achiziționate în comun; și, dacă informațiile sunt disponibile, nivelul de cooperare dintre centrele cibernetice naționale și comunitățile sectoriale și intersectoriale ale entităților esențiale și importante, astfel cum sunt menționate la articolul 3 din Directiva (UE) 2022/2555;***

(b) modul de utilizare și eficiența acțiunilor din cadrul mecanismului pentru situații de urgență în materie de securitate cibernetică care sprijină eforturile de pregătire, inclusiv formarea, răspunsul la incidentele de securitate cibernetică semnificative, incidentele de securitate cibernetică de mare amploare și incidentele de securitate cibernetică echivalente cu cele de mare amploare și redresarea inițială în urma acestora, inclusiv mobilizarea finanțării din cadrul DEP, precum și lecțiile învățate și recomandările care decurg din implementarea mecanismului pentru situații de urgență în materie de securitate cibernetică;

(c) modul de utilizare și eficiența rezervei UE pentru securitate cibernetică în raport cu tipurile de utilizatori, inclusiv utilizarea finanțării din cadrul DEP, frecvența utilizării serviciilor, inclusiv tipul lor, timpul mediu de răspuns la cereri și pentru mobilizarea rezervei UE pentru securitate cibernetică, ponderea serviciilor convertite în servicii de pregătire pentru prevenirea incidentelor și răspunsul la incidente, precum și lecțiile învățate și recomandările care decurg din implementarea rezervei UE pentru securitate cibernetică;

(d) contribuția prezentului regulament la consolidarea poziției concurențiale a industriei și a serviciilor din Uniune în întreaga economie digitală, inclusiv a microîntreprinderilor și a întreprinderilor mici și mijlocii, precum și a întreprinderilor nou-înființate și contribuția la îndeplinirea obiectivului general de a consolida competențele de securitate cibernetică și capacitățile forței de muncă.

(3) Pe baza rapoartelor menționate la alineatul (1), Comisia prezintă Parlamentului și Consiliului, dacă este cazul, o propunere legislativă de modificare a prezentului regulament.

Articolul 26

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la ...,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

Anexă

Regulamentul (UE) 2021/694 se modifică după cum urmează:

1. În anexa I, secțiunea „Obiectivul specific nr. 3 – Securitatea cibernetică și încrederea” se înlocuiește cu următorul text:

„Obiectivul specific nr. 3 – Securitatea cibernetică și încrederea

Programul stimulează consolidarea, construirea și achiziționarea de capacități esențiale, menite să garanteze securitatea economiei digitale, a societății și democrației Uniunii prin consolidarea potențialului industrial și a competitivității Uniunii în domeniul securității cibernetice, precum și prin îmbunătățirea capacității sectoarelor public și privat în scopul protejării cetățenilor și a întreprinderilor împotriva amenințărilor cibernetice, inclusiv prin sprijinirea punerii în aplicare a Directivei (UE) 2016/1148.

Acțiunile inițiale și, acolo unde este cazul, acțiunile subsecvente din cadrul acestui obiectiv includ:

1. Efectuarea de coinvestiții cu statele membre în echipamente, infrastructuri și know-how avansate în materie de securitate cibernetică, care sunt esențiale pentru protejarea infrastructurilor critice și a pieței unice digitale în ansamblu. Astfel de coinvestiții ar putea include investiții în instalații cuantice și resurse de date pentru securitatea cibernetică, conștientizarea situației în spațiul cibernetic, inclusiv la nivelul ***centrelor cibernetice*** naționale și al ***centrelor cibernetice*** transfrontaliere care formează ***sistemul european de alertă în materie de securitate cibernetică***, precum și alte instrumente care urmează să fie puse la dispoziția sectorului public și privat din întreaga Europă.

2. Îmbunătățirea capacităților tehnologice existente și conectarea în rețea a centrelor de competență din statele membre și garantarea faptului că respectivele capacități răspund nevoilor sectorului public și ale industriei, inclusiv prin produse și servicii care consolidează securitatea cibernetică și încrederea în piața unică digitală.

3. Asigurarea implementării la scară largă în toate statele membre a unor soluții de securitate cibernetică și de încredere eficiente și de ultimă generație. O astfel de implementare include consolidarea siguranței și securității produselor, din faza de proiectare până la cea de comercializare.

4. Sprijinul pentru eliminarea lacunelor în materie de competențe în domeniul securității cibernetice, ***ținând cont de echilibrul de gen,*** de exemplu prin alinierea programelor privind competențele în domeniul securității cibernetice, adaptarea acestora la nevoile sectoriale specifice și facilitarea accesului la formare specializată.

5. Promovarea solidarității între statele membre în ceea ce privește pregătirea legată de incidentele de securitate cibernetică semnificative și incidentele de securitate cibernetică de mare amploare și răspunsul la acestea prin implementarea de servicii de securitate cibernetică la nivel transfrontalier, inclusiv sprijinirea asistenței reciproce între autoritățile publice și crearea unei rezerve de furnizori de încredere de servicii de securitate gestionate la nivelul Uniunii.”

2. În anexa II, secțiunea „Obiectivul specific nr. 3 – Securitatea cibernetică și încrederea” se înlocuiește cu următorul text:

„Obiectivul specific nr. 3 – Securitatea cibernetică și încrederea

3.1. Numărul de infrastructuri de securitate cibernetică și/sau de instrumente achiziționate în comun***, inclusiv*** în cadrul ***sistemului european de alertă în materie de securitate cibernetică***

3.2. Numărul de utilizatori și de comunități de utilizatori care obțin acces la instalațiile europene de securitate cibernetică

3.3 Numărul de acțiuni de sprijinire a pregătirii în vederea incidentelor de securitate cibernetică și a răspunsului la acestea în cadrul mecanismului pentru situații de urgență în materie ***de securitate*** cibernetică”

▌_____

Cu privire la acest act legislativ a fost formulată o declarație care se regăsește în … [a se completa de către Oficiul pentru Publicații: JO C XXX, XX.XX.2024, p. XX] și care poate fi accesată la următorul link: [Oficiul pentru Publicații: a se introduce linkul către declarație].

Declarație a Comisiei referitoare la buget cu privire la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor

(Regulamentul privind solidaritatea cibernetică)[*]

(1) Fișa financiară legislativă a Comisiei care însoțește propunerea de regulament privind solidaritatea cibernetică a fost publicată în aprilie 2023. De atunci, cifrele estimate relevante s-au modificat ca urmare a adoptării sau a adoptării preconizate a altor acte legislative.

(2) La 5 martie 2024, colegiuitorii au ajuns la un acord politic preliminar care prevede limitarea la 22 de milioane EUR a realocării de la obiectivul specific nr. 4 – Competențele digitale avansate – către obiectivul specific nr. 3 – Securitatea cibernetică și încrederea – al programului „Europa digitală” prevăzut în fișa financiară legislativă.

(3) Pentru a reflecta termenii acordului politic preliminar, Comisia a actualizat fișa financiară legislativă a Regulamentului privind solidaritatea cibernetică în ceea ce privește pachetele financiare pentru obiectivul specific nr. 2 – Inteligența artificială, obiectivul specific nr. 3 – Securitatea cibernetică și încrederea – și obiectivul specific nr. 4 – Competențele digitale avansate, ținând seama de realocările convenite de colegiuitori.

(4) În consecință, pachetele financiare pentru perioada 2025-2027 prezentate în fișa financiară legislativă actualizată, fără a aduce atingere competențelor Comisiei în contextul procedurii bugetare anuale, sunt următoarele:

– [544 726 000 EUR] pentru obiectivul specific nr. 2 – Inteligența artificială, ținând seama de cei 65 de milioane EUR realocați obiectivului specific nr. 3 – Securitatea cibernetică și încrederea;

[*] Acordul politic provizoriu a concluzionat că prezenta declarație a Comisiei Europene va fi publicată în Jurnalul Oficial, seria C, și că în seria L vor figura o trimitere și un link la aceasta, împreună cu actul legislativ.

– [44 451 000 EUR] pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea – parte gestionată direct de Comisie, inclusiv 26 de milioane EUR realocați de la obiectivele specifice nr. 2 și nr. 4.

– [353 190 613 EUR] pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea – parte gestionată de Centrul european de competențe în materie de securitate cibernetică, inclusiv realocarea a 61 de milioane EUR de la obiectivele specifice nr. 2 și nr. 4.

– [167 162 423 EUR] pentru obiectivul specific nr. 4 – Competențele digitale avansate, luând în considerare realocarea a 22 de milioane EUR pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea.

(5) Rezerva UE pentru securitate cibernetică va fi finanțată din pachetul financiar al obiectivului specific nr. 3 – Securitatea cibernetică și încrederea – parte gestionată direct de Comisie (care, în conformitate cu fișa financiară legislativă actualizată, este estimată la [44 451 000] EUR).