Parlamentul European
2019-2024

Document de ședință

A9-0426/2023

8.12.2023

***I
RAPORT

referitor 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))

Comisia pentru industrie, cercetare și energie

Raportoare: Lina Gálvez Muñoz

Legenda simbolurilor utilizate

*	Procedura de consultare
***	Procedura de aprobare
***I	Procedura legislativă ordinară (prima lectură)
***II	Procedura legislativă ordinară (a doua lectură)
***III	Procedura legislativă ordinară (a treia lectură)

(Procedura indicată se bazează pe temeiul juridic propus în proiectul de act.)

Amendamente la un proiect de act

Amendamentele Parlamentului prezentate pe două coloane

Textul eliminat este evidențiat prin caractere ***cursive aldine*** în coloana din stânga. Textul înlocuit este evidențiat prin caractere ***cursive aldine*** în ambele coloane. Textul nou este evidențiat prin caractere ***cursive aldine*** în coloana din dreapta.

În primul și în al doilea rând din antetul fiecărui amendament se identifică fragmentul vizat din proiectul de act supus examinării. În cazul în care un amendament vizează un act existent care urmează să fie modificat prin proiectul de act, antetul conține două rânduri suplimentare în care se indică actul existent și, respectiv, dispoziția din acesta vizată de modificare.

Amendamentele Parlamentului prezentate sub formă de text consolidat

Părțile de text noi sunt evidențiate prin caractere ***cursive aldine***. Părțile de text eliminate sunt indicate prin simbolul ▌ sau sunt tăiate. Înlocuirile sunt semnalate prin evidențierea cu caractere ***cursive aldine*** a textului nou și prin eliminarea sau tăierea textului înlocuit.
Fac excepție de la regulă și nu se evidențiază modificările de natură strict tehnică efectuate de serviciile competente în vederea elaborării textului final.

CUPRINS

Pagina

PROIECT DE REZOLUȚIE LEGISLATIVĂ A PARLAMENTULUI EUROPEAN

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 Comitetului Economic și Social European din 13 iulie 2023[1],

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

2. aprobă declarația sa anexată la prezenta rezoluție;

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.

[1] JO C 349, 29.9.2023, p. 167.

Amendamentul 1

AMENDAMENTELE PARLAMENTULUI EUROPEAN*

la propunerea Comisiei

2023/0109 (COD)

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 *și de modificare a Regulamentului (UE) 2021/694*

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[2],

având în vedere avizul Comitetului Economic și Social European[3],

având în vedere avizul Comitetului Regiunilor[4],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale***, dar au introdus simultan posibile vulnerabilități,*** în toate sectoarele de activitate economică ***și ale democrației***, întrucât administrațiile publice, întreprinderile și cetățenii sunt astăzi mai interconectați și mai interdependenți decât oricând, între sectoare și dincolo de frontiere.

---

* Amendamente: textul nou sau modificat este marcat cu caractere cursive aldine; textul eliminat este marcat prin simbolul ▌ .

2 JO C […], […], p. […].

3 JO C , , p. .

4 JO C , , p. .

(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt în creștere ***la nivelul Uniunii și la nivel mondial în ceea ce privește metoda și impactul lor***, inclusiv numărul atacurilor asupra lanțului de aprovizionare în scopul spionajului cibernetic, al ransomware-ului sau al perturbării. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative ***economiilor și democrațiilor, precum și*** infrastructurilor critice ***din întreaga Uniune*** necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. Această amenințare depășește agresiunea militară a Rusiei asupra Ucrainei și este susceptibilă să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale ***și*** criminali implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei 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 în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări. ***Prin urmare, este necesară o cooperare strânsă și coordonată între sectorul public, sectorul privat, mediul academic, societatea civilă și mass-media. În plus, răspunsul Uniunii trebuie să fie coordonat cu instituțiile internaționale, precum și cu parteneri internaționali de încredere și care împărtășesc aceeași viziune. Partenerii internaționali de încredere și care împărtășesc aceeași viziune sunt țări care împărtășesc valorile Uniunii, și anume democrația, angajamentul față de drepturile omului, multilateralismul eficace și ordinea bazată pe norme, în conformitate cu cadrele și acordurile de cooperare internațională. Pentru a asigura cooperarea cu parteneri internaționali de încredere și care împărtășesc aceeași viziune, precum și protecția împotriva rivalilor sistemici, entitățile stabilite în țări terțe care nu sunt părți la AAP nu ar trebui să fie autorizate să participe la achiziții în temeiul prezentului regulament.***

(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate 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[5], este necesar să se sporească reziliența cetățenilor, a întreprinderilor***, în special a microîntreprinderilor, a întreprinderilor mici și mijlocii (IMM-uri), inclusiv a întreprinderilor nou-înființate*** și a entităților care operează infrastructuri critice***, inclusiv a autorităților locale și regionale,*** 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 detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească

[5] https://futureu.europa.eu/ro/

capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică.

(3a) Atacurile cibernetice vizează frecvent serviciile și infrastructurile publice locale, regionale sau naționale. Autoritățile locale se numără printre cele mai vulnerabile ținte ale atacurilor cibernetice din cauza lipsei de resurse financiare și umane. Prin urmare, este deosebit de important ca factorii de decizie de la nivel local să înțeleagă că trebuie să sporească reziliența digitală și capacitatea de a reduce impactul atacurilor cibernetice și să valorifice oportunitățile oferite de prezentul regulament.

(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 materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[6], Recomandarea (UE) 2017/1584 a Comisiei[7], Directiva 2013/40/UE a Parlamentului European și a Consiliului[8] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[9]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat 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) 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 cibernetice 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 și incidentelor de securitate cibernetică, o mai bună pregătire pentru acestea***,*** un răspuns mai bun la astfel de situații ***și o mai bună redresare în urma lor***. De asemenea, statele membre au invitat Comisia să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică în Concluziile Consiliului privind o poziție cibernetică a UE[10].

---

6 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).

7 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).

8 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*).

9 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).

10 Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene aprobate de Consiliu în cadrul reuniunii sale din 23 mai 2022 (9364/22).

(6) Comunicarea comună privind politica UE în domeniul apărării cibernetice[11], adoptată la 10 noiembrie 2022, a anunțat o inițiativă a UE privind solidaritatea cibernetică cu următoarele obiective: consolidarea capabilităților comune de detectare, de conștientizare a situației și de răspuns la nivelul UE prin promovarea implementării unei ***rețele*** a UE de centre de operațiuni de securitate („SOC”), sprijinirea creării treptate a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și testarea entităților 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 și incidentele de securitate cibernetică în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capabilităților statelor membre și ale Uniunii ***de a preveni*** incidentele de securitate cibernetică semnificative și de mare amploare ***și de a răspunde la acestea***. Prin urmare, ar trebui implementată o ***rețea*** paneuropeană de SOC (Scutul cibernetic european) pentru a crea și a consolida capabilitățile comune de detectare și de conștientizare a situației***, întărind totodată capabilitățile Uniunii de detectare a amenințărilor și de schimb de informații***; ar trebui instituit un mecanism pentru situații de urgență ***în materie de securitate*** cibernetică pentru a sprijini statele membre să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare, să răspundă la acestea și să se redreseze imediat în urma lor; ar trebui instituit un mecanism de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. Aceste acțiuni nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene („TFUE”).

(8) Pentru a atinge aceste obiective, este necesar, de asemenea, să se modifice Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului[12] 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 Scutul cibernetic european și de Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică în cadrul obiectivului specific nr. 3 din 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 transfrontaliere în materie de securitate cibernetică. În completare ar trebui să se stabilească condițiile specifice în care poate fi acordat sprijin financiar pentru acțiunile respective și să se definească mecanismele de guvernanță și de coordonare necesare pentru atingerea obiectivelor avute în vedere. 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 acestor noi obiective operaționale.

(9) 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 aceste acțiuni consacrate în cadrul obiectivului specific nr. 3 al DEP. În programele de

---

[11] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.

[12] 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).

lucru relevante se vor prevedea condiții specifice de participare pentru fiecare acțiune, în conformitate cu dispoziția aplicabilă din Regulamentul (UE) 2021/694.

(9a) Având în vedere evoluțiile geopolitice și peisajul amenințărilor cibernetice în creștere și pentru a asigura continuitatea și dezvoltarea în continuare a măsurilor prevăzute în prezentul regulament după 2027, în special Scutul cibernetic european și Mecanismul pentru situații de urgență în materie de securitate cibernetică, este necesar să se asigure o linie bugetară specifică în cadrul financiar multianual pentru perioada 2028-2034. Statele membre ar trebui să urmărească să se angajeze să sprijine toate măsurile necesare pentru a reduce amenințările și incidentele cibernetice în întreaga Uniune și pentru a consolida solidaritatea.

(10) 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) 2018/1046 al Parlamentului European și al Consiliului***[13] 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[14].

(11) În scopul bunei gestiuni financiare, ar trebui stabilite norme specifice pentru reportarea creditelor de angajament și de plată neutilizate. Respectând principiul potrivit căruia bugetul Uniunii este stabilit anual, prezentul regulament ar trebui să prevadă, având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice, posibilități de reportare a fondurilor neutilizate dincolo de cele prevăzute în Regulamentul ***(UE, Euratom) 2018/1046***, maximizând astfel capacitatea Mecanismului pentru situații de urgență ***în materie de securitate*** cibernetică de a sprijini statele membre în combaterea eficace a amenințărilor cibernetice.

(11a) Mecanismul pentru situații de urgență în materie de securitate cibernetică și rezerva UE pentru securitate cibernetică instituite prin prezentul regulament sunt inițiative noi și nu au fost avute în vedere la instituirea cadrului financiar multianual pentru perioada 2021-2027, iar finanțarea pentru aceste inițiative este menită să limiteze pe cât posibil reducerea finanțării pentru alte priorități ale programului „Europa digitală”. Prin urmare, resursele financiare dedicate rezervei UE pentru securitate cibernetică ar trebui să fie reduse și să provină în principal din marjele nealocate în limita plafoanelor cadrului financiar multianual sau să fie mobilizate prin intermediul instrumentelor speciale nematice ale cadrului financiar multianual.

---

13 ***Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012 (JO UE L 193, 30.7.2018, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=ro).***

14 ***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 433I, 22.12.2020, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2020/2092/oj?locale=ro).***

Orice alocare sau realocare a fondurilor din programele existente ar trebui menținută la minimul absolut, pentru a proteja programele existente, în special Erasmus+, de impactul negativ și pentru a se asigura că programele respective își pot atinge obiectivele stabilite.

(12) Pentru a preveni, a evalua***,*** a răspunde într-un mod mai eficace amenințărilor și incidentelor de securitate cibernetică***, precum și pentru a se redresa în urma acestora***, 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 a identificării, atenuării și prevenirii amenințărilor cibernetice potențiale include o capacitate sporită de capabilități avansate de detectare necesare pentru a opri amenințările persistente avansate. Informațiile privind amenințările sunt informații colectate, analizate și interpretate pentru a înțelege amenințările și riscurile potențiale. Prin analizarea și corelarea unor volume mari de date, ele indică modele, tendințe și indicatori de compromis care pot dezvălui activități răuvoitoare sau vulnerabilități.*** Ar trebui implementată o ***rețea*** de SOC („Scutul cibernetic european”), care să cuprindă mai multe platforme transfrontaliere interoperaționale, fiecare grupând mai multe SOC 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 și analiză a datelor, consolidând capabilitățile de detectare și gestionare a incidentelor cibernetice și asigurând conștientizarea în timp real a situației. ***Un SOC național se referă la o capacitate centralizată responsabilă pentru colectarea continuă a informațiilor privind amenințările și pentru îmbunătățirea poziției în materie de securitate cibernetică a entităților aflate sub jurisdicție națională prin prevenirea, detectarea și analizarea amenințărilor la adresa securității cibernetice.*** Infrastructura respectivă ar trebui să contribuie la creșterea gradului de detectare a amenințărilor și incidentelor de securitate cibernetică și, prin urmare, să completeze și să sprijine entitățile și rețelele Uniunii responsabile de gestionarea crizelor în Uniune, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe”), astfel cum este definită în Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[15].

(13) ***Pentru a participa la Scutul cibernetic,*** fiecare stat membru ar trebui să desemneze un organism public la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. ***Statele membre sunt încurajate să integreze capacitatea SOC națională în structura și guvernanța lor cibernetică existente, pentru a evita crearea unor niveluri suplimentare de guvernanță și pentru a alinia prezentul regulament la actul legislativ existent, inclusiv la Directiva (UE) 2022/2555.*** Aceste SOC naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea ***entităților private și publice, în special a SOC naționale ale acestora,*** la Scutul cibernetic european 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. ***SOC***

---

[15] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

naționale ar trebui să consolideze cooperarea și schimbul de informații între entitățile publice și private pentru a remedia comunicarea fragmentată existentă în prezent. În acest sens, ele pot sprijini crearea de modele de schimb de date și ar trebui să faciliteze și să încurajeze schimbul de informații într-un mediu de încredere și sigur. Cooperarea strânsă și coordonată între entitățile publice și private este esențială pentru consolidarea rezilienței Uniunii în domeniul securității cibernetice.

(14) În cadrul Scutului cibernetic european ar trebui înființate o serie de centre de operațiuni transfrontaliere în materie de securitate cibernetică („SOC transfrontaliere”). Acestea ar trebui să reunească SOC naționale din cel puțin trei state membre, astfel încât beneficiile detectării amenințărilor transfrontaliere și ale schimbului și gestionării informațiilor să poată fi realizate pe deplin. Obiectivul general al SOC transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor la adresa securității cibernetice și sprijinirea producerii de informații de înaltă calitate***, inclusiv colectarea și schimbul de date și informații privind posibile acte de piraterie informatică rău intenționate, amenințări și programe de tip „exploit” rău intenționate recent dezvoltate care nu au fost încă implicate în incidente cibernetice, precum și eforturi de analiză,*** privind amenințările cibernetice, în special prin schimbul de date 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 capabilităților de detectare, analiză și prevenire într-un mediu de încredere ***și sigur cu sprijinul ENISA, în chestiuni legate de cooperarea operațională dintre statele membre***. ***SOC transfrontaliere ar trebui să faciliteze și să încurajeze schimbul de informații într-un mediu sigur și de încredere și*** ar trebui să ofere noi capacități suplimentare, pe baza și în completarea SOC-urilor existente și a echipelor de intervenție în caz de incidente de securitate informatică („CSIRT”) și a altor actori relevanți.

(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă ***capacitate*** care să fie ***încorporată în infrastructura de securitate cibernetică existentă, în special în rețeaua*** CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, ***în special SOC ale acestora,*** sporind valoarea datelor respective prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind ***la suveranitatea tehnologică a Uniunii, la autonomia sa strategică deschisă, la competitivitatea și reziliența sa și la dezvoltarea unui ecosistem semnificativ de securitate cibernetică, inclusiv în cooperare cu parteneri internaționali de încredere și care împărtășesc aceeași viziune***. .

(16) SOC-urile transfrontaliere ar trebui să acționeze ca un punct central care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind amenințările cibernetice, să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de actori [de exemplu, echipe de intervenție în caz de urgență informatică („CERT”), CSIRT, centre de schimb de informații și de analiză („ISAC”), operatori de infrastructuri critice]***, pentru a remedia mai ușor comunicarea fragmentată existentă în prezent***. ***În acest sens, SOC transfrontaliere ar putea sprijini, de asemenea, crearea unor modele de schimb de date în întreaga Uniune.*** Informațiile schimbate între participanții la un SOC transfrontalier ar putea include date provenite de la rețele și

senzori, fluxuri de informații privind amenințările cibernetice, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări și vulnerabilități***, inclusiv colectarea și schimbul de date și informații privind posibile acte de piraterie informatică rău intenționate, amenințări și programe de tip „exploit” rău intenționate recent dezvoltate care nu au fost încă implicate în incidente cibernetice, precum și eforturi de analiză***. În plus, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere.

(17) 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 de mare amploare. Directiva (UE) 2022/2555 instituie 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 și agențiile Uniunii. Recomandarea (UE) 2017/1584 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare abordează rolul tuturor actorilor relevanți. Directiva (UE) 2022/2555 reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii („UCPM”) instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului[16], precum și de a furniza rapoarte analitice pentru mecanismul integrat pentru un răspuns politic la crize („IPCR”) în temeiul Deciziei de punere în aplicare (UE) 2018/1993 ***a Consiliului***[17]. Prin urmare, în situațiile în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea ar trebui să furnizeze informații relevante către EU-CyCLONe, rețelei CSIRT și Comisiei***, în conformitate cu Directiva (UE) 2022/2555***. 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 în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.

(18) Entitățile care participă la Scutul cibernetic european ar trebui să asigure un nivel ridicat de interoperabilitate între ele, inclusiv, după caz, în ceea ce privește formatele de date, taxonomia, instrumentele de manipulare și analiză a datelor și canalele de comunicații securizate, un nivel minim de securitate a nivelului de aplicație, tabloul de bord al conștientizării situației și indicatori. Adoptarea unei taxonomii comune și elaborarea unui model pentru rapoartele situaționale în vederea descrierii cauzei tehnice și a impactului incidentelor de securitate cibernetică ar trebui să țină seama de lucrările în

---

16 ***Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (Text cu relevanță pentru SEE) (***JO L 347, 20.12.2013, p. 924, ***ELI:*** https://eur-lex.europa.eu/eli/dec/2013/1313/oj?locale=ro***).***

17 ***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: https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj?locale=ro).***

curs privind notificarea incidentelor în contextul punerii în aplicare a Directivei (UE) 2022/2555.

(19) Pentru a permite schimbul de date privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere ***și sigur***, entitățile care participă la Scutul cibernetic european ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate ***și dotate cu 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.

(20) Prin colectarea, partajarea și schimbul de date, Scutul cibernetic european ar trebui să consolideze suveranitatea tehnologică a Uniunii, ***autonomia sa strategică deschisă, competitivitatea și reziliența sa, precum și un ecosistem semnificativ al UE în materie de securitate cibernetică***. Punerea în comun a datelor actualizate de înaltă calitate ar trebui să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. ***Inteligența artificială este cea mai eficientă atunci când este asociată cu analiza umană. Prin urmare, o forță de muncă calificată rămâne esențială pentru punerea în comun a datelor de înaltă calitate.*** Aceasta ar trebui facilitată prin conectarea Scutului cibernetic european cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173 al Consiliului[18].

(21) Deși Scutul cibernetic european este un proiect civil, comunitatea de apărare cibernetică ar putea beneficia de capabilități civile mai puternice de detectare și de conștientizare a situației dezvoltate pentru protecția infrastructurii critice. SOC transfrontaliere, cu sprijinul Comisiei și al Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) și în cooperare cu Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate („Înaltul Reprezentant”), ar trebui să elaboreze treptat protocoale și standarde specifice ***în materie de condiții de acces și de garanții*** pentru a permite cooperarea cu comunitatea de apărare cibernetică, inclusiv privind investigațiile și condițiile de securitate***, respectând caracterul civil al instituțiilor și destinația finanțării și folosind, prin urmare, fondurile disponibile pentru comunitatea de apărare***. Dezvoltarea Scutului cibernetic european ar trebui să fie însoțită de o reflecție care să permită colaborarea viitoare cu rețelele și platformele responsabile cu schimbul de informații în cadrul comunității de apărare cibernetică, în strânsă cooperare cu Înaltul Reprezentant ***și respectând pe deplin drepturile și libertățile***.

(22) Schimbul de informații între participanții la Scutul cibernetic european ar trebui să respecte cerințele juridice existente și, în special, legislația Uniunii și legislația națională 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

[18] Regulamentul (UE) 2021/1173 al Consiliului din 13 iulie 2021 privind instituirea întreprinderii comune pentru calculul european de înaltă performanță și de abrogare a Regulamentului (UE) 2018/1488 (JO L 256, 19.7.2021, p. 3, ***ELI: https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=ro***).

să distrugă datele de îndată ce acestea nu mai sunt necesare pentru scopul declarat și să informeze organismul care pune la dispoziție datele că datele au fost distruse.

(23) Fără a aduce atingere articolului 346 din TFUE, schimbul de informații care sunt confidențiale în temeiul ***dreptului*** Uniunii sau al ***dreptului național*** ar trebui să se limiteze la ceea ce este relevant și proporțional cu scopul respectivului schimb. Schimbul de astfel de informații ar trebui să păstreze confidențialitatea informațiilor și să protejeze securitatea și interesele comerciale ale entităților în cauză, cu respectarea deplină a secretelor comerciale și de afaceri.

(24) Având în vedere riscurile tot mai mari și numărul tot mai mare de incidente cibernetice care afectează statele membre, este necesar să se instituie un instrument de sprijin în caz de criză pentru a îmbunătăți reziliența Uniunii la incidentele de securitate cibernetică semnificative și de mare amploare și pentru a completa acțiunile statelor membre prin sprijin financiar de urgență pentru pregătirea, răspunsul și redresarea imediată a serviciilor esențiale. Instrumentul respectiv 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, pregătirea și răspunsul în caz de incidente și crize cibernetice 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”).

(25) 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 de mare amploare și al redresării imediate în urma acestora, cum ar fi serviciile furnizate de Agenția Uniunii Europene pentru Securitate Cibernetică („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 PESCO[19] și echipele de răspuns rapid în caz de amenințări hibride. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea incidentelor de securitate cibernetică în întreaga Uniune și în țările terțe și răspunsul la acestea.

(26) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[20], IPCR[21], și Directivei (UE) 2022/2555. Acesta poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE sau în situațiile definite la articolul 222 din TFUE sau poate

---

[19] 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.

[20] 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).

[21] Mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

completa aceste acțiuni. Utilizarea instrumentului respectiv ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, după caz.

(27) 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*** și statul membru afectat. Atunci când solicită sprijin în cadrul Mecanismului pentru situații de urgență ***în materie de securitate*** cibernetică, statul membru ar trebui să furnizeze informații relevante care să justifice necesitatea sprijinului.

(28) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să înființeze 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 înființa una sau mai multe 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 de mare amploare, pentru a sprijini redresarea imediată și/sau pentru a restabili funcționarea serviciilor esențiale.

(29) 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 deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. Sectoarele sau subsectoarele ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de testare coordonată 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, care urmează să fie efectuate de Comisie, de 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 (OAREC), de evaluările coordonate ale riscurilor 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) 2022/2554 al Parlamentului European și al Consiliului[22]. 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.

(30) În plus, Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să ofere sprijin pentru alte acțiuni de pregătire și să sprijine pregătirea în alte sectoare, care nu sunt acoperite de testarea coordonată a entităților care își desfășoară activitatea în sectoare deosebit de critice. Aceste acțiuni ar putea include diferite tipuri de activități de pregătire la nivel național.

(31) 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 și de mare amploare, să sprijine redresarea imediată 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 cibernetice asupra cetățenilor.

(32) Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică ar trebui să sprijine asistența acordată de statele membre, inclusiv de rețeaua CSIRT prevăzută la articolul 15 din Directiva (UE) 2022/2555, unui stat membru afectat de un incident de securitate cibernetică semnificativ sau de mare amploare. Statele membre care acordă 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.

(33) Ar trebui instituită treptat o rezervă de securitate cibernetică la nivelul Uniunii, care să constea în servicii furnizate de furnizori privați de servicii de securitate gestionate pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor***, consolidând în același timp reziliența Uniunii, inclusiv participarea furnizorilor europeni de servicii de securitate gestionate care sunt IMM-uri și asigurând crearea unui ecosistem de securitate cibernetică, format în special din microîntreprinderi, IMM-uri, inclusiv întreprinderi nou-înființate, cu investiții în cercetare și inovare (C&I) pentru a dezvolta tehnologii de ultimă generație, cum ar fi cele legate de cloud și inteligența artificială***. ***Furnizorii de încredere, inclusiv IMM-urile, ar trebui să poată coopera între ei pentru a îndeplini criteriile de mai sus.*** 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 critice sau deosebit de critice, în completarea propriilor acțiuni la

[22] 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.

nivel național. ***Prin urmare, rezerva pentru securitate cibernetică ar trebui să încurajeze investițiile în cercetare și inovare pentru a stimula dezvoltarea acestor tehnologii. După caz, s-ar putea desfășura exerciții comune cu furnizorii de încredere și cu potențialii utilizatori ai rezervei pentru securitate cibernetică pentru a asigura funcționarea eficientă a rezervei atunci când este necesar.*** Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, statele membre ar trebui să specifice sprijinul acordat entității afectate la nivel național, care ar trebui luat în considerare atunci când se evaluează cererea statului membru. Serviciile din rezerva UE pentru securitate cibernetică pot servi, de asemenea, la sprijinirea instituțiilor, a organelor***, a oficiilor*** și a agențiilor Uniunii, în condiții similare. ***Comisia ar trebui să asigure implicarea statelor membre și schimburi ample cu acestea, cu scopul de a evita suprapunerea cu inițiative similare, inclusiv în cadrul Organizației Tratatului Atlanticului de Nord (NATO).***

(34) 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 care ar trebui incluse în cererea de oferte pentru selectarea acestor furnizori, astfel încât să se asigure că sunt îndeplinite nevoile autorităților și entităților din statele membre care își desfășoară activitatea în sectoare critice sau deosebit de critice. ***Ar trebui încurajată participarea furnizorilor mai mici, activi la nivel regional și local.***

(35) Pentru a sprijini instituirea rezervei UE pentru securitate cibernetică, Comisia ar trebui să solicite ENISA să pregătească o propunere de sistem de certificare în temeiul Regulamentului (UE) 2019/881 pentru serviciile de securitate gestionate în domeniile acoperite de Mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică. ***Pentru a îndeplini sarcinile suplimentare care decurg din această dispoziție, ENISA ar trebui să primească finanțare suplimentară adecvată.***

(36) 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 de mare amploare, EU-CyCLONe, rețeaua CSIRT sau Comisia ar trebui să poată solicita ENISA să revizuiască și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de examinare a incidentelor, în colaborare cu părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ai statelor membre, ai Comisiei și ai altor instituții, organisme***, oficii*** și agenții relevante ale UE. În ceea ce privește sectorul privat, ENISA dezvoltă canale pentru schimbul de informații cu furnizorii specializați, inclusiv cu furnizorii de soluții de securitate gestionate și cu vânzătorii, pentru a contribui la misiunea ENISA de a atinge un nivel comun ridicat de securitate cibernetică în întreaga Uniune. Pe baza colaborării cu părțile interesate, inclusiv cu sectorul privat, raportul de examinare 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 rețelelor EU-CyCLONe și CSIRT și Comisiei și să contribuie la activitatea acestora. În cazul în care incidentul se referă la o țară terță, acesta va fi, de asemenea, transmis de către Comisie Înaltului Reprezentant.

(37) Având în vedere caracterul imprevizibil al atacurilor de securitate cibernetică 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 de mare amploare contribuie la protecția Uniunii în ansamblu. Prin urmare, țările terțe asociate la DEP pot fi sprijinite din rezerva UE pentru securitate cibernetică, în cazul în care acest lucru este prevăzut în acordul de asociere la DEP respectiv. Finanțarea pentru țările terțe asociate 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 de mare amploare și al redresării imediate în urma acestora. Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP.

(37a) Țările terțe ar putea avea acces la resurse și la sprijin în temeiul prezentului regulament, utilizând sprijinul pentru răspunsul la incidente din rezerva UE pentru securitate cibernetică. În plus, furnizorii de servicii de răspuns la incidente din țări terțe, inclusiv țări terțe asociate la programul „Europa digitală" sau alte țări partenere internaționale, precum și state membre ale NATO, pot fi necesari pentru furnizarea de servicii specifice în rezerva UE pentru securitate cibernetică. Prin derogare de la Regulamentul (UE, Euratom) 2018/1046, pentru a consolida suveranitatea tehnologică a Uniunii, autonomia strategică deschisă, competitivitatea și reziliența acesteia și pentru a proteja activele strategice, interesele sau securitatea Uniunii, entitățile stabilite în țări terțe care nu sunt parte la AAP și care nu au făcut obiectul unei examinări în sensul Regulamentului (UE) 2019/452 al Parlamentului European și al Consiliului[23] și, dacă este necesar, al unor măsuri de atenuare, ținând seama de obiectivele stabilite în prezentul regulament, nu ar trebui să fie autorizate să participe. Dimensiunea externă a prezentului regulament ar trebui să respecte dispozițiile stabilite în Acordul de asociere în cadrul programului „Europa digitală". Participarea țărilor terțe ar trebui să fie supusă controlului public, cu participarea competențelor legislative, pentru a garanta participarea cetățenilor la acest proces.

(38) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui conferite competențe de executare Comisiei pentru: a prevedea condițiile de interoperabilitate între SOC transfrontaliere; a stabili modalitățile procedurale pentru schimbul de informații cu privire la un incident de securitate cibernetică de mare amploare potențial sau în curs între SOC-urile transfrontaliere și entitățile Uniunii; a stabili cerințele tehnice pentru asigurarea securității Scutului cibernetic european; a specifica tipurile și numărul de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică; și pentru a specifica modalitățile detaliate de alocare a serviciilor de sprijin din rezerva UE pentru securitate cibernetică.

---

[23] Regulamentul (UE) 2019/452 al Parlamentului European și al Consiliului din 19 martie 2019 de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniune (JO L 79I, 21.3.2019, p. 1), ELI: https://eur-lex.europa.eu/eli/reg/2019/452/oj?locale=ro.

Respectivele competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului*.

---

* ***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: https://eur-lex.europa.eu/eli/reg/2011/182/oj?locale=ro).***

(38a) Pentru punerea în aplicare eficace a Scutului cibernetic european și a Mecanismului pentru situații de urgență în materie de securitate cibernetică, este absolut necesar personal calificat, care este capabil să furnizeze în mod fiabil serviciile relevante de securitate cibernetică la cele mai înalte standarde. Prin urmare, este îngrijorător faptul că Uniunea se confruntă cu un deficit de talente, caracterizat de un deficit de profesioniști calificați, și că se confruntă totodată cu un peisaj al amenințărilor care evoluează rapid, astfel cum se recunoaște în comunicarea Comisiei din 18 aprilie 2023 privind Academia de competențe în domeniul cibernetic. Este important să se reducă acest deficit de talente prin consolidarea cooperării și a coordonării între diferitele părți interesate, inclusiv între sectorul privat, mediul academic, statele membre, Comisia și ENISA, pentru a extinde și a crea sinergii, în toate regiunile, pentru investițiile în educație și formare, dezvoltarea de parteneriate public-privat, sprijinirea inițiativelor de cercetare și inovare, dezvoltarea și recunoașterea reciprocă a standardelor comune și certificarea competențelor în materie de securitate cibernetică, inclusiv prin intermediul Cadrului european pentru competențe în materie de securitate cibernetică. Acest lucru ar trebui, de asemenea, să faciliteze mobilitatea profesioniștilor în materie de securitate cibernetică în cadrul Uniunii. Prezentul regulament ar trebui să vizeze promovarea unei forțe de muncă mai diversificate în materie de securitate cibernetică. Toate măsurile care vizează îmbunătățirea competențelor în materie de securitate cibernetică necesită garanții pentru a evita un „exod al creierelor” și un risc pentru mobilitatea forței de muncă.

(38b) Se impune consolidarea aptitudinilor și competențelor specializate, interdisciplinare și generale în întreaga Uniune, cu un accent special pe femei, deoarece disparitatea de gen persistă în domeniul securității cibernetice, femeile reprezentând 20 % din media persoanelor active în domeniu la nivel mondial. Femeile trebuie să fie prezente și să facă parte din conceperea viitorului digital și a guvernanței acestuia.

(38c) Consolidarea cercetării și inovării (C&I) în domeniul securității cibernetice este menită să sporească reziliența și autonomia strategică deschisă a Uniunii. În mod similar, este important să se creeze sinergii cu programele de C&I și cu instrumentele și instituțiile existente și să se consolideze cooperarea și coordonarea între diferitele părți interesate, inclusiv sectorul privat, societatea civilă, mediul academic, statele membre, Comisia și ENISA;

(38d) Prezentul regulament ar trebui să contribuie la angajamentul asumat în Declarația europeană privind drepturile și principiile digitale pentru deceniul digital, legat de protejarea intereselor democrațiilor noastre, ale cetățenilor, ale întreprinderilor și ale instituțiilor publice împotriva riscurilor de securitate cibernetică și a criminalității informatice, inclusiv împotriva încălcării securității datelor și a furtului sau manipulării identității. Aplicarea prezentului regulament ar trebui, de asemenea, să

contribuie la îmbunătățirea punerii în aplicare a altor acte legislative, de exemplu în ceea ce privește inteligența artificială, confidențialitatea datelor și reglementarea datelor în ceea ce privește securitatea cibernetică și reziliența cibernetică.

(38e) Dezvoltarea ca bun public a culturii securității cibernetice care înglobează securitatea, inclusiv cea a mediului digital, va fi esențială pentru punerea în aplicare cu succes a prezentului regulament. Prin urmare, elaborarea de măsuri pentru a include și a îmbunătăți informarea cetățenilor ar trebui să fie un alt mijloc de garantare a protejării democrațiilor noastre și a valorilor noastre fundamentale.

(38f) 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 pentru a specifica condițiile de interoperabilitate dintre SOC transfrontaliere, pentru a stabili modalitățile procedurale pentru schimbul de informații între SOC transfrontaliere, pe de o parte, și EU-CyCLONe, rețeaua CSIRT și Comisie, pe de altă parte, pentru a specifica tipurile și numărul de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică și pentru a preciza suplimentar modalitățile detaliate de alocare a serviciilor de sprijin din 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*. 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.

****JO L 123, 12.5.2016, p. 1, ELI: https://eur-lex.europa.eu/eli/agree_interinstit/2016/512/oj?locale=ro.***

(39) ***Obiectivele*** prezentului regulament, ***și anume consolidarea capacităților Uniunii de prevenire, detectare, răspuns și redresare în legătură cu amenințările cibernetice, precum și instituirea unui cadru general care să remedieze comunicarea fragmentată, nu pot fi realizate suficient de către statele membre, ci pot*** fi ***realizate*** mai bine la nivelul Uniunii ▌. În consecință, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității și cu principiul proporționalității, astfel cum sunt prevăzute 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 obiectivului respectiv,

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I

OBIECTIVE GENERALE, OBIECT ȘI DEFINIȚII

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 contracararea lor, în special prin următoarele acțiuni:

(a) implementarea unei ***rețele*** paneuropene de centre de operațiuni de securitate („Scutul cibernetic european”) pentru a construi și a consolida capabilitățile comune de detectare și de conștientizare a situației;

(b) crearea unui mecanism pentru situații de urgență cibernetică pentru a sprijini statele membre să se pregătească pentru incidentele de securitate cibernetică semnificative și de mare amploare, să răspundă la acestea și să se redreseze imediat în urma lor;

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

(2) Prezentul regulament urmărește obiectivul de consolidare a solidarității la nivelul Uniunii prin următoarele obiective specifice:

(a) de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel ***sprijinirea capacității industriale a Uniunii și a statelor membre în sectorul securității cibernetice și de a consolida poziția competitivă*** a industriei***, în special a microîntreprinderilor, a IMM-urilor, inclusiv a întreprinderilor nou-înființate,*** și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la suveranitatea tehnologică a Uniunii, ***autonomia strategică deschisă, competitivitatea și reziliența sa în acest sector, consolidând ecosistemul securității cibernetice cu scopul de a asigura capacități puternice ale Uniunii, inclusiv în cooperare cu parteneri internaționali;***

(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea 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 prin analizarea și evaluarea incidentelor semnificative sau de mare amploare, inclusiv prin valorificarea lecțiilor învățate și, după caz, prin recomandări.

(ca) de a dezvolta, în mod coordonat, aptitudini, abilități de know-how și competențe ale forței de muncă pentru a asigura securitatea cibernetică și a crea sinergii cu Academia de competențe în materie de securitate cibernetică.

(3) Prezentul regulament nu aduce atingere responsabilității principale a statelor membre în ceea ce privește securitatea națională, siguranța publică și prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

-1a. „Centru național de operațiuni de securitate" sau „SOC național" înseamnă o capacitate națională centralizată care colectează și analizează încontinuu informații privind amenințările cibernetice și îmbunătățește poziția de securitate cibernetică în conformitate cu articolul 4;

1. „Centru transfrontalier de operațiuni de securitate" ***sau*** „SOC transfrontalier" înseamnă o platformă multinațională care reunește într-o structură coordonată de rețea SOC-uri naționale ***în conformitate cu articolul 5;***

2. „organism public" înseamnă ***organisme*** de drept public astfel cum ***sunt definite*** la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European și a Consiliului[24];

3. „consorțiu-gazdă" înseamnă un consorțiu alcătuit din state participante, reprezentate de SOC-urile naționale***, în conformitate cu articolul 5***;

4. „entitate" înseamnă o entitate astfel cum este definită la articolul 6 punctul 38 din Directiva (UE) 2022/2555;

4a. «entitate critică» înseamnă entitate critică astfel cum este definită la articolul 2 punctul 1 din Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului[25];

5. „entități care își desfășoară activitatea în sectoare critice sau deosebit de critice" înseamnă ▌ entități ***din sectoarele*** enumerate în anexele I și II la Directiva (UE) 2022/2555;

---

[24] 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 94, 28.3.2014, p. 65).

[25] Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164, ELI: https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=ro).

5a. „administrarea incidentelor” înseamnă o administrare a incidentelor astfel cum este definită la articolul 6 punctul 8 din Directiva (UE) 2022/2555;

5b. „risc” înseamnă un risc astfel cum este definit la articolul 6 punctul 9 din Directiva (UE) 2022/2555;

6. „amenințare cibernetică” înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

6a. „amenințare cibernetică semnificativă” înseamnă o amenințare cibernetică semnificativă astfel cum este definită la articolul 6 punctul 11 din Directiva (UE) 2022/2555;

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

8. „incident de securitate cibernetică de mare amploare” înseamnă un incident astfel cum este definit la articolul 6 punctul 7 din Directiva (UE) 2022/2555;

9. „pregătire” înseamnă o stare de promptitudine și o capabilitate, obținute ca urmare a unor acțiuni prealabile de evaluare și monitorizare a riscurilor, de a asigura un răspuns rapid și eficace la incidente de securitate semnificative sau de mare amploare;

10. „răspuns” înseamnă o acțiune întreprinsă în cazul unui incident de securitate cibernetică semnificativ sau de mare amploare sau în timpul sau după un astfel de incident, pentru a aborda consecințele negative imediate și pe termen scurt ale acestuia;

10a. „furnizor de servicii de securitate gestionate” înseamnă un furnizor de servicii de securitate gestionate astfel cum este definit la articolul 6 punctul 40 din Directiva (UE) 2022/2555;

11. „furnizori de ***servicii de securitate gestionate de*** încredere” înseamnă furnizori de servicii de securitate gestionate ▌ selectați ***pentru a fi incluși în rezerva UE pentru securitate cibernetică*** în conformitate cu articolul 16 din prezentul regulament.

Capitolul II

SCUTUL CIBERNETIC EUROPEAN

Articolul 3

Instituirea Scutului cibernetic european

(1) Se instituie o ***rețea*** de centre de operațiuni de securitate („Scutul cibernetic european”) pentru a dezvolta capabilități avansate pentru ca Uniunea să detecteze, să analizeze și să prelucreze date privind amenințările și ***să prevină*** incidentele de securitate cibernetică din

Uniune. Aceasta este formată din toate centrele naționale de operațiuni de securitate („SOC naționale”) și din centrele transfrontaliere de operațiuni de securitate („SOC transfrontaliere”).

Acțiunile de punere în aplicare a Scutului cibernetic european sunt sprijinite prin finanțare din programul „Europa digitală” și sunt puse în aplicare în conformitate cu Regulamentul (UE) 2021/694, în special cu obiectivul specific nr. 3.

(2) Scutul cibernetic european:

(a) pune în comun și face schimb de date privind amenințările și incidentele de securitate cibernetică din diferite surse, prin intermediul SOC transfrontaliere ***și, dacă este relevant, face schimb de informații cu rețeaua CSIRT***;

(b) furnizează informații de înaltă calitate, operative și informații privind amenințările cibernetice, prin utilizarea unor instrumente de ultimă generație, în special a tehnologiilor de inteligență artificială și de analiză a datelor;

(c) contribuie la o mai bună protecție împotriva amenințărilor cibernetice și la un răspuns mai bun la acestea***, inclusiv prin furnizarea de recomandări concrete entităților***;

(d) contribuie la detectarea mai rapidă a amenințărilor cibernetice și la conștientizarea situației în întreaga Uniune;

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

Acesta este dezvoltat în cooperare cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173.

Articolul 4

Centrele naționale de operațiuni de securitate

(1) Pentru ***a putea*** participa la Scutul cibernetic european, fiecare stat membru desemnează cel puțin un SOC național. SOC național este ***o capacitate centralizată într-un*** organism public. ***Atunci când este posibil, SOC naționale sunt integrate în CSIRT sau în alte infrastructuri sau structuri de guvernanță existente în domeniul securității cibernetice.***

Acesta are capacitatea de a acționa ca punct de referință și punct de acces către alte organizații publice și private de la nivel național***, în special SOC-urile lor naționale,*** pentru colectarea și analizarea informațiilor privind amenințările și incidentele de securitate cibernetică și***, dacă este relevant, partajarea acestor informații cu membrii rețelei CSIRT din statul membru respectiv, precum și*** pentru contribuția la un SOC transfrontalier. Acesta este echipat cu

tehnologii de ultimă generație capabile ***să prevină,*** să detecteze, să reunească și să analizeze datele relevante pentru amenințările și incidentele de securitate cibernetică.

Un SOC național sau CSIRT poate solicita date obținute prin telemetrie, senzori sau evidențe despre entitățile lor critice naționale de la furnizorii de servicii de securitate gestionate care furnizează un serviciu entității critice. Datele sunt partajate în conformitate cu dreptul Uniunii în materie de protecție a datelor și cu unicul scop de a sprijini SOC naționale sau CSIRT în detectarea și prevenirea amenințărilor și incidentelor de securitate cibernetică.

(2) În urma unei cereri de exprimare a interesului, SOC naționale ***pot fi*** selectate de către Centrul european de competențe în materie de securitate cibernetică („ECCC”) pentru a participa la o achiziție de instrumente și infrastructuri în comun cu ECCC. ECCC poate acorda granturi SOC-urilor naționale selectate pentru a finanța funcționarea acestor instrumente și infrastructuri. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de statul membru. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și SOC național încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

(3) Un SOC național selectat în temeiul alineatului (2) se angajează să solicite participarea la un SOC transfrontalier în termen de doi ani de la data achiziționării instrumentelor și infrastructurilor sau de la data la care primește finanțare prin granturi, în funcție de evenimentul care survine mai întâi. În cazul în care nu participă la un SOC transfrontalier până la momentul respectiv, SOC-ul național în cauză nu este eligibil pentru sprijin suplimentar din partea Uniunii în temeiul prezentului regulament.

Articolul 5

Centrele transfrontaliere de operațiuni de securitate

(1) Un consorțiu-gazdă alcătuit din cel puțin trei state membre, reprezentate de SOC naționale, care se angajează să colaboreze pentru a-și coordona activitățile de detectare cibernetică și de monitorizare a amenințărilor este eligibil să participe la acțiuni de instituire a unui SOC transfrontalier. ***Un SOC transfrontalier este conceput să detecteze și să analizeze amenințările la adresa securității cibernetice, să prevină incidentele și să sprijine producerea de informații de înaltă calitate, în special prin schimbul de date din diferite surse, publice și private, precum și prin partajarea instrumentelor de ultimă generație și prin dezvoltarea în comun a capabilităților de detectare, analiză, prevenire și protecție cibernetică într-un mediu securizat și de încredere.***

(2) În urma unei cereri de exprimare a interesului, un consorțiu-gazdă ***poate fi*** selectat de către ECCC pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor și a infrastructurilor. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor

urmând să fie acoperite de către consorțiul-gazdă. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

(2a) Prin derogare de la articolul 176 din Regulamentul (UE, Euratom) 2018/1046, entitățile stabilite în țări terțe care nu sunt părți la AAP nu participă la achizițiile publice comune de instrumente și infrastructuri.

(3) Membrii consorțiului-gazdă încheie un acord de consorțiu scris care stabilește procedurile lor interne pentru punerea în aplicare a acordului de găzduire și de utilizare.

(4) Un SOC transfrontalier este reprezentat din punct de vedere juridic de un SOC național, care acționează în calitate de SOC coordonator, sau de consorțiul-gazdă, dacă acesta are personalitate juridică. SOC-ul coordonator este responsabil de respectarea cerințelor acordului de găzduire și utilizare și ale prezentului regulament.

Articolul 6

Cooperarea și schimbul de informații în cadrul SOC transfrontaliere și între acestea

(1) Membrii unui consorțiu-gazdă fac schimb între ei, în cadrul SOC transfrontalier, de informații relevante, inclusiv 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 un astfel de schimb de informații:

(a) ***îmbunătățește schimbul de informații privind amenințările cibernetice între SOC naționale și transfrontaliere și ISAC din sector, cu scopul de a preveni, detecta sau atenua amenințările;***

(b) sporește nivelul de securitate cibernetică, în special prin sensibilizarea cu privire la amenințările cibernetice, prin limitarea sau împiedicarea posibilității răspândirii unor asemenea amenințări, sprijinirea gamei de capabilități defensive, remedierea și divulgarea vulnerabilităților, detectarea amenințărilor, tehnicile de limitare și prevenire a amenințărilor, strategiile de atenuare sau 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 ***datele semnificative*** menționate la alineatul (1) și condițiile în care urmează să fie partajate informațiile respective;

(b) un cadru de guvernanță care să stimuleze schimbul de informații între toți participanții;

(c) ținte privind contribuția la dezvoltarea unor instrumente avansate de inteligență artificială și de analiză a datelor.

(3) Pentru a încuraja schimbul de informații între SOC-urile transfrontaliere ***și cu ISAC din sector, SOC-urile transfrontaliere*** asigură un nivel ridicat de interoperabilitate între ele ***și, dacă este posibil, cu ISAC din sector***. Pentru a facilita interoperabilitatea dintre SOC-urile transfrontaliere ***și ISAC din sector, standardele și protocoalele pentru schimbul de informații pot fi armonizate cu standardele internaționale și cu cele mai bune practici ale sectorului***. ***Se încurajează, de asemenea, achizițiile publice comune de infrastructuri, servicii și instrumente cibernetice. În plus,*** după consultarea ECCC ***și ENISA, Comisia este împuternicită ca, până la ... [șase luni de la data intrării în vigoare a prezentului regulament] să adopte acte delegate în conformitate cu articolul 20a pentru a completa prezentul regulament, specificând condițiile acestei interoperabilități în strânsă coordonare cu SOC-urile transfrontaliere și pe baza standardelor internaționale și a celor mai bune practici ale sectorului***.

(4) SOC-urile transfrontaliere încheie acorduri de cooperare între ele ***și, după caz, cu ISAC din sector,*** specificând principiile schimbului de informații ***și interoperabilității*** între platformele transfrontaliere***, luând în considerare mecanismele pertinente de schimb de informații deja existente prevăzute în Directiva (UE) 2022/2555***. ***După caz, SOC-urile transfrontaliere încheie acorduri de cooperare cu ISAC din sector. În contextul unui incident de securitate cibernetică de mare amploare potențial sau în curs, mecanismele de schimb de informații respectă dispozițiile pertinente din Directiva (UE) 2022/2555.***

Articolul 7

Cooperarea și schimbul de informații cu *rețeaua CSIRT*

(1) În cazul în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs ***în scopul conștientizării comune a situației, SOC-ul coordonator*** furnizează, fără întârzieri nejustificate, ***informațiile*** relevante ***echipei sale*** CSIRT ***sau autorității competente, care va comunica acest lucru EU-CyCLONe, rețelei CSIRT*** și Comisiei ***și ENISA, în conformitate cu*** rolurile ***și procedurile*** lor respective de gestionare a crizelor în conformitate cu Directiva (UE) 2022/2555. ***Prezentul alineat nu impune nicio obligație suplimentară entităților publice sau private de a comunica un incident de securitate cibernetică de mare amploare, potențial sau în curs, în vederea respectării obligațiilor prevăzute în Directiva (UE) 2022/2555.***

(2) ▌Comisia ***este împuternicită să adopte acte delegate în conformitate cu articolul 20a, după consultarea rețelei CSIRT, pentru completarea prezentului regulament, determinând*** modalitățile procedurale pentru schimbul de informații prevăzut la alineatul (1) ***de la prezentul articol și în conformitate cu Directiva (UE) 2022/2555***.

Articolul 8

Securitate

(1) Statele membre care participă la Scutul cibernetic european asigură un nivel ridicat de ***confidențialitate și*** securitate a datelor și de securitate fizică a infrastructurii Scutului cibernetic european și se asigură că infrastructura 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 schimbate prin intermediul infrastructurii.

(2) Statele membre care participă la Scutul cibernetic european se asigură că schimbul de informații în cadrul Scutului cibernetic european cu entități care nu sunt organisme publice ale statelor membre nu afectează în mod negativ interesele de securitate ale Uniunii.

(3) Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice pentru ca statele membre să își respecte obligațiile care le revin în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament. ***Acestea respectă Directivele (UE) 2022/2555 și (UE) 2022/2557.*** În ***actele sale de punere în aplicare***, Comisia, sprijinită de Înaltul Reprezentant, ține seama de standardele de securitate relevante la nivel de apărare, pentru a facilita cooperarea cu actorii militari.

Capitolul III

MECANISMUL PENTRU SITUAȚII DE URGENȚĂ ÎN MATERIE DE SECURITATE CIBERNETICĂ

Articolul 9

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 îmbunătăți reziliența Uniunii la amenințările semnificative la adresa securității cibernetice și pentru a pregăti Uniunea, în spiritul solidarității, pentru impactul pe termen scurt al incidentelor de securitate cibernetică semnificative și de mare amploare și pentru a atenua acest impact („mecanismul”).

(2) Acțiunile de punere în aplicare a mecanismului ▌ 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.

Articolul 10

Tipul acțiunilor

(1) Mecanismul sprijină următoarele tipuri de acțiuni:

(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice în cadrul Uniunii;

(b) acțiuni de răspuns, care sprijină răspunsul la incidentele de securitate cibernetică semnificative și de mare amploare și redresarea imediată în urma acestora, care urmează să fie furnizate de furnizorii ***de servicii de securitate gestionate*** de încredere care participă la rezerva UE pentru securitate cibernetică instituită în temeiul articolului 12;

(c) acțiuni de asistență reciprocă constând în furnizarea de asistență din partea autorităților naționale ale unui stat membru unui alt stat membru, în special astfel cum se prevede la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555.

(1a) În urma declanșării mecanismului, Comisia analizează și publică în fiecare an un raport cu privire la aspectele pozitive și cele negative ale funcționării mecanismului, precizând inclusiv dacă sunt necesare cerințe suplimentare de cooperare sau de formare.

Articolul 11

Testarea coordonată a pregătirii entităților

(1) În scopul de a sprijini testarea coordonată a pregătirii entităților menționate la articolul 10 alineatul (1) litera (a) în întreaga Uniune, Comisia identifică, după consultarea Grupului de cooperare NIS și a ENISA, sectoarele sau subsectoarele vizate din sectoarele cu o importanță critică ridicată enumerate în anexa I la Directiva (UE) 2022/2555 ale căror entități pot face obiectul testării coordonate a pregătirii, ținând seama de evaluările coordonate ale riscurilor și de testele de reziliență existente și planificate la nivelul Uniunii***, în conformitate cu modalitățile stabilite pentru entitățile din sectoarele cu o importanță critică ridicată enumerate în anexa I la Directiva (UE) 2022/2555***.

(2) Grupul de cooperare NIS, în colaborare cu Comisia, ENISA, Înaltul Reprezentant ***și entitățile care fac obiectul testării coordonate a pregătirii în conformitate cu alineatul (1)***, elaborează scenarii de risc și metodologii comune pentru exercițiile de testare ***coordonată a pregătirii, în urma cărora se întocmește un plan de lucru concertat***. ***Entitățile care fac obiectul testării coordonate a pregătirii elaborează și implementează un plan de redresare care transpune recomandările rezultate în urma testării pregătirii.***

Grupul de cooperare NIS poate furniza informații pentru stabilirea ordinii de prioritate a sectoarelor sau a subsectoarelor pentru exercițiile de testare coordonată a pregătirii.

Articolul 12

Instituirea rezervei UE pentru securitate cibernetică

(1) Pentru a ajuta utilizatorii menționați la alineatul (3) să răspundă sau să ofere sprijin pentru răspunsul la incidentele de securitate cibernetică semnificative sau de mare amploare și pentru redresarea imediată în urma unor astfel de incidente, se instituie o rezervă a UE pentru securitate cibernetică.

În cazul în care se constată că serviciile achiziționate nu pot fi utilizate pe deplin în scopul furnizării de sprijin pentru răspunsul la incidente semnificative sau de mare amploare,

serviciile respective pot fi convertite în mod excepțional în exerciții sau formări pentru a trata incidentele și pot fi furnizate utilizatorilor, la cerere, de către autoritatea contractantă.

(2) Rezerva UE pentru securitate cibernetică constă în servicii de răspuns la incidente furnizate de furnizorii ***de servicii de securitate gestionate*** de încredere selectați în conformitate cu criteriile prevăzute la articolul 16. Rezerva ***UE pentru securitate cibernetică*** include servicii angajate în prealabil. Serviciile trebuie să poată fi desfășurate în toate statele membre***, consolidează suveranitatea tehnologică a Uniunii, autonomia sa strategică deschisă, competitivitatea și reziliența în sectorul securității cibernetice, inclusiv prin stimularea inovării pe piața unică digitală în întreaga Uniune***.

(3) Printre utilizatorii serviciilor din rezerva UE pentru securitate cibernetică se numără:

(a) autoritățile de gestionare a crizelor cibernetice și 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) instituțiile, organele și agențiile Uniunii***, astfel cum sunt menționate la articolul 3 punctul 1 din Regulamentul (UE) .../2023 al Parlamentului European și al Consiliului[26] și CERT-UE***.

(4) Utilizatorii menționați la alineatul (3) litera (a) utilizează serviciile din rezerva UE pentru securitate cibernetică pentru a răspunde sau a oferi sprijin pentru răspunsul la incidentele semnificative sau de mare amploare care afectează entitățile care își desfășoară activitatea în sectoare critice sau deosebit de critice și pentru redresarea imediată în urma acestora.

(5) 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 coordonare NIS2 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.

(6) Comisia ***încredințează*** ENISA funcționarea și administrarea rezervei UE pentru securitate cibernetică, integral sau parțial, prin intermediul unor acorduri de contribuție.

(7) Pentru a sprijini Comisia în instituirea rezervei UE pentru securitate cibernetică, ENISA elaborează o cartografiere a serviciilor necesare, ***inclusiv a competențelor și capacităților necesare ale forței de muncă în domeniul securității cibernetice*** după consultarea statelor membre și a Comisiei ***și, după caz, a furnizorilor de servicii de securitate gestionate și a altor reprezentanți ai sectorului securității cibernetice***. ENISA elaborează o cartografiere similară, după consultarea Comisiei***, a furnizorilor de servicii de securitate gestionate și, după caz, a altor reprezentanți ai sectorului securității cibernetice***, pentru a identifica nevoile țărilor terțe eligibile pentru sprijin din rezerva UE pentru securitate cibernetică în temeiul articolului 17. După caz, Comisia consultă Înaltul Reprezentant ***și informează Consiliul despre necesitățile țărilor terțe***.

---

26 ***Regulamentul (UE) .../2023 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii (JO C , , p, , ELI: ...).***

(8) Comisia ***este împuternicită să adopte acte delegate în conformitate cu articolul 20a pentru completarea prezentului regulament, specificând*** tipurile și numărul de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică. ▌..

Articolul 13

Cereri de sprijin din rezerva UE pentru securitate cibernetică

(1) Utilizatorii menționați la articolul 12 alineatul (3) pot solicita servicii din rezerva UE pentru securitate cibernetică pentru a sprijini răspunsul la incidentele de securitate cibernetică semnificative sau de mare amploare și redresarea imediată în urma acestora.

(2) Pentru a primi sprijin din rezerva UE pentru securitate cibernetică, utilizatorii menționați la articolul 12 alineatul (3) iau măsuri pentru a atenua efectele incidentului pentru care se solicită sprijin, inclusiv furnizarea de asistență tehnică directă și alte resurse pentru a sprijini răspunsul la incident, precum și eforturile imediate de redresare.

(3) Cererile de sprijin din partea utilizatorilor menționați la articolul 12 alineatul (3) litera (a) din prezentul regulament se transmit Comisiei și ENISA prin intermediul punctului unic de contact desemnat sau instituit de statul membru în conformitate cu articolul 8 alineatul (3) din Directiva (UE) 2022/2555.

(4) Statele membre informează rețeaua CSIRT și, după caz, EU-CyCLONe cu privire la cererile lor de răspuns la incidente și de sprijin imediat pentru redresare în temeiul prezentului articol.

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

(a) informații adecvate privind entitatea afectată și impactul potențial al incidentului și utilizarea planificată a sprijinului solicitat, inclusiv o indicație a nevoilor estimate;

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

(c) informații cu privire la alte forme de sprijin aflate la dispoziția entității afectate, inclusiv acorduri contractuale în vigoare pentru răspunsul la incidente și servicii de redresare imediată, precum și contracte de asigurare care ar putea acoperi un astfel de tip de incident.

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

(7) Comisia ***este împuternicită să adopte acte delegate în conformitate cu articolul 20a pentru a completa prezentul regulament, precizând*** modalitățile detaliate de alocare a serviciilor de sprijin din rezerva UE pentru securitate cibernetică. ▌

Articolul 14

Punerea în aplicare a sprijinului din rezerva UE pentru securitate cibernetică

(1) Cererile de sprijin din rezerva UE pentru securitate cibernetică sunt evaluate de Comisie, cu sprijinul ENISA sau astfel cum sunt definite în acordurile de contribuție în temeiul

articolului 12 alineatul (6), iar utilizatorilor menționați la articolul 12 alineatul (3) li se transmite ▌ un răspuns ***fără întârzieri nejustificate și în orice caz în termen de 24 de ore***.

(2) Pentru a stabili prioritatea cererilor, în cazul cererilor concurente multiple, se iau în considerare următoarele criterii, după caz:

(a) gravitatea incidentului de securitate cibernetică;

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

(c) impactul potențial asupra statului membru (statelor membre) afectat(e) sau asupra utilizatorilor afectați;

(d) ***amploarea și*** caracterul transfrontalier potențial al incidentului și riscul de propagare către alte state membre sau alți utilizatori;

(e) măsurile luate de utilizator pentru a sprijini răspunsul și eforturile imediate de redresare, astfel cum se menționează la articolul 13 alineatul (2) și la articolul 13 alineatul (5) litera (b).

(3) Serviciile din rezerva UE pentru securitate cibernetică sunt furnizate în conformitate cu acordurile specifice dintre furnizorul de servicii și utilizatorul căruia i se acordă sprijin din cadrul rezervei UE pentru securitate cibernetică. Aceste acorduri includ condiții de răspundere ***și orice alte dispoziții pe care părțile la acord le consideră necesare pentru furnizarea serviciului respectiv***.

(4) Acordurile menționate la alineatul (3) se ***bazează*** pe modele elaborate de ENISA, după consultarea statelor membre ***și, după caz, a altor utilizatori ai rezervei UE pentru securitate cibernetică***.

(5) Comisia și ENISA nu își asumă răspunderea contractuală pentru daunele cauzate terților de serviciile furnizate în cadrul punerii în aplicare a rezervei UE pentru securitate cibernetică***, cu excepția cazurilor de neglijență gravă în evaluarea solicitării furnizorului de servicii sau a cazului în care Comisia sau ENISA sunt utilizatori ai rezervei UE pentru securitate cibernetică în conformitate cu articolul 14 alineatul (3)***.

(6) În termen de o lună de la încheierea acțiunii de sprijin, utilizatorii prezintă Comisiei și ENISA***, rețelei CSIRT și, după caz, EU-CyCLONe*** un raport de sinteză privind serviciul furnizat, rezultatele obținute și învățămintele desprinse. În cazul în care utilizatorul provine dintr-o țară terță, astfel cum se prevede la articolul 17, acest raport este transmis Înaltului Reprezentant.
Raportul respectă dreptul Uniunii și dreptul intern privind protecția informațiilor sensibile sau clasificate.

(7) Comisia raportează ▌ Grupului de cooperare NIS ***periodic și cel puțin de două ori pe an*** cu privire la utilizarea și rezultatele sprijinului. ***În acest proces protejează informațiile confidențiale, în conformitate cu dreptul Uniunii și cu dreptul intern privind protecția informațiilor sensibile sau clasificate.***

Articolul 15

Coordonarea cu mecanismele de gestionare a crizelor

(1) În cazurile în care incidentele de securitate cibernetică semnificative sau de mare amploare își au originea în dezastre sau determină dezastre, astfel cum sunt definite în Decizia 1313/2013/UE[27], sprijinul acordat în temeiul prezentului regulament pentru răspunsul la astfel de incidente completează acțiunile prevăzute în Decizia 1313/2013/UE și nu aduc atingere acesteia.

(2) În cazul unui incident transfrontalier de securitate cibernetică de mare amploare în care sunt declanșate mecanisme integrate ale UE pentru un răspuns politic la crize (IPCR), sprijinul acordat în temeiul prezentului regulament pentru răspunsul la un astfel de incident este gestionat în conformitate cu protocoalele și procedurile relevante din cadrul IPCR.

(3) În consultare cu Înaltul Reprezentant, sprijinul acordat în cadrul mecanismului 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. De asemenea, acesta poate completa asistența acordată de un stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din ***TUE*** sau poate contribui la aceasta.

(4) Sprijinul acordat în cadrul mecanismului pentru situații de urgență ***în materie de securitate*** cibernetică poate face parte din răspunsul comun al Uniunii și al statelor membre în situațiile menționate la articolul 222 din TFUE.

Articolul 16

Furnizori de încredere

(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) 2018/1046 și cu următoarele principii:

(a) se asigură că rezerva UE pentru securitate cibernetică include servicii care pot fi implementate în toate statele membre, ținând seama în special de cerințele naționale pentru furnizarea unor astfel de servicii, inclusiv 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 europeană, contribuind la obiectivele prevăzute la articolul 3 din Regulamentul (UE) 2021/694, inclusiv prin promovarea dezvoltării competențelor în materie de securitate cibernetică în UE ***și atingerea echilibrului de gen în sector, și întărind suveranitatea tehnologică a Uniunii, autonomia strategică deschisă, competitivitatea și reziliența acesteia***.

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

(a) furnizorul demonstrează că personalul său are cel mai înalt grad de integritate profesională, independență, responsabilitate și competență tehnică necesară pentru a

[27] 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).

desfășura activitățile în domeniul său specific și asigură permanența/continuitatea expertizei, precum și resursele tehnice necesare;

(b) furnizorul, filialele și subcontractanții acestuia dispun de un cadru pentru protecția informațiilor sensibile referitoare la serviciu, în special a dovezilor, a constatărilor și a rapoartelor, și respectă normele de securitate ale Uniunii privind protecția informațiilor UE clasificate;

(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;

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

(f) furnizorul este dotat cu echipamentele tehnice hardware și software ***actualizate*** necesare pentru a sprijini serviciul solicitat ***și respectă, după caz, Regulamentul (UE) .../... al Parlamentului European și al Consiliului[28] (2022/0272(COD))***;

(g) furnizorul este în măsură să demonstreze că are experiență în furnizarea de servicii similare autorităților sau entităților naționale relevante care își desfășoară activitatea în sectoare critice sau deosebit de critice;

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

(i) furnizorul este în măsură să furnizeze serviciul în limba locală a statului membru (statelor membre) ***sau într-una dintre limbile de lucru ale instituțiilor Uniunii*** în care poate furniza serviciul;

(j) odată ce se instituie ▌ un sistem ***european*** de certificare ***a securității cibernetice*** pentru serviciul de securitate gestionat ***în conformitate cu Regulamentul (UE) 2019/881***, furnizorul este certificat în conformitate cu sistemul respectiv***, într-o perioadă de doi ani după ce sistemul a fost adoptat***.

(ja) furnizorul este în măsură să furnizeze serviciul independent și nu ca parte a unui pachet, garantându-i astfel utilizatorului posibilitatea de a trece la un alt furnizor de servicii;

(jb) în sensul articolului 12 alineatul (1), furnizorul include în propunerea de oferte posibilitatea ca serviciile de răspuns la incidente care nu au fost utilizate să fie transformate în exerciții sau formări;

(jc) furnizorul are sediul și structurile de gestionare executivă în Uniune, într-o țară asociată sau într-o țară terță care este parte la Acordul privind achizițiile publice în contextul Organizației Mondiale a Comerțului (AAP).

(jd) . Furnizorul nu este supus controlului unei țări terțe neasociate sau al unei entități dintr-o țară terță neasociată care nu este parte la AAP sau, alternativ, o astfel de entitate trebuie să fi făcut obiectul unei examinări în înțelesul Regulamentului (UE)

---

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

2019/452 și, dacă este necesar, al unor măsuri de atenuare, ținând seama de obiectivele enunțate în prezentul regulament.

Articolul 17

Sprijinul acordat țărilor terțe

(1) Țările terțe pot solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care acordurile de asociere încheiate cu privire la participarea lor la DEP prevăd acest lucru.

(2) Sprijinul din rezerva UE pentru securitate cibernetică este în conformitate cu prezentul regulament și respectă toate condițiile specifice prevăzute în acordurile de asociere menționate la alineatul (1).

(3) Printre utilizatorii din țările terțe asociate eligibile pentru a beneficia de servicii din rezerva UE pentru securitate cibernetică se numără autoritățile competente, cum ar fi CSIRT și autoritățile de gestionare a crizelor cibernetice.

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

(5) Înainte de a primi orice sprijin din rezerva UE pentru securitate cibernetică, țările terțe furnizează Comisiei și Înaltului Reprezentant informații cu privire la reziliența lor cibernetică și la capabilitățile lor de gestionare a riscurilor, incluzând cel puțin informații cu privire la măsurile naționale luate în vederea pregătirii pentru incidente de securitate cibernetică semnificative sau de mare amploare, precum și informații privind entitățile naționale responsabile, inclusiv CSIRT sau entitățile echivalente, capabilitățile acestora și resursele care le sunt alocate. Dispozițiile articolelor 13 și 14 din prezentul regulament care fac referire la statele membre se aplică țărilor terțe, astfel cum se prevede la alineatul (1).

(6) Comisia ***informează Consiliul fără întârzieri nejustificate*** și se consultă cu Înaltul Reprezentant cu privire la cererile primite și la punerea în aplicare a sprijinului acordat țărilor terțe din rezerva UE pentru securitate cibernetică.

Capitolul IV

MECANISMUL DE ANALIZĂ A INCIDENTELOR DE SECURITATE CIBERNETICĂ

Articolul 18

Mecanismul de analiză a incidentelor de securitate cibernetică

(1) La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA analizează și evaluează amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA transmite rețelei CSIRT, EU-CyCLONe și Comisiei un raport de evaluare a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, având-le

în vedere în special pe cele prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. Dacă este cazul, Comisia transmite raportul Înaltului Reprezentant.

(2) Pentru a elabora raportul de evaluare a incidentelor menționat la alineatul (1), ENISA colaborează cu toate părțile interesate relevante ***și adună observațiile acestora***, inclusiv ***cu*** reprezentanți ai statelor membre, ai Comisiei sau ai altor instituții, organisme***, birouri*** și agenții relevante ale UE, ***cu*** furnizori de servicii de securitate gestionate ***în SOC-urile naționale și transfrontaliere*** și ***cu*** utilizatori de servicii de securitate cibernetică***, împreună cu garanții și monitorizări corespunzătoare pentru a asigura sprijinul actorilor din sectorul serviciilor de securitate cibernetică pentru lecțiile învățate și cele mai bune practici identificate***. După caz, ENISA colaborează și cu entitățile afectate de incidente de securitate cibernetică semnificative sau de mare amploare. Pentru a sprijini evaluarea, ENISA poate consulta și alte tipuri de părți interesate. Reprezentanții consultați comunică orice potențial conflict de interese.

(3) Raportul cuprinde o evaluare și o analiză a incidentului specific de securitate cibernetică semnificativ sau de mare amploare, incluzând principalele cauze, vulnerabilități și învățăminte desprinse. Acesta protejează informațiile confidențiale, în conformitate cu dreptul Uniunii sau cu dreptul intern privind protecția informațiilor sensibile sau clasificate. ***Raportul nu trebuie să conțină detalii cu privire la vulnerabilitățile exploatate activ și care nu sunt încă remediate.***

(3a) În raportul menționat la alineatul (1) sunt prezentate lecțiile învățate din evaluările inter pares efectuate în temeiul articolului 19 din Directiva (UE) 2022/2555.

(4) După caz, raportul formulează recomandări***, inclusiv pentru toate părțile interesate vizate,*** pentru îmbunătățirea poziției cibernetice a Uniunii.

(5) Dacă este posibil, se pune la dispoziția publicului o versiune a raportului. Această versiune include numai informații publice.

Capitolul V

DISPOZIȚII FINALE

Articolul 19

Modificări aduse 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):

„(aa) sprijinirea dezvoltării unui Scut cibernetic al UE, inclusiv dezvoltarea, implementarea și operarea platformelor SOC naționale și transfrontaliere care contribuie la conștientizarea

situației în Uniune și la consolidarea capacităților de informații privind amenințările cibernetice ale Uniunii”;

(***ii***) se adaugă următoarea literă (g):

„(g) instituirea și gestionarea unui mecanism pentru situații de urgență ***în materie de securitate*** cibernetică pentru a sprijini statele membre în pregătirea pentru incidentele semnificative de securitate cibernetică și răspunsul la acestea, complementar resurselor și capabilităților naționale și altor forme de sprijin disponibile la nivelul Uniunii, inclusiv instituirea unei rezerve a UE pentru securitate cibernetică”;

(***b***) Alineatul (2) se înlocuiește cu următorul text:

„(2) Acțiunile din cadrul obiectivului specific nr. 3 sunt puse în aplicare 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 excepția acțiunilor de punere în aplicare a rezervei UE pentru securitate cibernetică, care sunt puse în aplicare de către Comisie și ENISA.

---

* 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).”;***

2. Articolul 9 se modifică după cum urmează:

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

„(b) 1 776 956 000 EUR pentru obiectivul specific nr. 2 – Inteligența artificială;

(c) ***1 620 566 000*** EUR pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea;

(d) ***500 347 000*** EUR pentru obiectivul specific nr. 4 – Competențele digitale avansate;”;

(aa) se introduce următorul alineat (2a):

„ (2a) Cuantumul menționat la alineatul (2) litera (c) se utilizează în principal pentru atingerea obiectivelor operaționale menționate la articolul 6 alineatul (1) literele (a)-(f) din program.”;

(ab) se adaugă următorul alineat (2b):

„ (2b) Cuantumul prevăzut pentru instituirea și executarea rezervei destinate securității cibernetice a UE nu depășește 27 de milioane EUR pentru durata prevăzută a aflării în vigoare a Regulamentului de stabilire a unor măsuri de consolidare a solidarității și a capacităților Uniunii pentru detectarea amenințărilor și incidentelor de securitate

cibernetică, pentru pregătirea legată de acestea și pentru contracararea lor.";

(b) se adaugă următorul alineat (8):

„(8) Prin derogare de la articolul 12 alineatul (4) din Regulamentul (UE, Euratom) 2018/1046, creditele de angajament și de plată neutilizate pentru acțiuni care***, în contextul executării rezervei UE pentru securitate cibernetică,*** urmăresc obiectivele stabilite 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 conformitate cu articolul 12 alineatul (6) din Regulamentul (UE, Euratom) 2018/1046.

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

„(2) Programul poate oferi finanțare în oricare dintre formele prevăzute de Regulamentul ***(UE, Euratom) 2018/1046***, 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 [27] și 2014/25/UE [28] 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.

Pentru 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 pun în aplicare proceduri de achiziții pentru rezerva UE pentru securitate cibernetică instituită prin articolul 12 din Regulamentul (UE) 2023***/...***, 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. 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 169 alineatul (3) din Regulamentul (UE) ***.../...***, solicitarea unei singure țări terțe este suficientă pentru a mandata Comisia sau ENISA să acționeze.

Atunci când pun în aplicare procedurile de achiziții pentru rezerva UE pentru securitate cibernetică instituită prin articolul 12 din Regulamentul (UE) 2023/***...***, Comisia și ENISA pot acționa ca organism central de achiziție pentru a achiziționa în numele sau în contul instituțiilor, organelor și 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 și agențiile Uniunii. Prin derogare de la articolul 169 alineatul (3) din Regulamentul (UE) ***.../...***, solicitarea din partea unei singure instituții, a unui singur organ sau a unei singure agenții a (al) Uniunii este suficientă pentru a mandata Comisia sau ENISA să acționeze.

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

4. Se adaugă următorul articol 16a:

„***Articolul 16a***

În cazul acțiunilor de punere în aplicare a Scutului cibernetic european instituit prin articolul 3 din Regulamentul (UE) 2023/XX, normele aplicabile sunt cele prevăzute la articolele 4 și 5 din Regulamentul (UE) 2023/***...***. În cazul unui conflict între dispozițiile prezentului regulament și articolele 4 și 5 din Regulamentul (UE) 2023/***...***, acestea din urmă prevalează și se aplică acțiunilor specifice respective.”

5. Articolul 19 se înlocuiește cu următorul text:

„Granturile din cadrul programului sunt acordate și gestionate în conformitate cu titlul VIII din Regulamentul ***(UE, Euratom) 2018/1046*** și pot acoperi până la 100 % din costurile eligibile, fără a aduce atingere principiului cofinanțării prevăzut la articolul 190 din Regulamentul ***(UE, Euratom) 2018/1046***. 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, către SOC-urile naționale menționate la articolul 4 din Regulamentul ***(UE) .../...*** și către consorțiul-gazdă menționat la articolul 5 din Regulamentul ***(UE) .../...***, în conformitate cu articolul 195 alineatul (1) litera (d) din Regulamentul ***(UE, Euratom) 2018/1046***.

Sprijinul sub formă de granturi pentru mecanismul pentru situații de urgență ***în materie de securitate*** cibernetică, astfel cum este prevăzut la articolul 10 din Regulamentul ***(UE) .../...***, poate fi acordat direct de ECCC statelor membre fără o cerere de propuneri, în conformitate cu articolul 195 alineatul (1) litera (d) din Regulamentul ***(UE, Euratom) 2018/1046***.

Pentru acțiunile menționate la articolul 10 alineatul (1) litera (c) din Regulamentul ***(UE) .../...***, ECCC informează Comisia și ENISA cu privire la cererile de granturi directe ale statelor membre fără o cerere de propuneri.

Pentru sprijinirea asistenței reciproce ca răspuns la un incident de securitate cibernetică semnificativ sau de mare amploare, astfel cum este definit la articolul 10 litera (c) din Regulamentul ***(UE) .../...*** și în conformitate cu articolul 193 alineatul (2) al doilea paragraf litera (a) din Regulamentul ***(UE, Euratom) 2018/1046***, în cazuri justificate în mod corespunzător, costurile pot fi considerate eligibile chiar dacă au fost suportate înainte de depunerea cererii de grant.”

6. Anexele I și II la Regulamentul (UE) 2021/694 se modifică în conformitate cu anexa la prezentul regulament.

Articolul 19a
Resurse suplimentare pentru ENISA

ENISA primește resurse suplimentare pentru a-și îndeplini sarcinile suplimentare ce îi sunt conferite prin prezentul regulament. Acest sprijin suplimentar, inclusiv sub formă de finanțare, nu pune în pericol realizarea obiectivelor altor programe ale Uniunii, în special ale programului „Europa digitală”.

Articolul 20

Evaluarea *și revizuirea*

(1) Până la ... [***doi*** ani de la data de la care se aplică prezentul regulament] ***și, ulterior, o dată la doi ani,*** Comisia ***efectuează o evaluare a funcționării măsurilor prevăzute în prezentul*** regulament ***și transmite un raport Parlamentului European și Consiliului***.

(2) În cadrul evaluării se analizează în special:

(a) utilizarea și valoarea adăugată a SOC-urilor transfrontaliere și măsura în care acestea contribuie la depistarea mai rapidă a amenințărilor cibernetice și la realizarea mai rapidă a unui răspuns la acestea, precum și la conștientizarea situației; participarea activă a SOC-urilor naționale la Scutul cibernetic european, inclusiv numărul de SOC naționale și de SOC transfrontaliere înființate și măsura în care acestea contribuie la generarea și la schimbul de informații operative de înaltă calitate și de date operative privind amenințările cibernetice; numărul și costul infrastructurilor și/sau ale instrumentelor de securitate cibernetică achiziționate în comun; numărul de acorduri de cooperare încheiate între SOC transfrontaliere și ISAC din sector; numărul de incidente raportate rețelei CSIRT și impactul pe care aceasta îl are asupra activității rețelei CSIRT;

(b) atât aspectele pozitive, cât și cele negative ale funcționării mecanismului pentru situații de urgență în materie de securitate cibernetică, inclusiv dacă sunt necesare cerințe suplimentare de cooperare sau de formare;

(c) contribuția prezentului regulament la consolidarea rezilienței și a autonomiei strategice deschise ale Uniunii, la îmbunătățirea competitivității sectoarelor corespunzătoare, inclusiv a microîntreprinderilor, IMM-urilor și a întreprinderilor

nou-înființate, și la dezvoltarea competențelor în materie de securitate cibernetică în UE;

(d) utilizarea și valoarea adăugată a rezervei UE pentru securitate cibernetică, inclusiv numărul de furnizori de securitate de încredere care fac parte din rezerva UE pentru securitate cibernetică; numărul, tipul, costurile și impactul acțiunilor întreprinse pentru a sprijini răspunsul la incidentele de securitate cibernetică, precum și ale utilizatorilor și furnizorilor acestora; timpul mediu necesar pentru ca Comisia să recunoască existența unor incidente, ca rezerva UE pentru securitate cibernetică să fie activată și să răspundă la acestea și ca utilizatorul să se redreseze în urma acestora; dacă domeniul de aplicare al rezervei UE pentru securitate cibernetică ar trebui extins la serviciile de pregătire pentru incidente sau la exercițiile comune cu furnizorii de încredere de servicii de securitate gestionate și cu potențialii utilizatori ai rezervei UE pentru securitate cibernetică, pentru a se asigura funcționarea eficientă a rezervei UE pentru securitate cibernetică atunci când este necesar;

(e) contribuția prezentului regulament la dezvoltarea și îmbunătățirea aptitudinilor și competențelor forței de muncă din sectorul securității cibernetice, necesare pentru a întări capacitatea Uniunii de a depista, de a preveni, de a răspunde la amenințările și incidentele de securitate cibernetică și de a se redresa în urma acestora;

(f) contribuția prezentului regulament la implementarea și dezvoltarea în Uniune a tehnologiilor de ultimă generație.

(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 20a

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 prevăzută la articolul 6 alineatul (3), articolul 7 alineatul (2), articolul 12 alineatul (8) și articolul 13 alineatul (7) se conferă Comisiei pe o perioadă de ... ani de la ... [data intrării în vigoare a actului legislativ de bază sau orice altă dată stabilită de colegiuitori]. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de ... 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 6 alineatul (3), la articolul 7 alineatul (2), la articolul 12 alineatul (8) și la articolul 13 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 6 alineatul (3), al articolului 7 alineatul (2), al articolului 12 alineatul (8) sau al articolului 13 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 formula obiecții. Respectivul termen se prelungește cu [două luni] la inițiativa Parlamentului European sau a Consiliului.

Articolul 21

Procedura comitetului

(1) Comisia este asistată de Comitetul de coordonare al programului „Europa digitală” instituit prin Regulamentul (UE) 2021/694. Acesta este un comitet în sensul Regulamentului (UE) nr. 182/2011.

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

Articolul 22

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 Strasbourg,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

ANEXĂ

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

(1) În anexa I, secțiunea/capitolul „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 Uniunii, a societății și democrației 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 informatice, 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 și conștientizarea situației în spațiul cibernetic, ***inclusiv la nivelul SOC-urilor naționale și al SOC-urilor transfrontaliere care formează Scutul cibernetic european***, 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***, cu un accent deosebit pe atingerea echilibrului de gen în acest sector***, de exemplu prin alinierea programelor privind competențele în domeniul securității cibernetice, adaptarea acestora la nevoile sectoriale specifice***, inclusiv un accent interdisciplinar și general,*** și facilitarea accesului la formare specializată specifică ***pentru a permite accesul***

tuturor persoanelor și teritoriilor, fără a afecta posibilitatea de a beneficia de oportunitățile oferite de prezentul regulament.

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

(2) În anexa II, secțiunea/capitolul „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 ***în cadrul scutului 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***, tipul, costul și impactul acțiunilor desfășurate pentru a sprijini pregătirea*** în vederea incidentelor de securitate cibernetică și ***răspunsul*** la acestea în cadrul mecanismului pentru situații de urgență ***în materie de securitate*** cibernetică. ***Măsura în care recomandările privind testele de pregătire au fost puse în aplicare și efectuate de utilizator, precum și timpul mediu în care Comisia constată incidentele, rezerva UE pentru securitate cibernetică răspunde la acestea și utilizatorul se redresează în urma lor."***

EXPUNERE DE MOTIVE

CONTEXTUL

Securitatea cibernetică este, în mod firesc, un concept esențial pentru democrațiile noastre. Amenințările la adresa securității cibernetice provoacă insecuritate în rândul populației și al întreprinderilor și accentuarea dezinformării, ceea ce periclitează principiile democratice privind respectarea drepturilor omului. Pentru a preveni o atare situație, un mediu digital sigur, supus controlului public, este esențial pentru democrațiile noastre.

Atacurile cibernetice în UE sunt în creștere ca metode și ca impact. În plus, atacul Rusiei împotriva Ucrainei a creat schimbări profunde, chiar și înainte de invazie, și a inaugurat o nouă eră pentru **programele cibernetice**, potrivit raportului ENISA privind situația amenințărilor din 2022.[1] Prioritățile identificate în urma acestui conflict în domeniul cibernetic sunt necesitatea de a **consolida capacitățile** în cadrul **programelor** și proiectelor **multilaterale** și necesitatea de **a dezvolta** rapid **competențele**. Pentru o mai mare reziliență este urgent necesar un răspuns european comun, cu o cooperare mai strânsă la nivel european, dincolo de cel național.

Dezvoltarea ca bun public a unei veritabile culturi a securității cibernetice, care să înglobeze securitatea, inclusiv cea a mediului digital, va fi esențială pentru punerea în aplicare cu succes a prezentului regulament.

În plus, atacurile cibernetice vizează frecvent **serviciile și infrastructurile publice locale, regionale sau naționale** (de exemplu sectorul asistenței medicale, care rămâne o țintă predilectă pentru atacurile cibernetice[2]). Datele arată, de asemenea, că **autoritățile locale** se numără printre cele mai vulnerabile ținte din cauza lipsei de resurse financiare și umane și că este deosebit de important ca liderii de la nivel local să fie sensibilizați cu privire la creșterea rezilienței digitale[3]. Atacurile afectează în primul rând și în mod direct cetățenii și, prin urmare, pun în pericol democrațiile noastre, inclusiv prin campanii de dezinformare. Sentimentul de nesiguranță pe care îl pot crea în rândul populației aceste situații poate conduce la preferințe politice pentru un angajament radical în materie de securitate, în detrimentul respectării drepturilor fundamentale. Însă este adevărat mai degrabă contrariul: securitatea este o parte esențială a democrațiilor noastre, care este compatibilă cu toate celelalte drepturi și necesară pentru acestea.

În plus, **întreprinderile și IMM-urile** din UE se confruntă și ele cu criminalitatea informatică și, având în vedere utilizarea tot mai frecventă a sferei digitale pentru activități comerciale, există un interes mai pronunțat față de securitatea cibernetică. IMM-urile sunt cele mai puțin

[1] ENISA Threat Landscape 2022, octombrie 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[2] Raportul ENISA privind situația amenințărilor: sectorul sănătății, iulie 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[3] Comitetul European al Regiunilor, Reziliența digitală, 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

pregătite, cu mai puține resurse pentru a se proteja și mai puțin conștiente de faptul că pot face obiectul unor astfel de atacuri.

Se preconizează că aceste atacuri vor continua și vor crește în viitor, în special în situații de instabilitate politică și cu atât mai mult în contextul unor războaie. Pe măsură ce tranziția digitală avansează în fiecare zi, reziliența digitală devine din ce în ce mai importantă pentru viața noastră de zi cu zi și pentru **autonomia strategică deschisă a UE**.

PROPUNEREA RAPORTOAREI

Raportoarea consideră că UE trebuie să fie mai bine pregătită pentru viitor și salută acest act legislativ stringent necesar pentru a pune în comun resursele, informațiile și cunoștințele în vederea asigurării solidarității între statele membre, a creșterii capacității industriale în UE, a dezvoltării, **în mod coordonat, a competențelor și capacităților** care să asigure securitatea cibernetică, pentru a rezista mai bine la atacurile viitoare și pentru a ne proteja democrațiile de situații în care nevoile în materie de securitate sunt invocate abuziv. În plus, este important să protejăm integritatea proceselor noastre electorale. Acest act legislativ reprezintă un angajament esențial pentru atingerea obiectivului **autonomiei strategice deschise**.

Din aceste motive, UE are nevoie de o **guvernanță** puternică și **coordonată** în UE și de o cooperare structurată cu sectorul privat, pentru a stimula dezvoltarea industriei cibernetice europene. Pe lângă colaborarea cu parteneri internaționali care împărtășesc aceeași viziune se poate coopera și cu alte țări care nu au aceleași capacități și care ar putea avea nevoie de asistență atunci când cad victime ale unor atacuri cibernetice. Regulamentul UE privind solidaritatea cibernetică trebuie să își definească bine nivelurile de guvernanță și să nu se suprapună inițiativelor și legislației deja existente, cum ar fi Directiva NIS2.

Propunerea se bazează mult pe schimbul voluntar de informații între statele membre. Din acest motiv, raportoarea propune consolidarea garanțiilor pentru cultivarea încrederii între statele membre, cu scopul de a spori participarea și cooperarea acestora, de exemplu în ceea ce privește achizițiile comune de infrastructură, precum și implicarea puterilor legislative, pentru a asigura încrederea cetățenilor și **garanțiile democratice**.

În al doilea rând, raportoarea propune ca în viitoarele CFM **să se asigure bugetul** necesar pentru această inițiativă, inclusiv cu participarea statelor membre, pentru a se garanta continuitatea activităților dezvoltate în temeiul Regulamentului UE privind solidaritatea cibernetică și după 2027.

În al treilea rând, raportoarea propune îmbunătățirea **structurii de guvernanță**, formularea unei definiții clare a guvernanței și corelarea acesteia cu legislația existentă.

Raportoarea propune și o mai bună **coordonare** între diferitele entități din statele membre responsabile cu securitatea cibernetică, pentru a se constitui o protecție cibernetică comună. În plus, este necesară creșterea contribuției ENISA la coordonarea și interacțiunea dintre diferiții actori ai comunităților naționale.

În ceea ce privește **noua rezervă pentru securitate cibernetică**, raportoarea consideră că aceasta are potențialul de a dezvolta capacități industriale în UE, inclusiv pentru IMM-uri, prin

investiții în cercetare și inovare, cu scopul de a dezvolta tehnologii de ultimă generație, cum ar fi tehnologiile cloud și tehnologiile de inteligență artificială. În plus, raportoarea propune menținerea participării actorilor din acest sector, consolidarea criteriilor și a încrederii în legătură cu participarea acestora (și anume, conectarea participării lor la o întreprindere națională sau locală) prin clarificarea **criteriilor** și a definiției **suveranității tehnologice** și garantarea unui echilibru între actorii din afara UE și cei din UE. În plus, raportoarea propune ca **mecanismul pentru situații de urgență cibernetică** să fie utilizat cu un **sistem de certificare** pentru furnizorii privați, astfel încât să se construiască un parteneriat de lungă durată și de încredere.

În ceea ce privește **mecanismul de analiză a incidentelor**, raportoarea propune consolidarea rolului ENISA și al sectorului privat în cadrul SOC, cu garanțiile și monitorizarea corespunzătoare, pentru a se verifica dacă învățămintele trase sunt susținute și de actorii din sector. În plus, raportoarea propune includerea învățămintelor trase prin evaluările inter pares, astfel cum se prevede în Directiva NIS2, și creșterea finanțării ENISA, cu scopul de a asigura o aplicare efectivă a legislației și o protecție adecvată împotriva amenințărilor la adresa securității cibernetice.

În plus, prezenta propunere, prin definiție, are o **dimensiune externă** foarte relevantă, fie că țările terțe pot avea acces la resurse și la sprijin prin intermediul Regulamentului UE privind solidaritatea cibernetică, utilizând sprijinul pentru răspunsul la incidente din rezerva UE pentru securitate cibernetică, fie că sunt încă necesari pentru rezerva cibernetică actori din afara UE din sectorul privat. Dimensiunea externă ar trebui de asemenea supusă controlului public, cu participarea ramurilor legislative, pentru a se garanta participarea cetățenilor la acest proces. Securitatea cibernetică ar trebui considerată un bun public.

În plus, un element central al prezentei propuneri este dezvoltarea de aptitudini și competențe care ar trebui să depășească simpla investiție în dezvoltarea cunoștințelor, urmând să se asigure investiții în accesul tuturor cetățenilor la dobândirea de astfel de competențe. Raportoarea propune să se întărească legătura cu **Academia de competențe în materie de securitate cibernetică a UE**, care intenționează să elimine deficitul de specialiști în materie de securitate cibernetică prin reunirea inițiativelor private și publice și prin asigurarea formării și certificării cetățenilor. Acest proces de consolidare va necesita garanții prin care să se evite exodul creierelor, fără însă a fi afectată mobilitatea forței de muncă.

În plus, raportoarea propune să se investească și să se includă măsuri active de dezvoltare a competențelor în acest sector, având în vedere că 2023 este Anul european al competențelor, precum și să se intensifice campaniile de informare a cetățenilor. Măsurile vor fi concepute astfel încât investițiile să nu creeze dezechilibre între statele membre, deoarece cererea actuală ridicată și salariile ridicate din acest sector pot duce la un exod al creierelor către cele mai bine plătite opțiuni.

Din aceste motive, raportoarea propune consolidarea aptitudinilor și competențelor specializate, interdisciplinare și generale în întreaga UE, cu un accent special pe femei, deoarece disparitatea de gen persistă în domeniul securității cibernetice, femeile reprezentând 20 % din media

persoanelor active în domeniu la nivel mondial.[4] Femeile trebuie să fie prezente și să facă parte din conceperea viitorului digital și a guvernanței acestuia.

În plus, raportoarea propune să se consolideze triunghiul dintre centrele naționale de competență, Centrul european de competențe în materie de securitate cibernetică (ECCC) și ENISA în dezvoltarea aptitudinilor și competențelor. În plus, trebuie intensificat rolul **sectorului** în **dezvoltarea competențelor** și în crearea de parteneriate cu **mediul academic** și cu actorii societății civile, luând în considerare experiența, cunoștințele și specializarea regionale și alianțele cu țările terțe, cu parteneri care împărtășesc aceeași viziune, pentru a intensifica schimburile și a asigura o abordare globală pentru a sprijini cetățenii, întreprinderile și instituțiile.

Raportoarea propune și o cooperare în ceea ce privește specialiștii și măsurarea daunelor aduse oamenilor de atacurile cibernetice (de exemplu impactul unui atac de tip ransomware asupra sectorului sănătății).

Raportoarea propune măsuri pentru a se include și a se îmbunătăți informarea cetățenilor fără alarmism, ca o altă măsură care să garanteze protejarea democrațiilor și a valorilor noastre fundamentale. Dezvoltarea ca bun public a unei veritabile **culturi a securității cibernetice**, care să înglobeze securitatea, inclusiv cea a mediului digital. Astfel, vom putea garanta un model de democrație digitală, spre deosebire de unul de autoritarism digital, cu transparență, democrație și cu certitudinea pe care o poate aduce elaborarea unei legislații de reglementare.

Totodată, raportoarea consideră că consolidarea **C&I** în domeniul securității cibernetice va spori reziliența și autonomia strategică deschisă a Uniunii. În mod similar, asigurarea unor sinergii cu programele de cercetare și inovare și cu instrumentele și instituțiile existente și consolidarea triunghiului cunoașterii pentru a elimina lacunele în materie de competențe în întreaga UE.

În plus, această legislație va spori reziliența UE și a statelor sale membre, nu numai direct prin intermediul legislației privind securitatea cibernetică și reziliența cibernetică, ci și prin impactul pe care aceasta îl poate avea asupra dezvoltării exponențiale a inteligenței artificiale și cel pe care îl poate avea reglementarea datelor și a confidențialității datelor asupra securității cibernetice.

În plus, această legislație ne va permite să realizăm angajamentul asumat în **Declarația europeană privind drepturile și principiile digitale pentru deceniul digital**, legat de protejarea intereselor cetățenilor, ale întreprinderilor și ale instituțiilor publice împotriva riscurilor de securitate cibernetică și a criminalității informatice, inclusiv împotriva încălcării securității datelor și a furtului sau manipulării identității.

În acest context, raportoarea consideră că această propunere ar trebui să fie operațională cât mai rapid posibil, inclusiv Scutul cibernetic european și mecanismul pentru situații de urgență cibernetică, pentru a dispune de un cadru general și pentru a se evita compartimentarea,

[4] Rezoluția Parlamentului European din 10 iunie 2021 referitoare la promovarea egalității de gen în învățământul și carierele din domeniile științei, tehnologiei, ingineriei și matematicii (STIM) (2019/2164 (INI)) https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52021IP0296

întrucât spațiul cibernetic nu cunoaște frontiere.

ANEXĂ: ENTITĂȚILE SAU PERSOANELE DE LA CARE RAPORTOAREA A PRIMIT CONTRIBUȚII

Potrivit articolului 8 din anexa I la Regulamentul de procedură, raportoarea declară că a primit contribuții de la următoarele entități sau persoane pentru întocmirea raportului, înainte de adoptarea acestuia în comisie:

Entitatea și/sau persoana
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Lista de mai sus este elaborată sub responsabilitatea exclusivă a raportoarei.

27.10.2023

AVIZ AL COMISIEI PENTRU AFACERI EXTERNE

destinat Comisiei pentru industrie, cercetare și energie

referitor 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))

Raportor pentru aviz: Dragoş Tudorache

Amendamentul 1

Propunere de regulament
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică, întrucât administrațiile publice, întreprinderile și cetățenii sunt astăzi mai interconectați și mai interdependenți decât oricând, între sectoare și dincolo de frontiere.	(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică ***și militară***, întrucât administrațiile publice, întreprinderile și cetățenii***, precum și actorii din domeniul militar și al apărării*** sunt astăzi mai interconectați și mai interdependenți decât oricând, între sectoare și dincolo de frontiere.

Amendamentul 2

Propunere de regulament
Considerentul 2

Textul propus de Comisie	*Amendamentul*
(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt	(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt

în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. ***Această amenințare depășește*** agresiunea militară a Rusiei asupra Ucrainei și ***este susceptibilă*** să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei 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 în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări.

în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. ***Gravitatea acestor amenințări a devenit și mai pertinentă ca urmare a revenirii războiului pe continentul nostru. Aceste amenințări depășesc*** agresiunea militară a Rusiei asupra Ucrainei și ***sunt susceptibile*** să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii și ar putea avea chiar consecințe asupra sănătății sau asupra vieții ***în cazul unei eventuale subminări a instalațiilor legate de securitatea locală sau națională***. În plus, incidentele de securitate cibernetică sunt imprevizibile, deoarece adesea apar și evoluează în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări. ***Securitatea cibernetică este importantă pentru a ne proteja valorile europene și asigură funcționarea democrațiilor noastre, apărându-ne infrastructura electorală și procedurile democratice de orice ingerință străină.***

Amendamentul 3

Propunere de regulament
Considerentul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	(2a) Securitatea cibernetică este esențială pentru a menține siguranța Uniunii noastre și pentru a împiedica actorii răuvoitori, statali și nestatali, să submineze democrația, economia și securitatea noastră. Este necesar să se prevină un peisaj fragmentat, deoarece o astfel de situație nu ar reprezenta o abordare adecvată, în special în fața unui viitor atac cibernetic la scară largă care vizează simultan mai multe state membre sau infrastructuri critice transnaționale. Prin urmare, este nevoie de un organ al Uniunii care să acționeze ca platformă de coordonare pentru toate instrumentele, fondurile și mecanismele de securitate cibernetică existente și viitoare.

Amendamentul 4

Propunere de regulament
Considerentul 3

Textul propus de Comisie	*Amendamentul*
(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate 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[16], este necesar să se sporească reziliența cetățenilor, a întreprinderilor 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 care	(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate 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[16], este necesar să se sporească reziliența cetățenilor, a întreprinderilor 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 care

vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică.

[16] https://futureu.europa.eu/ro/?locale=ro.

vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică***, precum și capacitatea sa de a acționa în mod proactiv și de a reacționa în mod decisiv în astfel de cazuri***.

[16] https://futureu.europa.eu/ro/?locale=ro.

Amendamentul 5

Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(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 materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea (UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile vizate, pentru a spori reziliența infrastructurii critice utilizate	(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 materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea (UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient ***și proactiv***, solidar și coordonat între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile vizate, pentru a spori reziliența infrastructurii

pentru a furniza servicii esențiale pe piața internă.

critice utilizate pentru a furniza servicii esențiale pe piața internă. ***În plus, în martie 2022, Uniunea a aprobat și a lansat Busola strategică pentru securitate și apărare, care se concentrează, printre altele, pe întărirea securității cibernetice și pe consolidarea cooperării internaționale cu aliații care împărtășesc aceeași viziune și cu partenerii democratici, în special în această privință. În plus, securitatea cibernetică a fost un punct central al celei de-a treia declarații comune privind cooperarea UE-NATO din ianuarie 2023. În plus, raportul final de evaluare al grupului operativ UE-NATO a recomandat utilizarea deplină a sinergiilor dintre UE și NATO[1], inclusiv schimbul de bune practici între actorii civili și militari cu privire la punerea în aplicare a politicilor și a legislației pertinente din domeniul cibernetic.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] 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).

[18] 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).

[19] 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).

[17] 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).

[18] 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).

[19] 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).

[20] 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).

[20] 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).

Amendamentul 6

Propunere de regulament
Considerentul 6

Textul propus de Comisie	*Amendamentul*
(6) Comunicarea comună privind politica UE în domeniul apărării cibernetice[22], adoptată la 10 noiembrie 2022, a anunțat o inițiativă a UE privind solidaritatea cibernetică cu următoarele obiective: consolidarea capabilităților 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”), sprijinirea creării treptate a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și testarea entităților critice în vederea identificării vulnerabilităților potențiale pe baza evaluărilor riscurilor la nivelul UE.	(6) Comunicarea comună privind politica UE în domeniul apărării cibernetice[22], adoptată la 10 noiembrie 2022, a anunțat o inițiativă a UE privind solidaritatea cibernetică cu următoarele obiective: consolidarea capabilităților 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”), sprijinirea creării treptate a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și testarea entităților critice în vederea identificării vulnerabilităților potențiale pe baza evaluărilor riscurilor la nivelul UE. ***În plus, evoluția rapidă a peisajului amenințărilor cibernetice și ritmul rapid al dezvoltării tehnologice demonstrează, de asemenea, necesitatea unei mai bune coordonări și cooperări civile și militare, astfel cum a subliniat Consiliul în concluziile sale privind politica UE în domeniul apărării cibernetice[1].*** ***[1] Concluziile Consiliului privind politica UE în domeniul apărării cibernetice aprobate de Consiliu în cadrul reuniunii***

	sale din 22 mai 2023, (9618/23).
[22] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.	[22] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.

Amendamentul 7

Propunere de regulament
Considerentul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	(6a) Având în vedere estomparea liniilor de demarcație dintre domeniul civil și cel militar și caracterul dual al instrumentelor și tehnologiilor cibernetice, este nevoie de o abordare cuprinzătoare și holistică a domeniului digital. În cazul unui incident și al unei crize de securitate cibernetică de mare amploare care implică mai multe state membre, ar trebui să se instituie o gestionare și o guvernare adecvate a crizelor. Aceste structuri ar trebui să organizeze schimbul de informații, coordonarea și cooperarea cu structurile de securitate externă și militare de gestionare a crizelor ale Uniunii, precum și cu organele statelor membre responsabile cu securitatea și apărarea (comunitatea de apărare cibernetică). Acest lucru ar trebui să se aplice, de asemenea, operațiunilor și misiunilor din cadrul politicii de securitate și apărare comune desfășurate de Uniune pentru a asigura pacea și stabilitatea în vecinătatea sa și dincolo de aceasta.

Amendamentul 8

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Este necesar să se consolideze detectarea și conștientizarea situației privind amenințările și incidentele de securitate cibernetică în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capabilităților statelor membre și ale Uniunii de a răspunde la incidentele de securitate cibernetică semnificative și de mare amploare. Prin urmare, ar trebui implementată o infrastructură paneuropeană de SOC (Scutul cibernetic european) pentru a crea și a consolida capabilitățile comune de detectare și de conștientizare a situației; ar trebui instituit un mecanism pentru situații de urgență cibernetică pentru a sprijini statele membre să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare***, să răspundă la acestea și să se redreseze imediat în urma lor***; ar trebui instituit un mecanism de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. Aceste acțiuni nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene („TFUE”).	(7) Este necesar să se consolideze detectarea și conștientizarea situației privind amenințările și incidentele de securitate cibernetică în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capabilităților statelor membre și ale Uniunii de a răspunde la incidentele de securitate cibernetică semnificative și de mare amploare. Prin urmare, ar trebui implementată o infrastructură paneuropeană de SOC (Scutul cibernetic european) pentru a crea și a consolida capabilitățile comune de detectare și de conștientizare a situației; ar trebui instituit un mecanism pentru situații de urgență cibernetică pentru a sprijini statele membre să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare***, inclusiv incidente care implică mai multe state membre***; ***Atunci când este fezabil și necesar, un mecanism pentru situații de urgență cibernetică ar trebui să organizeze schimbul de informații și cooperarea cu autoritățile de apărare ale statelor membre și să fie sprijinit de instituțiile, organele și agențiile UE (comunitatea de apărare cibernetică a UE)***; ar trebui instituit un mecanism de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. ***Astfel de structuri noi ar trebui, de asemenea, să sprijine operațiunile și misiunile PSAC ale UE.*** Aceste acțiuni nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene („TFUE”).

Amendamentul 9

Propunere de regulament
Considerentul 11

Textul propus de Comisie	*Amendamentul*
(11) În scopul bunei gestiuni financiare, ar trebui stabilite norme specifice pentru reportarea creditelor de angajament și de plată neutilizate. Respectând principiul potrivit căruia bugetul Uniunii este stabilit anual, prezentul regulament ar trebui să prevadă, având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice, posibilități de reportare a fondurilor neutilizate dincolo de cele prevăzute în Regulamentul financiar, maximizând astfel capacitatea mecanismului pentru situații de urgență cibernetică de a sprijini statele membre în combaterea eficace a amenințărilor cibernetice.	(11) În scopul bunei gestiuni financiare, ar trebui stabilite norme specifice pentru reportarea creditelor de angajament și de plată neutilizate. Respectând principiul potrivit căruia bugetul Uniunii este stabilit anual, prezentul regulament ar trebui să prevadă, având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice, posibilități de reportare a fondurilor neutilizate dincolo de cele prevăzute în Regulamentul financiar, maximizând astfel capacitatea mecanismului pentru situații de urgență cibernetică de a sprijini statele membre în combaterea eficace a amenințărilor cibernetice. ***Aceste norme specifice ar permite, de asemenea, acordarea de sprijin financiar pe termen mai lung pentru achizițiile publice comune de instrumente și infrastructuri foarte sigure de generație următoare, pentru a îmbunătăți capacitățile de detectare colectivă prin utilizarea celor mai recente tehnologii de inteligență artificială (IA) și de analiză a datelor.***

Amendamentul 10

Propunere de regulament
Considerentul 13

Textul propus de Comisie	*Amendamentul*
(13) Fiecare stat membru ar trebui să desemneze un organism public la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. Aceste SOC naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea la Scutul cibernetic european și ar trebui să se asigure că informațiile privind amenințările cibernetice provenite de la entități publice și private sunt partajate și	(13) Fiecare stat membru ar trebui să desemneze un organism public la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. Aceste SOC naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea la Scutul cibernetic european 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.

colectate la nivel național într-un mod eficace și raționalizat. ***Atunci când este fezabil și necesar, SOC ar trebui să permită, de asemenea, participarea entităților din domeniul apărării, instituind un „pilon al apărării” în ceea ce privește guvernarea și tipul de informații partajate, astfel cum se prevede în comunicarea comună privind politica UE în materie de apărare cibernetică[1] și cu sprijinul Înaltului Reprezentant.***

[1] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN/2022/49 final

Amendamentul 11

Propunere de regulament
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) În cadrul Scutului cibernetic european ar trebui înființate o serie de centre de operațiuni transfrontaliere în materie de securitate cibernetică („SOC transfrontaliere”). Acestea ar trebui să reunească SOC naționale din cel puțin trei state membre, astfel încât beneficiile detectării amenințărilor transfrontaliere și ale schimbului și gestionării informațiilor să poată fi realizate pe deplin. Obiectivul general al SOC transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor la adresa securității cibernetice și sprijinirea producerii de informații de înaltă calitate privind amenințările cibernetice, în special prin schimbul de date 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 capabilităților de detectare, analiză și prevenire într-un mediu de încredere. Acestea ar trebui să ofere noi capacități suplimentare, pe baza	(14) În cadrul Scutului cibernetic european ar trebui înființate o serie de centre de operațiuni transfrontaliere în materie de securitate cibernetică („SOC transfrontaliere”). Acestea ar trebui să reunească SOC naționale din cel puțin trei state membre, ***incluzând un „pilon al apărării”,*** astfel încât beneficiile detectării amenințărilor transfrontaliere și ale schimbului și gestionării informațiilor să poată fi realizate pe deplin. Obiectivul general al SOC transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor la adresa securității cibernetice și sprijinirea producerii de informații de înaltă calitate privind amenințările cibernetice, în special prin schimbul de date din diferite surse, publice sau private ***și, atunci când este necesar și fezabil, militare, cu orientări suficiente pentru schimbul de informații,*** precum și prin partajarea și utilizarea în comun a instrumentelor de ultimă generație și prin dezvoltarea în comun a

și în completarea SOC-urilor existente și a echipelor de intervenție în caz de incidente de securitate informatică („CSIRT”) și a altor actori relevanți.

capabilităților de detectare, analiză și prevenire într-un mediu de încredere. Acestea ar trebui să ofere noi capacități suplimentare, pe baza și în completarea SOC-urilor existente și a echipelor de intervenție în caz de incidente de securitate informatică („CSIRT”) și a altor actori relevanți.

Amendamentul 12

Propunere de regulament
Considerentul 15

Textul propus de Comisie	*Amendamentul*
(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a ***suveranității tehnologice ale*** Uniunii.	(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a ***rezilienței*** Uniunii.

Amendamentul 13

Propunere de regulament
Considerentul 16

Textul propus de Comisie	*Amendamentul*
(16) SOC-urile transfrontaliere ar trebui să acționeze ca un punct central care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind	(16) SOC-urile transfrontaliere ar trebui să acționeze ca un punct central care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind

amenințările cibernetice, să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de actori [de exemplu, echipe de intervenție în caz de urgență informatică („CERT”), CSIRT, centre de schimb de informații și de analiză („ISAC”), operatori de infrastructuri critice]. Informațiile schimbate între participanții la un SOC transfrontalier ar putea include date provenite de la rețele și senzori, fluxuri de informații privind amenințările cibernetice, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări și vulnerabilități. În plus, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere.

amenințările cibernetice, să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de actori [de exemplu, echipe de intervenție în caz de urgență informatică („CERT”), CSIRT, centre de schimb de informații și de analiză („ISAC”), operatori de infrastructuri critice]***, precum și comunitatea de apărare cibernetică***. Informațiile schimbate între participanții la un SOC transfrontalier ar putea include date provenite de la rețele și senzori, fluxuri de informații privind amenințările cibernetice, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări și vulnerabilități. În plus, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere ***și cu rețeaua operațională pentru milCERT (MICNET), atunci când va fi înființată***.

Amendamentul 14

Propunere de regulament
Considerentul 17

Textul propus de Comisie	*Amendamentul*
(17) 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 de mare amploare. Directiva (UE) 2022/2555 instituie 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 și agențiile Uniunii. Recomandarea (UE) 2017/1584 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare abordează rolul tuturor actorilor relevanți. Directiva (UE) 2022/2555	(17) 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 de mare amploare. Directiva (UE) 2022/2555 instituie 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 și agențiile Uniunii. Recomandarea (UE) 2017/1584 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare abordează rolul tuturor actorilor relevanți. Directiva (UE) 2022/2555

reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii („UCPM”) instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului, precum și de a furniza rapoarte analitice pentru mecanismul integrat pentru un răspuns politic la crize („IPCR”) în temeiul Deciziei de punere în aplicare (UE) 2018/1993. Prin urmare, în situațiile în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea ar trebui să furnizeze informații relevante către EU-CyCLONe, rețelei CSIRT și Comisiei. 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 în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.

reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii („UCPM”) instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului, precum și de a furniza rapoarte analitice pentru mecanismul integrat pentru un răspuns politic la crize („IPCR”) în temeiul Deciziei de punere în aplicare (UE) 2018/1993. Prin urmare, în situațiile în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea ar trebui să furnizeze informații relevante către EU-CyCLONe, rețelei CSIRT***, comunității de apărare cibernetică*** și Comisiei. 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 în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.

Amendamentul 15

Propunere de regulament
Considerentul 19

Textul propus de Comisie	*Amendamentul*
(19) Pentru a permite schimbul de date privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere, entitățile care participă la Scutul cibernetic european ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate. Acest lucru ar trebui să permită îmbunătățirea capacităților de detectare colectivă și avertizarea în timp util a autorităților și a entităților relevante,	(19) Pentru a permite schimbul de date privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere, entitățile care participă la Scutul cibernetic european ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate***, excluzând furnizorii de mare risc de produse critice cu elemente digitale***. Acest lucru ar trebui să permită îmbunătățirea capacităților de detectare

în special prin utilizarea celor mai recente tehnologii de inteligență artificială și de analiză a datelor.	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. ***Utilizarea IA ar trebui să fie supusă supravegherii umane, iar persoanele care exercită această funcție ar trebui să dispună de un nivel suficient de cunoștințe în domeniul IA, precum și de sprijinul și de autoritatea necesare.***

Amendamentul 16

Propunere de regulament
Considerentul 19 a (nou)

Textul propus de Comisie	*Amendamentul*
	(19a) În concordanță cu Regulamentul [XX/XXXX (Actul privind reziliența cibernetică)], entitățile care participă la Scutul cibernetic european ar trebui să îndeplinească, de asemenea, cerințele prevăzute în prezentul regulament pentru toate produsele cu elemente digitale. Având în vedere riscurile tot mai mari generate de dependențele economice, este necesar să se reducă la minimum expunerea la furnizorii cu risc ridicat de produse critice, prin intermediul unui cadru strategic comun pentru securitatea economică a UE. Dependențele de furnizorii cu grad ridicat de risc de produse critice cu elemente digitale prezintă un risc strategic care ar trebui abordat la nivelul Uniunii, în special dacă o țară se angajează în spionaj economic sau în constrângere economică, iar legislația sa impune accesul arbitrar la orice tip de operațiuni sau date ale întreprinderii, în special atunci când produsele critice sunt destinate utilizării de către entitățile esențiale menționate în Directiva (UE) 2022/2555.

Amendamentul 17

Propunere de regulament
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) Prin colectarea, partajarea și schimbul de date, Scutul cibernetic european ar trebui să consolideze suveranitatea tehnologică a Uniunii. Punerea în comun a datelor actualizate de înaltă calitate ar trebui să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. Aceasta ar trebui facilitată prin conectarea Scutului cibernetic european cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173 al Consiliului[25].	(20) Prin colectarea, partajarea și schimbul de date, Scutul cibernetic european ar trebui să consolideze suveranitatea tehnologică a Uniunii***, autonomia, competitivitatea și reziliența strategice ale sale***. Punerea în comun a datelor actualizate de înaltă calitate ar trebui să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. Aceasta ar trebui facilitată prin conectarea Scutului cibernetic european cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173 al Consiliului[25].
[25] Regulamentul (UE) 2021/1173 al Consiliului din 13 iulie 2021 privind instituirea întreprinderii comune pentru calculul european de înaltă performanță și de abrogare a Regulamentului (UE) 2018/1488 (JO L 256, 19.7.2021, p. 3).	[25] Regulamentul (UE) 2021/1173 al Consiliului din 13 iulie 2021 privind instituirea întreprinderii comune pentru calculul european de înaltă performanță și de abrogare a Regulamentului (UE) 2018/1488 (JO L 256, 19.7.2021, p. 3).

Amendamentul 18

Propunere de regulament
Considerentul 25

Textul propus de Comisie	*Amendamentul*
(25) Mecanismul pentru situații de urgență 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 de mare amploare și al redresării imediate în urma acestora, cum ar fi serviciile furnizate de Agenția Uniunii Europene pentru Securitate Cibernetică	(25) Mecanismul pentru situații de urgență 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 de mare amploare și al redresării imediate în urma acestora, cum ar fi serviciile furnizate de Agenția Uniunii Europene pentru Securitate Cibernetică

(„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 PESCO[26] și echipele de răspuns rapid în caz de amenințări hibride. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea incidentelor de securitate cibernetică în întreaga Uniune și în țările terțe și răspunsul la acestea.

[26] 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.

(„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 PESCO***[1], noul Centru de coordonare a domeniului de informații cibernetice (CIDCC) al proiectului PESCO și succesorul său propus, Centrul de coordonare a apărării cibernetice al UE (EUCDCC)*** și echipele de răspuns rapid în caz de amenințări hibride. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea incidentelor de securitate cibernetică în întreaga Uniune și în țările terțe și răspunsul la acestea***, îndeosebi în țările candidate la UE aliniate la politica externă și de securitate comună și la politica de securitate și apărare comună ale UE, sprijinindu-le în dezvoltarea capacităților lor cibernetice și consolidând cooperarea transfrontalieră și regională între aceste țări candidate în domeniul cibernetic.***

[1] 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.

[26] 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.

Amendamentul 19

Propunere de regulament
Considerentul 26

Textul propus de Comisie	*Amendamentul*
(26) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[27], IPCR[28], și Directivei (UE) 2022/2555. Acesta poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE sau în situațiile definite la articolul 222 din TFUE sau poate completa aceste acțiuni. Utilizarea acestui instrument ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, ***după caz***.	(26) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[27], IPCR[28], și Directivei (UE) 2022/2555. Acesta poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE sau în situațiile definite la articolul 222 din TFUE sau poate completa aceste acțiuni. Utilizarea acestui instrument ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, ***consolidând cooperarea la nivel strategic, operațional și tehnic între apărarea cibernetică și alte comunități cibernetice, în special în vederea consolidării capacităților împotriva amenințărilor la adresa securității cibernetice din afara Uniunii, inclusiv a măsurilor restrictive, care pot fi utilizate pentru a preveni și a răspunde la activitățile cibernetice rău intenționate***.
[27] 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).	[27] 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).
[28] Mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.	[28] Mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

Amendamentul 20

Propunere de regulament
Considerentul 28

Textul propus de Comisie	*Amendamentul*
(28) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să înființeze 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 înființa una sau mai multe 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 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 de mare amploare, pentru a sprijini redresarea imediată și/sau pentru a restabili funcționarea serviciilor esențiale.	(28) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să înființeze 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 înființa una sau mai multe 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 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 de mare amploare, pentru a sprijini redresarea imediată și/sau pentru a restabili funcționarea serviciilor esențiale***, utilizând în mod corespunzător întreaga gamă de opțiuni defensive aflate la dispoziția comunităților civile și militare***.

Amendamentul 21

Propunere de regulament
Considerentul 29

Textul propus de Comisie	*Amendamentul*
(29) 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 deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. ***Sectoarele sau subsectoarele*** ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de testare coordonată 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, care urmează să fie efectuate de Comisie, de 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	(29) 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 deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. ***Atunci când este cazul, Serviciul European de Acțiune Externă (SEAE), în special prin intermediul Centrului de informații al UE (INTCEN) și al Celulei sale de fuziune împotriva amenințărilor hibride, cu sprijinul Direcției de informații a Statului-Major al Uniunii Europene (EUMS) din cadrul Capacității unice de analiză a informațiilor (SIAC), ar trebui, de asemenea, să fie asociat pentru a furniza evaluări actualizate și, astfel, să contribuie la identificarea sectoarelor sau a subsectoarelor care*** ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de testare coordonată ar trebui să se bazeze pe scenarii și metodologii de risc comune. ***Aceste exerciții ar trebui să joace, de asemenea, un rol important în îmbunătățirea cooperării dintre entitățile civile și militare. Prin urmare, atunci când organizează exerciții, Comisia, SEAE și ENISA ar trebui să ia în considerare în mod sistematic includerea participanților din alte comunități***

Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), de evaluările coordonate ale riscurilor 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) 2022/2554 al Parlamentului European și al Consiliului[29]. 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.

cibernetice, cum ar fi Agenția Europeană de Apărare (AEA) și alte entități pertinente. 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, care urmează să fie efectuate de Comisie, de 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 (OAREC), de evaluările coordonate ale riscurilor 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) 2022/2554 al Parlamentului European și al Consiliului***[1]***. 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.

[1] 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.

---

[29] Regulamentul (UE) 2022/2554 al

---

[29] 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.	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.

Amendamentul 22

Propunere de regulament
Considerentul 32

Textul propus de Comisie	*Amendamentul*
(32) Mecanismul pentru situații de urgență cibernetică ar trebui să sprijine asistența acordată de statele membre, inclusiv de rețeaua CSIRT prevăzută la articolul 15 din Directiva (UE) 2022/2555, unui stat membru afectat de un incident de securitate cibernetică semnificativ sau de mare amploare. Statele membre care acordă 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.	(32) Mecanismul pentru situații de urgență cibernetică ar trebui să sprijine asistența acordată de statele membre, inclusiv de rețeaua CSIRT prevăzută la articolul 15 din Directiva (UE) 2022/2555, unui stat membru afectat de un incident de securitate cibernetică semnificativ sau de mare amploare. Statele membre care acordă asistență ar trebui să aibă posibilitatea de a depune cereri pentru a acoperi costurile legate de trimiterea echipelor de experți în cadrul asistenței reciproce***, asigurând o coordonare eficientă între programele și instrumentele pertinente ale UE, printre care Instrumentul european pentru pace (IEP), PESC și IVCDCI, atunci când acordă asistență țărilor terțe, în special Ucrainei și Moldovei.*** Costurile eligibile ar putea include cheltuielile de deplasare, cazare și diurnă ale experților în securitate cibernetică.

Amendamentul 23

Propunere de regulament
Considerentul 33

Textul propus de Comisie	*Amendamentul*
(33) Ar trebui instituită treptat o rezervă de securitate cibernetică la nivelul Uniunii,	(33) Ar trebui instituită treptat o rezervă de securitate cibernetică la nivelul Uniunii,

care să constea în servicii furnizate de furnizori privați de servicii de securitate gestionate pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor. 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 critice sau deosebit de critice, în completarea propriilor acțiuni la nivel național. Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, statele membre ar trebui să specifice sprijinul acordat entității afectate la nivel național, care ar trebui luat în considerare atunci când se evaluează cererea statului membru. Serviciile din rezerva UE pentru securitate cibernetică pot servi, de asemenea, la sprijinirea instituțiilor, a organelor și a agențiilor Uniunii, în condiții similare.	care să constea în servicii furnizate de furnizori privați de servicii de securitate gestionate pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor. 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 critice sau deosebit de critice, în completarea propriilor acțiuni la nivel național. Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, statele membre ar trebui să specifice sprijinul acordat entității afectate la nivel național, care ar trebui luat în considerare atunci când se evaluează cererea statului membru. Serviciile din rezerva UE pentru securitate cibernetică pot servi, de asemenea, la sprijinirea instituțiilor, a organelor și a agențiilor Uniunii, ***inclusiv a misiunilor PSAC,*** în condiții similare.

Amendamentul 24

Propunere de regulament
Considerentul 34

Textul propus de Comisie	*Amendamentul*
(34) 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 care ar trebui incluse în cererea de oferte pentru selectarea acestor furnizori, astfel încât să se asigure că sunt îndeplinite nevoile autorităților și entităților din statele membre care își desfășoară activitatea în sectoare critice sau deosebit de critice.	(34) 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 care ar trebui incluse în cererea de oferte pentru selectarea acestor furnizori, astfel încât să se asigure că sunt îndeplinite nevoile autorităților și entităților din statele membre care își desfășoară activitatea în sectoare critice sau deosebit de critice***, luând în considerare, de asemenea, riscurile asociate participării furnizorilor***

din țările concurente strategice, care pot genera riscuri de securitate economică, precum și implicațiile pentru securitatea strategică a Uniunii.

Amendamentul 25

Propunere de regulament
Considerentul 36

Textul propus de Comisie	*Amendamentul*
(36) 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 de mare amploare, EU-CyCLONe, rețeaua CSIRT sau Comisia ar trebui să poată solicita ENISA să revizuiască și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de examinare a incidentelor, în colaborare cu părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ai statelor membre, ai Comisiei și ai altor instituții, organisme și agenții relevante ale UE. În ceea ce privește sectorul privat, ENISA dezvoltă canale pentru schimbul de informații cu furnizorii specializați, inclusiv cu furnizorii de soluții de securitate gestionate și cu vânzătorii, pentru a contribui la misiunea ENISA de a atinge un nivel comun ridicat de securitate cibernetică în întreaga Uniune. Pe baza colaborării cu părțile interesate, inclusiv cu sectorul privat, raportul de examinare 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	(36) 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 de mare amploare, EU-CyCLONe, rețeaua CSIRT sau Comisia ar trebui să poată solicita ENISA să revizuiască și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau de mare amploare. ***În vederea dezvoltării unui sistem de conectivitate securizat, bazat pe infrastructura europeană de comunicații cuantice (EuroQCI) și pe programul de comunicare guvernamentală prin satelit a Uniunii Europene (GOVSATCOM), îndeosebi pe punerea în aplicare a GNSS GALILEO pentru utilizatorii din domeniul apărării, orice eventuală dezvoltare viitoare ar trebui să ia în considerare apariția "hiperrăzboiului", care îmbină viteza și sofisticarea informaticii cuantice cu sisteme militare extrem de autonome.*** După finalizarea unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de examinare a incidentelor, în colaborare cu părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ai statelor membre, ai Comisiei și ai altor instituții, organisme și agenții relevante ale UE. În ceea ce privește sectorul privat, ENISA dezvoltă canale

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 rețelelor EU-CyCLONe și CSIRT și Comisiei și să contribuie a activitatea acestora. În cazul în care incidentul se referă la o țară terță, acesta va fi, de asemenea, transmis de către Comisie Înaltului Reprezentant.

pentru schimbul de informații cu furnizorii specializați, inclusiv cu furnizorii de soluții de securitate gestionate și cu vânzătorii, pentru a contribui la misiunea ENISA de a atinge un nivel comun ridicat de securitate cibernetică în întreaga Uniune. Pe baza colaborării cu părțile interesate, inclusiv cu sectorul privat, raportul de examinare 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 rețelelor EU-CyCLONe și CSIRT și Comisiei și să contribuie a activitatea acestora. În cazul în care incidentul se referă la o țară terță, acesta va fi, de asemenea, transmis de către Comisie Înaltului Reprezentant***, SEAE și oricărei misiuni PSAC din țara afectată de incident, prin intermediul sediului lor central***.

Amendamentul 26

Propunere de regulament
Considerentul 37

Textul propus de Comisie	*Amendamentul*
(37) Având în vedere caracterul imprevizibil al atacurilor de securitate cibernetică 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 de mare amploare contribuie la protecția Uniunii în ansamblu. Prin urmare, țările terțe asociate la DEP ***pot fi*** sprijinite din rezerva UE	(37) Având în vedere caracterul imprevizibil al atacurilor de securitate cibernetică și faptul că, adesea, acestea nu sunt limitate la o anumită zonă geografică și prezintă un risc ridicat de propagare, consolidarea rezilienței țărilor învecinate***, îndeosebi Ucraina și Moldova,*** și a capacității lor de a răspunde în mod eficace la incidentele de securitate cibernetică semnificative și de mare amploare contribuie la protecția Uniunii în ansamblu. Prin urmare, țările terțe asociate la DEP ***ar***

pentru securitate cibernetică***, în cazul în care acest lucru este prevăzut în acordul de asociere la DEP respectiv***. Finanțarea pentru țările terțe asociate 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 de mare amploare și al redresării imediate în urma acestora. Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP.

trebui să fie sprijinite din rezerva UE pentru securitate cibernetică***. Sprijinul ar trebui să se aplice, de asemenea, țărilor terțe în care este desfășurată o misiune PSAC cu un mandat specific de întărire a rezilienței la amenințările hibride, inclusiv cele cibernetice, sau în care a fost adoptată o măsură de asistență a IEP pentru a întări reziliența cibernetică a țării***. Finanțarea pentru țările terțe asociate 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 de mare amploare și al redresării imediate în urma acestora. Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP.

Amendamentul 27

Propunere de regulament
Articolul 1 – alineatul 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) instituirea unui mecanism european de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare.	(c) instituirea unui mecanism european de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele ***sau amenințările*** semnificative sau de mare amploare.

Amendamentul 28

Propunere de regulament
Articolul 1 – alineatul 2 – litera a

Textul propus de Comisie	*Amendamentul*
(a) de a consolida detectarea și conștientizarea comună a situației la	(a) de a consolida detectarea și conștientizarea comună a situației la

nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la ***suveranitatea*** tehnologică a Uniunii în domeniul securității cibernetice;	nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la ***reziliența*** tehnologică a Uniunii în domeniul securității cibernetice;

Amendamentul 29

Propunere de regulament
Articolul 1 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) a sprijinului din partea UE pentru răspunsul la incidentele de securitate cibernetică;	(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) ***sau a țărilor terțe care sunt candidate la aderare și care nu contravin intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în conformitate cu titlul V din TUE; Statele membre ar trebui să considere că un program activ de apărare cibernetică face parte din strategia lor națională în materie de securitate cibernetică, care include exerciții de instruire comune periodice între statele membre și între organizațiile internaționale. Un astfel de program ar trebui să ofere o capacitate în timp real, sincronizată, de a descoperi, detecta, analiza și atenua amenințările***;

Amendamentul 30

Propunere de regulament
Articolul 1 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. să reducă riscurile sistemice în materie de securitate cibernetică reprezentate de dependențele de echipamente critice din țări care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE;.

Amendamentul 31

Propunere de regulament
Articolul 2 – punctul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	„comunitate de apărare cibernetică” înseamnă autoritățile de apărare ale statelor membre și sprijinite de instituțiile, organismele și agențiile UE, astfel cum se prevede în comunicarea comună privind politica UE în domeniul apărării cibernetice[1];
	[1] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN/2022/49 final

Amendamentul 32

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 1 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	(ba) să contribuie la modernizarea întregului sistem de apărare cibernetică, îmbunătățind calitatea capacităților de

	apărare cibernetică prin implementarea sistemelor de IA și să accelereze schimbul de informații între SOC naționale și SOC transfrontaliere;

Amendamentul 33

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 1 – litera da (nouă)

Textul propus de Comisie	*Amendamentul*
	(da) să examineze și să evalueze tehnologiile și echipamentele critice de securitate cibernetică utilizate de SOC pentru a răspunde la incidentele de securitate cibernetică în ceea ce privește riscurile sistemice generate de controlul exercitat de țări asupra furnizorilor cu risc ridicat, care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE.

Amendamentul 34

Propunere de regulament
Articolul 4 – alineatul 1 – paragraful 2

Textul propus de Comisie	*Amendamentul*
Acesta 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 și incidentele de securitate cibernetică și pentru contribuția la un SOC transfrontalier. Acesta este echipat cu tehnologii de ultimă generație capabile să detecteze, să reunească și să analizeze datele relevante pentru amenințările și incidentele de securitate cibernetică.	Acesta are capacitatea de a acționa ca punct de referință și punct de acces către alte organizații publice și private ***și, după caz, militar,*** de la nivel național pentru colectarea și analizarea informațiilor privind amenințările și incidentele de securitate cibernetică și pentru contribuția la un SOC transfrontalier. Acesta este echipat cu tehnologii de ultimă generație capabile să detecteze, să reunească și să analizeze datele relevante pentru amenințările și incidentele de securitate cibernetică.

Amendamentul 35

Propunere de regulament
Articolul 4 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. În urma unei cereri de exprimare a interesului, SOC naționale sunt selectate de către Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) pentru a participa la o achiziție de instrumente și infrastructuri în comun cu ECCC. ECCC poate acorda granturi SOC-urilor naționale selectate pentru a finanța funcționarea acestor instrumente și infrastructuri. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de statul membru. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și SOC național încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.	2. În urma unei cereri de exprimare a interesului, SOC naționale sunt selectate de către Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) pentru a participa la o achiziție de instrumente și infrastructuri în comun cu ECCC. ECCC poate acorda granturi SOC-urilor naționale selectate pentru a finanța funcționarea acestor instrumente și infrastructuri***, cu condiția strictă ca astfel de instrumente și infrastructuri să fie furnizate de furnizori de încredere în conformitate cu articolul 16***. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de statul membru. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și SOC național încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

Amendamentul 36

Propunere de regulament
Articolul 5 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. În urma unei cereri de exprimare a interesului, un consorțiu-gazdă este selectat de către ECCC pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor și a	2. În urma unei cereri de exprimare a interesului, un consorțiu-gazdă este selectat de către ECCC pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor și a

infrastructurilor. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de către consorțiul-gazdă. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.	infrastructurilor***, cu condiția strictă ca astfel de instrumente și infrastructuri să fie furnizate de furnizori de încredere în conformitate cu articolul 16***. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de către consorțiul-gazdă. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

Amendamentul 37

Propunere de regulament
Articolul 5 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Orice infrastructură sau furnizor originar dintr-o țară terță cu grad ridicat de risc este exclus în mod automat.

Amendamentul 38

Propunere de regulament
Articolul 6 – alineatul 1 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	***(ba) sprijină în mod direct întărirea capacităților militare și de apărare ale membrilor participanți sau împiedică o amenințare directă și iminentă la adresa securității acestora. Deși exploatarea vulnerabilităților din sectorul apărării poate cauza perturbări și daune semnificative, securitatea cibernetică a sectorului apărării necesită măsuri speciale pentru a asigura securitatea lanțurilor de aprovizionare, îndeosebi a entităților aflate în poziții inferioare în lanțurile de aprovizionare, care nu**

	necesită acces la informații clasificate, dar care ar putea prezenta riscuri grave pentru întregul sector. Ar trebui să se acorde o atenție deosebită impactului oricărei încălcări și amenințării cu o eventuală manipulare a datelor de rețea care ar putea face ca mijloacele de apărare esențiale să devină inutile sau chiar să le neutralizeze sistemele de operare, făcându-le vulnerabile la acte de piraterie.

Amendamentul 39

Propunere de regulament
Articolul 6 – alineatul 1 – litera bb (nouă)

Textul propus de Comisie	*Amendamentul*
	(bb) sprijină întărirea capacităților de apărare ale membrilor participanți sau împiedică o amenințare directă și iminentă la adresa securității acestora, asigurând securitatea lanțurilor de aprovizionare, în special a acelor entități aflate la un nivel inferior în lanțurile de aprovizionare, care nu necesită acces la informații clasificate, dar care ar putea implica riscuri grave pentru întregul sector.

Amendamentul 40

Propunere de regulament
Articolul 7 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În cazul în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea furnizează, fără întârzieri nejustificate, informații relevante rețelelor EU-CyCLONe și CSIRT și Comisiei, având în vedere rolurile lor respective de gestionare a crizelor în conformitate cu	1. În cazul în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea furnizează, fără întârzieri nejustificate, informații relevante rețelelor EU-CyCLONe și CSIRT și Comisiei, ***inclusiv Înaltului Reprezentant și SEAE atunci când se referă la o țară terță,*** având

Directiva (UE) 2022/2555.	în vedere rolurile lor respective de gestionare a crizelor în conformitate cu Directiva (UE) 2022/2555.

Amendamentul 41

Propunere de regulament
Articolul 8 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre care participă la Scutul cibernetic european asigură un nivel ridicat de securitate a datelor și de securitate fizică a infrastructurii Scutului cibernetic european și se asigură că infrastructura 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 schimbate prin intermediul infrastructurii.	1. Statele membre care participă la Scutul cibernetic european asigură un nivel ridicat de securitate a datelor și de securitate fizică a infrastructurii Scutului cibernetic european și se asigură că infrastructura este gestionată și controlată în mod adecvat, astfel încât să fie protejată de amenințări și să se garanteze securitatea sa și a sistemelor, ***reducerea riscurilor și promovarea avantajului tehnologic al UE în sectoarele critice,*** inclusiv ***măsuri de restricționare sau excludere a furnizorilor cu grad ridicat de risc, precum și de protejare a securității*** datelor schimbate prin intermediul infrastructurii.

Amendamentul 42

Propunere de regulament
Articolul 8 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Statele membre care participă la Scutul cibernetic european se asigură că schimbul de informații în cadrul Scutului cibernetic european cu entități care nu sunt organisme publice ale statelor membre nu afectează în mod negativ interesele de securitate ale Uniunii.	2. Statele membre care participă la Scutul cibernetic european se asigură că schimbul de informații în cadrul Scutului cibernetic european cu entități care nu sunt organisme publice ale statelor membre nu afectează în mod negativ interesele de securitate ale Uniunii ***și că orice schimb de informații cu furnizorii cu grad ridicat de risc are un domeniu de aplicare limitat și nu aduce atingere intereselor strategice și de securitate ale Uniunii***.

Amendamentul 43

Propunere de regulament
Articolul 8 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice pentru ca statele membre să își respecte obligațiile care le revin în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament. În acest sens, Comisia, sprijinită de Înaltul Reprezentant, ține seama de standardele de securitate relevante la nivel de apărare, pentru a facilita cooperarea cu actorii militari.	3. Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice pentru ca statele membre să își respecte obligațiile care le revin în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament. În acest sens, Comisia, sprijinită de Înaltul Reprezentant, ține seama de standardele de securitate relevante la nivel de apărare, pentru a facilita cooperarea cu actorii militari***, utilizând în mod adecvat întreaga gamă de opțiuni defensive aflate la dispoziția comunităților civile și militare pentru securitatea și apărarea mai largă a UE, și informează Parlamentul European***.

Amendamentul 44

Propunere de regulament
Articolul 9 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Acțiunile de punere în aplicare a mecanismului pentru situații de urgență 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.	2. Acțiunile de punere în aplicare a mecanismului pentru situații de urgență 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***, și prin Instrumentul european pentru pace (IEP), atunci când furnizează măsuri de asistență țărilor terțe, îndeosebi Ucrainei și Moldovei;***

Amendamentul 45

Propunere de regulament

Articolul 10 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice în cadrul Uniunii;	(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice***, cum ar fi infrastructura publică, infrastructura electorală, transporturile, asistența medicală, finanțele, telecomunicațiile, aprovizionarea cu alimente și securitatea*** în cadrul Uniunii;

Amendamentul 46

Propunere de regulament
Articolul 10 – alineatul 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) acțiuni de asistență reciprocă constând în furnizarea de asistență din partea autorităților naționale ale unui stat membru unui alt stat membru, în special astfel cum se prevede la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555.	(c) acțiuni de asistență reciprocă constând în furnizarea de asistență din partea autorităților naționale ale unui stat membru unui alt stat membru, în special astfel cum se prevede la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555 ***și în contextul articolului 42 alineatul (7) din TUE și al articolului 222 din TFUE;***

Amendamentul 47

Propunere de regulament
Articolul 10 – alineatul 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) înlocuirea și eliminarea treptată a echipamentelor critice provenite de la furnizorii cu risc ridicat, ceea ce ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE;

Amendamentul 48

Propunere de regulament
Articolul 11 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Grupul de cooperare NIS, în colaborare cu Comisia, ENISA ***și*** Înaltul Reprezentant, elaborează scenarii de risc și metodologii comune pentru exercițiile de testare coordonate.	2. Grupul de cooperare NIS, în colaborare cu Comisia, ENISA***,*** Înaltul Reprezentant, ***SEAE și, după caz, AEA,*** elaborează scenarii de risc și metodologii comune pentru exercițiile de testare coordonate.

Amendamentul 49

Propunere de regulament
Articolul 12 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Rezerva UE pentru securitate cibernetică constă în servicii de răspuns la incidente furnizate de furnizori de încredere selectați în conformitate cu criteriile prevăzute la articolul 16. Rezerva include servicii angajate în prealabil. Serviciile trebuie să poată fi desfășurate în toate statele membre.	2. Rezerva UE pentru securitate cibernetică constă în servicii de răspuns la incidente furnizate de furnizori de încredere selectați în conformitate cu criteriile prevăzute la articolul 16. Rezerva include servicii angajate în prealabil. Serviciile trebuie să poată fi desfășurate în toate statele membre ***și în țările terțe care îndeplinesc cerințele aplicabile ale prezentului regulament***.

Amendamentul 50

Propunere de regulament
Articolul 12 – alineatul 3 – litera b

Textul propus de Comisie	*Amendamentul*
(b) instituțiile, organele și agențiile Uniunii.	(b) instituțiile, organele și agențiile Uniunii***, inclusiv misiunile PSAC***.

Amendamentul 51

Propunere de regulament
Articolul 12 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Utilizatorii menționați la alineatul (3) litera (a) utilizează serviciile din rezerva UE pentru securitate cibernetică pentru a răspunde sau a oferi sprijin pentru răspunsul la incidentele semnificative sau de mare amploare care afectează entitățile care își desfășoară activitatea în sectoare critice sau deosebit de critice ***și pentru redresarea imediată în urma acestora***.	4. Utilizatorii menționați la alineatul (3) litera (a) utilizează serviciile din rezerva UE pentru securitate cibernetică pentru a răspunde sau a oferi sprijin pentru răspunsul la incidentele semnificative sau de mare amploare care afectează entitățile care își desfășoară activitatea în sectoare critice sau deosebit de critice***, precum infrastructura publică, infrastructura electorală, transporturile, asistența medicală, finanțele, telecomunicațiile, aprovizionarea cu alimente și securitatea***.

Amendamentul 52

Propunere de regulament
Articolul 12 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. 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 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.	5. 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 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***,*** programe ***și obiective*** ale Uniunii***, în special obiectivul strategic de reducere a dependenței de furnizorii cu risc ridicat, care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE***.

Amendamentul 53

Propunere de regulament
Articolul 12 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. Pentru a sprijini Comisia în instituirea rezervei UE pentru securitate cibernetică, ENISA elaborează o cartografiere a serviciilor necesare, după consultarea statelor membre și a Comisiei. ENISA elaborează o cartografiere similară, după consultarea Comisiei, pentru a identifica nevoile țărilor terțe eligibile pentru sprijin din rezerva UE pentru securitate cibernetică în temeiul articolului 17. După caz, Comisia consultă Înaltul Reprezentant.	7. Pentru a sprijini Comisia în instituirea rezervei UE pentru securitate cibernetică, ENISA elaborează o cartografiere a serviciilor necesare, după consultarea statelor membre și a Comisiei. ENISA elaborează o cartografiere similară, după consultarea Comisiei, pentru a identifica nevoile țărilor terțe eligibile pentru sprijin din rezerva UE pentru securitate cibernetică în temeiul articolului 17***, cu sprijinul SEAE***. După caz, Comisia consultă Înaltul Reprezentant.

Amendamentul 54

Propunere de regulament
Articolul 14 – alineatul 2 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) impactul incidentului asupra securității și a apărării Uniunii;

Amendamentul 55

Propunere de regulament
Articolul 15 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. În consultare cu Înaltul Reprezentant, sprijinul acordat în cadrul mecanismului pentru situații de urgență 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. De asemenea, acesta poate completa asistența acordată de un	3. În consultare cu Înaltul Reprezentant, sprijinul acordat în cadrul mecanismului pentru situații de urgență 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 ***(CRRT), cu scopul de a sprijini mai bine statele membre ale UE,***

stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană sau poate contribui la aceasta.	***misiunile și operațiunile PSAC și țările terțe aliniate la politica externă și de securitate comună a UE și la politica de securitate și apărare comună în eforturile lor de consolidare a capacităților de apărare cibernetică, îndeosebi Ucraina și Moldova***. De asemenea, acesta poate completa asistența acordată de un stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană sau poate contribui la aceasta.

Amendamentul 56

Propunere de regulament
Articolul 16 – alineatul 2 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) furnizorul demonstrează că structurile sale decizionale și de gestionare nu sunt supuse niciunei influențe necuvenite din partea guvernelor statelor, ceea ce ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum se prevede în cadrul PESC în temeiul titlului V din TUE;

Amendamentul 57

Propunere de regulament
Articolul 16 – alineatul 2 – litera f

Textul propus de Comisie	*Amendamentul*
(f) furnizorul este dotat cu echipamentele tehnice hardware și software necesare pentru a sprijini serviciul solicitat;	(f) furnizorul este dotat cu echipamentele tehnice hardware și software necesare pentru a sprijini serviciul solicitat ***și îndeplinește cerințele prevăzute la articolul X din Regulamentul XX/XXXX (Actul privind reziliența cibernetică)***;

Amendamentul 58

Propunere de regulament
Articolul 16 – alineatul 2 – litera ja (nouă)

Textul propus de Comisie	*Amendamentul*
	(ja) Nu poate fi admis niciun furnizor originar dintr-o țară terță cu grad ridicat de risc.

Amendamentul 59

Propunere de regulament
Articolul 16 – alineatul 2 – litera jb (nouă)

Textul propus de Comisie	*Amendamentul*
	(jb) furnizorul este în strânsă cooperare cu IMM-urile relevante, dacă este posibil;

Amendamentul 60

Propunere de regulament
Articolul 17 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Țările terțe pot solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care acordurile de asociere încheiate cu privire la participarea lor la DEP prevăd acest lucru.	1. Țările terțe pot solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care***:***
	(a) acordurile de asociere încheiate cu privire la participarea lor la DEP prevăd acest lucru***;***
	(b) țările terțe în care este desfășurată o misiune PSAC cu un mandat specific pentru a întări reziliența la amenințările hibride, inclusiv cele cibernetice, sau în care a fost adoptată o măsură de asistență a IEP pentru a întări reziliența cibernetică a țării.

Amendamentul 61

Propunere de regulament
Articolul 17 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Sprijinul din rezerva UE pentru securitate cibernetică este în conformitate cu prezentul regulament și respectă toate condițiile specifice prevăzute în acordurile de asociere menționate la ***alineatul (1)***.	2. Sprijinul din rezerva UE pentru securitate cibernetică este în conformitate cu prezentul regulament și respectă toate condițiile specifice prevăzute în acordurile de asociere menționate la ***alineat***, ***cu excepția țărilor terțe care fac obiectul dispozițiilor prevăzute la alineatul (1) litera (b)***.

Amendamentul 62

Propunere de regulament
Articolul 18 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA analizează și evaluează amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA transmite rețelei CSIRT, EU-CyCLONe și Comisiei un raport de evaluare a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, având-le în vedere în special pe cele prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. Dacă este cazul, Comisia transmite raportul Înaltului Reprezentant.	1. La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA analizează și evaluează amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA transmite rețelei CSIRT, EU-CyCLONe și Comisiei un raport de evaluare a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, având-le în vedere în special pe cele prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. Dacă este cazul, ***în special atunci când incidentul se referă la o țară terță,*** Comisia transmite raportul Înaltului Reprezentant ***și SEAE***.

Amendamentul 63

Propunere de regulament
Articolul 18 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. Raportul este transmis Parlamentului European în concordanță cu dreptul Uniunii sau cu dreptul intern în domeniul protecției informațiilor sensibile clasificate.

Amendamentul 64

Propunere de regulament
Articolul 19 – paragraful 1 – punctul 1 – litera a – punctul 1 (nou)
Regulamentului (UE) 2021/694
Articolul 6 – alineatul 1

Textul propus de Comisie	*Amendamentul*
(aa) sprijinirea dezvoltării unui Scut cibernetic al UE, inclusiv dezvoltarea, implementarea și operarea platformelor SOC naționale și transfrontaliere care contribuie la conștientizarea situației în Uniune și la consolidarea capacităților de informații privind amenințările cibernetice ale Uniunii;	(aa) sprijinirea dezvoltării unui Scut cibernetic al UE, inclusiv dezvoltarea, implementarea și operarea platformelor SOC naționale și transfrontaliere care contribuie la conștientizarea situației în Uniune și la consolidarea capacităților de informații privind amenințările cibernetice ale Uniunii ***și reducerea dependenței Uniunii de furnizorii cu grad ridicat de risc de echipamente sau componente critice de securitate cibernetică care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în conformitate cu titlul V din TUE***;

Amendamentul 65

Propunere de regulament
Articolul 20 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Până la [***patru*** ani de la data de la care se aplică prezentul regulament] Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament.	Până la [***trei*** ani de la data de la care se aplică prezentul regulament ***și, ulterior, o dată la doi ani***], Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea

prezentului regulament.

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Stabilirea 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
Referințe	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Comisie competentă Data anunțului în plen	ITRE 1.6.2023
Aviz emis de către Data anunțului în plen	AFET 1.6.2023
Raportor pentru aviz Data numirii	Dragoş Tudorache 16.6.2023
Examinare în comisie	18.9.2023
Data adoptării	24.10.2023
Rezultatul votului final	+: 39 –: 4 0: 0
Membri titulari prezenți la votul final	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Membri supleanți prezenți la votul final	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOT FINAL PRIN APEL NOMINAL ÎN COMISIA SESIZATĂ PENTRU AVIZ

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri

25.10.2023

AVIZ AL COMISIEI PENTRU TRANSPORT ȘI TURISM

destinat Comisiei pentru industrie, cercetare și energie

referitor 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))

Raportor pentru aviz: Gheorghe Falcă

JUSTIFICARE SUCCINTĂ

Organizațiile afectate de atacuri cibernetice, inclusiv cele din sectorul transporturilor, raportează rar aceste atacuri, deoarece tind să le vadă ca „publicitate negativă”. Acest lucru este valabil mai ales în cazul întreprinderilor din sectorul privat. Majoritatea organizațiilor preferă să se ocupe de ele pe plan intern și, de multe ori, autorii atacurilor sunt cei care le fac publice. În UE, vestea bună este că intrarea în vigoare a Directivei 2022/2555 privind securitatea rețelelor (cunoscută sub denumirea de „Directiva NIS 2”), pe care statele membre trebuie să o transpună până în octombrie 2024, armonizează obligațiile de raportare a incidentelor în toate statele membre. Astfel, este destul de probabil ca, în următorii ani, să se înțeleagă mai bine natura și amploarea acestei probleme.

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat recent un raport1 care oferă informații despre amenințările la adresa securității cibernetice în sectorul transporturilor. În raport se subliniază că mai mult de jumătate din incidentele observate în perioada de raportare 2022 (55 %) au fost cauzate de infractori cibernetici, iar principalul motiv al atacurilor a fost acela de a obține câștiguri financiare. De asemenea, s-a constatat că majoritatea atacurilor cibernetice din sectorul transporturilor vizează sistemele informatice, cauzând perturbări operaționale.

În ceea ce privește pregătirea și răspunsul la incidentele de securitate cibernetică, în prezent sprijinul la nivelul Uniunii și solidaritatea între statele membre sunt limitate. Concluziile Consiliului din mai 2022 au subliniat necesitatea de a aborda aceste lacune, solicitând Comisiei să prezinte o propunere privind un nou **Fond de răspuns la situații de urgență legate de**

[1] „Understanding Cyber Threats in Transport”, ENISA, publicat la 21 martie 2023.

securitatea cibernetică[2].

Prezentul regulament pune în aplicare **Strategia de securitate cibernetică a UE** adoptată în decembrie 2020, care a anunțat crearea unui **scut cibernetic european**, consolidând capacitățile de detectare a amenințărilor cibernetice și de schimb de informații în Uniunea Europeană prin intermediul unei federații de centre de operațiuni de securitate (SOC) naționale și transfrontaliere. Acțiunile prevăzute în regulament vor fi sprijinite prin **finanțare în cadrul obiectivului strategic „Securitate cibernetică" al programului „Europa digitală"**.

Bugetul total include o majorare de 100 milioane EUR pe care acest regulament propune să o realoce de la alte obiective strategice ale programului „Europa digitală". Astfel, noua sumă totală disponibilă pentru acțiuni în materie de securitate cibernetică în cadrul programului „Europa digitală" va ajunge la 842,8 milioane EUR.

O parte din suma suplimentară de 100 milioane EUR va consolida bugetul gestionat de Centrul european de competențe în materie de securitate cibernetică (ECCC) pentru a pune în aplicare acțiuni privind SOC și pregătirea ca parte a programului (programelor) lor de lucru. În plus, finanțarea suplimentară va servi la sprijinirea instituirii rezervei UE pentru securitate cibernetică. Aceasta completează bugetul deja prevăzut pentru acțiuni similare în cadrul Grupului de lucru DEP principal și al Grupului de lucru pentru securitate cibernetică din perioada 2023-2027, ceea ce ar putea aduce suma totală la 551 de milioane pentru perioada 2023-2027, în timp ce 115 milioane au fost deja dedicate sub forma unor proiecte-pilot pentru perioada 2021-2022. Incluzând contribuțiile statelor membre, bugetul total s-ar putea ridica la 1,109 miliarde de euro.

[2] Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene, 23 mai 2022, (9364/22).

Poziția raportorului

Raportorul salută noua propunere și consideră că aceasta va aduce beneficii semnificative diferitelor părți interesate. Raportorul subliniază că trebuie să se înțeleagă mai bine nevoile și cerințele în materie de securitate cibernetică în domeniul transporturilor, dar și să se asigure accesul entităților critice din sectorul transporturilor la o finanțare adecvată pentru pregătirea și răspunsul la incidente și soluționarea acestora.

Raportorul sprijină „setul de instrumente pentru securitatea cibernetică în domeniul transporturilor", care urmărește să contribuie la un nivel mai ridicat de conștientizare în domeniul cibernetic și de igienă cibernetică, cu accent special pe sectorul transporturilor. Acesta vizează organizațiile din sectorul transporturilor, indiferent de dimensiunea și domeniul lor de activitate, precum și, luând în considerare infrastructura critică de transport și mobilitatea militară, mai ales având în vedere războiul din Ucraina, în special, dar nu numai:

- transportatorii aerieni, organismele de administrare a aeroporturilor, aeroporturile principale, centrele de management al traficului aerian și de control al traficului aerian, Agenția Uniunii Europene pentru Siguranța Aviației și Eurocontrol;
- administratorii de infrastructură, întreprinderile feroviare și Sistemul european de management al traficului feroviar (ERTMS);
- societățile de transport interior, maritim și costier de pasageri și mărfuri, organismele de administrare a porturilor, inclusiv instalațiile portuare ale acestora, entitățile care realizează lucrări și operează echipamente în porturi, operatorii de servicii de trafic naval;
- autoritățile rutiere responsabile cu controlul gestionării traficului, operatorii de sisteme de transport inteligente;
- serviciile poștale și de curierat.

Raportorul consideră că dimensiunea bugetului pentru funcționarea **Fondului de răspuns la situații de urgență legate de securitatea cibernetică** (ERFC) va determina succesul acestuia; prin urmare, ar trebui să fie suficient de mare pentru a sprijini statele membre **să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare, să răspundă la acestea și să se redreseze** imediat în urma lor. Instituțiile, organele, oficiile și agențiile Uniunii ar trebui să beneficieze și de sprijin pentru a putea răspunde la incidente.

Scutul cibernetic european va îmbunătăți capabilitățile statelor membre de detectare a amenințărilor cibernetice. **Mecanismul pentru situații de urgență cibernetică** va completa acțiunile statelor membre oferind sprijin de urgență pentru pregătire, răspuns și redresare imediată/restabilirea funcționării serviciilor esențiale.

AMENDAMENTE

Comisia pentru transport și turism recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele:

Amendamentul 1

Propunere de regulament
Considerentul 2

Textul propus de Comisie	*Amendamentul*
(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. Această amenințare depășește agresiunea militară a Rusiei asupra Ucrainei și este susceptibilă să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor ***și*** să provoace pagube majore economiei 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 în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări.	(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice***, precum și pentru infrastructura informatică și fizică critică***. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. Această amenințare depășește agresiunea militară a Rusiei asupra Ucrainei și este susceptibilă să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice***, a transportului public și privat*** și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor***,*** să provoace pagube majore economiei ***Uniunii, precum și mobilității în interiorul*** 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 în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări.

Amendamentul 2

Propunere de regulament
Considerentul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	(2a) Actorii sponsorizați de stat, infractorii cibernetici și hacktiviștii care vizează autoritățile, operatorii, producătorii, furnizorii și prestatorii de servicii din sectorul aviației, maritim, feroviar și rutier reprezintă o amenințare din ce în ce mai gravă la adresa securității cibernetice în sectorul transporturilor. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a observat o creștere cu 25 % a numărului mediu lunar de incidente raportate care au afectat sectorul transporturilor în 2022, comparativ cu nivelurile din 2021. Majoritatea atacurilor asupra sectorului transporturilor vizează sistemele de tehnologie a informației (IT), având ca rezultat posibile perturbări operaționale[14a].
	[14b] ENISA (2023), Situația amenințărilor ENISA: Sectorul transporturilor, paginile 7 și 17.

Amendamentul 3

Propunere de regulament
Considerentul 2 b (nou)

Textul propus de Comisie	*Amendamentul*
	(2b) Invadarea neprovocată a Ucrainei de către Rusia a determinat o creștere semnificativă a incidentelor de securitate cibernetică, inclusiv a atacurilor cibernetice vizând blocarea accesului (DDoS), care vizează sectorul transporturilor din UE și zonele din apropierea UE, în special aeroporturile, căile ferate și autoritățile din domeniul transporturilor[14b]. Este foarte probabil ca această creștere a numărului de atacuri

să continue.

---

*[14b] **ENISA (2023), Situația amenințărilor ENISA: Sectorul transporturilor, pagina 9.***

Amendamentul 4

Propunere de regulament
Considerentul 2 c (nou)

Textul propus de Comisie	*Amendamentul*
	(2c) Atacurile cibernetice vizează autorități și organisme din toate subsectoarele transporturilor, fiind afectate întreprinderile feroviare și administratorii de infrastructură, precum și operatorii portuari. În ceea ce privește sectorul rutier, au fost vizați producătorii de echipamente originale (OEM), furnizorii și prestatorii de servicii, precum și operatorii de transport public. În sectorul aviației, principalele obiective au fost companiile aeriene și operatorii aeroportuari, urmați de furnizorii de servicii, operatorii de transport de suprafață și lanțul de aprovizionare[14c].

---

*[14c] **ENISA (2023), Situația amenințărilor ENISA: Sectorul transporturilor, pagina 17.***

Amendamentul 5

Propunere de regulament
Considerentul 3

Textul propus de Comisie	*Amendamentul*
(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate și sprijinirea transformării digitale a acestora, prin consolidarea	(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate 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***16***, este necesar să se sporească reziliența cetățenilor, a întreprinderilor 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 care vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică.

[16] https://futureu.europa.eu/ro/?locale=ro

nivelului de securitate cibernetică pe piața unică digitală. Astfel cum se recomandă în trei propuneri diferite ale Conferinței privind viitorul Europei[16], este necesar să se sporească reziliența cetățenilor, a întreprinderilor***, a operatorilor de transport*** 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 care vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică***, precum și privind starea și evoluția pieței muncii în materie de securitate cibernetică, deoarece joacă un rol esențial în furnizarea serviciilor necesare de detectare și răspuns***.

[16] https://futureu.europa.eu/ro/?locale=ro

Amendamentul 6

Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(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 materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea	(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 materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea

(UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat 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.

(UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]**,** ***precum și propunerea de regulament privind orientările Uniunii pentru dezvoltarea rețelei transeuropene de transport și propunerea de regulament privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale (Regulamentul privind reziliența cibernetică)***. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat 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.

---

[17] 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).

[18] 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).

[19] 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).

[20] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului

[17] 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).

[18] 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).

[19] 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).

[20] 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).

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).

Amendamentul 7

Propunere de regulament
Considerentul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	(4a) Deși salută setul de instrumente al Comisiei Europene pentru securitatea cibernetică în domeniul transporturilor[2a], care conține informații de bază privind amenințările care pot afecta organizațiile de transport (difuzarea programelor malware, blocarea accesului, accesul neautorizat și furtul și manipularea software-ului) și enumeră bunele practici de atenuare a acestora, operatorii de transport ar trebui să beneficieze de o formare adecvată privind securitatea cibernetică și de instrumente adecvate pentru a preveni amenințările cibernetice. Bugetul Uniunii ar trebui să acopere, de asemenea, sprijinul, cum ar fi formarea, furnizat de ENISA pentru a permite punerea în aplicare eficace de către operatorii de transport a celor mai bune practici de atenuare incluse în setul de instrumente.
	[1a] Raportul ENISA privind situația amenințărilor: Sectorul transporturilor / ENISA, martie 2023
	[2a] Comisia Europeană, (2021). Setul de instrumente pentru securitatea cibernetică în domeniul transporturilor, disponibil la adresa

https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Amendamentul 8

Propunere de regulament
Considerentul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	(4a) O abordare coordonată la nivelul Uniunii pentru a consolida gradul de pregătire și reziliența infrastructurii critice, de exemplu a infrastructurii de transport, se bazează pe consolidarea capacităților statelor membre. După cum s-a recunoscut în recenta comunicare a Comisiei către Parlamentul European și Consiliu intitulată „Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE”[19a], securitatea UE nu poate fi garantată fără cel mai valoros atu al UE: cetățenii săi.
	[19a] Comunicare a Comisiei către Parlamentul European și Consiliu - Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE („Academia de competențe în materie de securitate cibernetică”) COM(2023) 207 final

Amendamentul 9

Propunere de regulament
Considerentul 12

Textul propus de Comisie	*Amendamentul*
(12) Pentru a preveni, a evalua și a răspunde într-un mod mai eficace amenințărilor și incidentelor de securitate cibernetică, este necesar să se dezvolte	(12) Pentru a preveni, a evalua și a răspunde într-un mod mai eficace amenințărilor și incidentelor de securitate cibernetică, 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. Ar trebui implementată o infrastructură la scară largă a Uniunii de SOC („Scutul cibernetic european”), care să cuprindă mai multe platforme transfrontaliere interoperaționale, fiecare grupând mai multe SOC 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 și analiză a datelor, consolidând capabilitățile de detectare și gestionare a incidentelor cibernetice și asigurând conștientizarea în timp real a situației. Infrastructura respectivă ar trebui să contribuie la creșterea gradului de detectare a amenințărilor și incidentelor de securitate cibernetică și, prin urmare, să completeze și să sprijine entitățile și rețelele Uniunii responsabile de gestionarea crizelor în Uniune, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe”), astfel cum este definită în Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[24].

[24] 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

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. ***Printre aceste active și infrastructuri critice se numără sistemele de transport inteligente, care, deși sunt esențiale pentru mobilitatea automatizată și multimodală, funcționează pe baza unor schimburi cruciale de date sensibile.*** Ar trebui implementată o infrastructură la scară largă a Uniunii de SOC („Scutul cibernetic european”), care să cuprindă mai multe platforme transfrontaliere interoperaționale, fiecare grupând mai multe SOC 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 și analiză a datelor, consolidând capabilitățile de detectare și gestionare a incidentelor cibernetice și asigurând conștientizarea în timp real a situației. Infrastructura respectivă ar trebui să contribuie la creșterea gradului de detectare a amenințărilor și incidentelor de securitate cibernetică și, prin urmare, să completeze și să sprijine entitățile și rețelele Uniunii responsabile de gestionarea crizelor în Uniune, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice („EU-CyCLONe”), astfel cum este definită în Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[24].

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

Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).	Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

Amendamentul 10

Propunere de regulament
Considerentul 14 a (nou)

Textul propus de Comisie	*Amendamentul*
	(14a) Sectorul transporturilor devine din ce în ce mai mult unul dintre cele mai profitabile activități pentru infractorii cibernetici, datele clienților fiind considerate o marfă extrem de valoroasă, iar lanțul de aprovizionare al transporturilor devenind tot mai des țința. Din acest motiv, infrastructura de transport caracterizată de un aspect transfrontalier sau de schimbul de date prin intermediul tehnologiilor fără fir ar trebui considerată un obiectiv esențial al analizei și monitorizării atât pentru SOC naționale, cât și, în special, pentru SOC transfrontaliere. De exemplu, recenta propunere de revizuire a Regulamentului TEN-T necesită o mai mare solidaritate și cooperare în ceea ce privește schimbul de informații privind amenințările cibernetice transfrontaliere cu care s-ar putea confrunta această rețea transnațională. În mod similar, sistemele de transport inteligente (STI) sunt esențiale pentru ca transportul să devină mai sigur, mai eficient și mai sustenabil, însă sistemele de transport devin mai vulnerabile la atacurile cibernetice care pot crea accidente, blocaje de trafic sau pot cauza pierderi economice atât pentru operatorii privați, cât și pentru cei publici. Pentru a proteja siguranța pasagerilor, protecția datelor utilizatorilor și ale furnizorilor și pentru a evita daunele financiare, este esențial ca programul de punere în aplicare a Directivei revizuite privind sistemele de transport inteligente să includă dispoziții și instrumente de consolidare a colaborării dintre statele

membre în vederea detectării amenințărilor și a incidentelor de securitate cibernetică, a pregătirii legate de acestea și a contracarării lor.

Amendamentul 11

Propunere de regulament
Considerentul 15

Textul propus de Comisie	*Amendamentul*
(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a suveranității tehnologice ale Uniunii.	(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a suveranității tehnologice ale Uniunii. ***În acest sens, pentru a consolida autonomia Uniunii în domeniul cibernetic și cu trimitere la articolul 47 alineatul (4) din propunerea de regulament privind orientările pentru dezvoltarea rețelei transeuropene de transport (COM(2021)0812), este, de asemenea, necesar să se prevină accesul la date care conduc la amenințări cibernetice prin aplicarea unui cadru de reglementare solid care să reglementeze proprietatea străină și investițiile în infrastructura critică, cum ar fi în sectorul transporturilor.***

Amendamentul 12

Propunere de regulament
Considerentul 21

Textul propus de Comisie	*Amendamentul*
(21) Deși Scutul cibernetic european este un proiect civil, comunitatea de apărare cibernetică ar putea beneficia de capabilități civile mai puternice de detectare și de conștientizare a situației dezvoltate pentru protecția infrastructurii critice. SOC transfrontaliere, cu sprijinul Comisiei și al Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) și în cooperare cu Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate („Înaltul Reprezentant”), ar trebui să elaboreze treptat protocoale și standarde specifice pentru a permite cooperarea cu comunitatea de apărare cibernetică, inclusiv privind investigațiile și condițiile de securitate. Dezvoltarea Scutului cibernetic european ar trebui să fie însoțită de o reflecție care să permită colaborarea viitoare cu rețelele și platformele responsabile cu schimbul de informații în cadrul comunității de apărare cibernetică, în strânsă cooperare cu Înaltul Reprezentant.	(21) Deși Scutul cibernetic european este un proiect civil, comunitatea de apărare cibernetică ar putea beneficia de capabilități civile mai puternice de detectare și de conștientizare a situației dezvoltate pentru protecția infrastructurii critice. SOC transfrontaliere, cu sprijinul Comisiei și al Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) și în cooperare cu Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate („Înaltul Reprezentant”), ar trebui să elaboreze treptat protocoale și standarde specifice pentru a permite cooperarea cu comunitatea de apărare cibernetică, inclusiv privind investigațiile și condițiile de securitate. Dezvoltarea Scutului cibernetic european ar trebui să fie însoțită de o reflecție care să permită colaborarea viitoare cu rețelele și platformele responsabile cu schimbul de informații în cadrul comunității de apărare cibernetică, în strânsă cooperare cu Înaltul Reprezentant. ***Aceasta ar trebui, de asemenea, să permită sinergii cu Planul de acțiune vizând mobilitatea militară 2.0. O rețea de mobilitate militară funcțională trebuie să fie reziliență, inclusiv în contextul amenințărilor cibernetice și al altor amenințări hibride care ar putea afecta nodurile critice din sistemul de transport care sunt cu dublă utilizare. De exemplu, un atac cibernetic asupra sistemelor utilizate în aeroporturi, porturi sau căi ferate sau un atac cibernetic asupra activelor militare ar putea avea consecințe majore. Astfel, digitalizarea proceselor și a procedurilor, inclusiv pentru cooperarea civilă și militară necesară, va impune consolidarea sistemelor informatice împotriva amenințărilor cibernetice.***

Amendamentul 13

Propunere de regulament
Considerentul 21 a (nou)

Textul propus de Comisie	*Amendamentul*
	(21a) În cazul unei crize de securitate cibernetică, un schimb eficace de informații este esențial pentru a asigura conștientizarea situației în rândul sectoarelor de transport militar și civil. Acest schimb de informații ar trebui, de asemenea, să stimuleze cooperarea dintre autoritățile sectoriale relevante responsabile cu transporturile, autoritățile competente în materie de securitate cibernetică, SOC și CSIRT.

Amendamentul 14

Propunere de regulament
Considerentul 29

Textul propus de Comisie	*Amendamentul*
(29) 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 deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. Sectoarele sau subsectoarele ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de	(29) 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 deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. Sectoarele sau subsectoarele ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). ***Ar trebui să***

testare coordonată 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, care urmează să fie efectuate de Comisie, de 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 (OAREC), de evaluările coordonate ale riscurilor 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) 2022/2554 al Parlamentului European și al Consiliului[29]. 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.

se acorde o atenție deosebită sectorului transporturilor și subsectoarelor sale (aerian, feroviar, pe apă, rutier), deoarece acestea includ infrastructuri critice în cazul cărora incidentele și atacurile cibernetice ar putea submina grav siguranța pasagerilor și a operatorilor. Exercițiile de testare coordonată 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, care urmează să fie efectuate de Comisie, de 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 (OAREC), de evaluările coordonate ale riscurilor 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) 2022/2554 al Parlamentului European și al Consiliului[29]. 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.

[29] Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența

[29] 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.	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.

Amendamentul 15

Propunere de regulament
Considerentul 30 a (nou)

Textul propus de Comisie	*Amendamentul*
	(30a) Având în vedere caracterul critic al sectorului și implicațiile amenințărilor cibernetice asupra mobilității și, în consecință, asupra vieților omenești ale pasagerilor și pietonilor, sectorul transporturilor ar trebui să aibă prioritate în ceea ce privește testarea coordonată a pregătirii entităților.

Amendamentul 16

Propunere de regulament
Considerentul 35 a (nou)

Textul propus de Comisie	*Amendamentul*
	(35a) Având în vedere sarcinile și responsabilitățile sporite conferite ENISA prin prezenta propunere, precum și prin propunerea referitoare la Regulamentul privind reziliența cibernetică, este necesară adoptarea bugetului rectificativ nr. 1/2022 al ENISA pentru implementarea pilot a unei acțiuni de sprijin în materie de securitate cibernetică. În plus, având în vedere interesele Uniunii care sunt în joc, ar trebui alocate resurse financiare și umane suplimentare ENISA.

Amendamentul 17

Propunere de regulament

Considerentul 38 a (nou)

Textul propus de Comisie	*Amendamentul*
	(38a) Dezvoltarea aptitudinilor și a competențelor ar trebui, prin urmare, să beneficieze de un rol central, în toate sectoarele, nu în ultimul rând în cele care sunt vulnerabile la amenințările la adresa securității cibernetice, cum ar fi personalul care lucrează în transportul în masă sau în infrastructurile critice, inclusiv sistemele de control al trenurilor și instrumentele digitale de planificare a transporturilor pentru toate modurile de transport. Prin urmare, introducerea și dezvoltarea în continuare a culturii securității cibernetice sunt esențiale pentru succesul punerii în aplicare a prezentului regulament, atât pentru sensibilizarea cetățenilor, cât și pentru cunoștințele specialiștilor din toate sectoarele infrastructurii critice.

Amendamentul 18

Propunere de regulament
Articolul 1 – alineatul 2 – litera a

Textul propus de Comisie	*Amendamentul*
(a) de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la suveranitatea tehnologică a Uniunii în domeniul securității cibernetice;	(a) de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei***, a infrastructurii de transport*** și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la suveranitatea tehnologică a Uniunii în domeniul securității cibernetice;

Amendamentul 19

Propunere de regulament
Articolul 1 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) a sprijinului din partea UE pentru răspunsul la incidentele de securitate cibernetică;	(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, ***acordând o atenție deosebită infrastructurii informatice și fizice critice,*** inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) a sprijinului din partea UE pentru răspunsul la incidentele de securitate cibernetică;

Amendamentul 20

Propunere de regulament
Articolul 1 – alineatul 2 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) de a consolida gradul de pregătire, cooperarea și eficacitatea Uniunii în ceea ce privește protejarea infrastructurii și a serviciilor de transport din statele membre împotriva incidentelor de securitate cibernetică, de a asigura funcționarea continuă a sectorului transporturilor, integritatea lanțurilor de aprovizionare și mobilitatea la nivelul Uniunii.

Amendamentul 21

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) contribuie la o mai bună protecție împotriva amenințărilor cibernetice și la un răspuns mai bun la acestea***;***	(c) contribuie la o mai bună protecție împotriva amenințărilor cibernetice și la un răspuns mai bun la acestea***, inclusiv pentru infrastructura de transport caracterizată de un aspect transfrontalier, cum ar fi TEN-T, sau de schimbul de date prin***

	intermediul tehnologiilor fără fir, cum ar fi sistemele de transport inteligente.

Amendamentul 22

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 2

Textul propus de Comisie	*Amendamentul*
Acesta este dezvoltat în cooperare cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173.	Acesta este dezvoltat în cooperare cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173. ***Acesta permite colaborarea, prin intermediul unor protocoale și standarde specifice, cu comunitatea de apărare cibernetică, pentru a asigura dezvoltarea unor capabilități civile mai puternice de detectare și de conștientizare a situației pentru protecția infrastructurii critice. În acest sens, se dezvoltă sinergii și cu Planul de acțiune vizând mobilitatea militară 2.0 și se asigură un schimb eficace de informații pentru a asigura conștientizarea situației în rândul sectoarelor de transport militar și civil.***

Amendamentul 23

Propunere de regulament
Articolul 8 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Comisia implică Scutul cibernetic european, în special SOC transfrontaliere, în avizul său adresat statelor membre în cadrul propunerii de regulament privind rețeaua transeuropeană de transport (COM(2021)0812), ori de câte ori participarea sau contribuția de orice fel a unei persoane fizice dintr-o țară terță sau a unei întreprinderi dintr-o țară terță este de natură să afecteze securitatea cibernetică a infrastructurii critice

transfrontaliere, cum ar fi TEN-T.

Amendamentul 24

Propunere de regulament
Articolul 10 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice în cadrul Uniunii;	(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice în cadrul Uniunii***, acordând o atenție deosebită infrastructurii de transport și subsectoarelor acesteia incluse în anexa I la Directiva (UE) 2022/255***;

Amendamentul 25

Propunere de regulament
Articolul 18 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Pentru a elabora raportul de evaluare a incidentelor menționat la alineatul (1), ENISA colaborează cu toate părțile interesate relevante, inclusiv reprezentanți ai statelor membre, ai Comisiei sau ai altor instituții, organisme și agenții relevante ale UE, furnizori de servicii de securitate gestionate și utilizatori de servicii de securitate cibernetică. După caz, ENISA colaborează și cu entitățile afectate de incidente de securitate cibernetică semnificative sau de mare amploare. Pentru a sprijini evaluarea, ENISA poate consulta și alte tipuri de părți interesate. Reprezentanții consultați comunică orice potențial conflict de interese.	2. Pentru a elabora raportul de evaluare a incidentelor menționat la alineatul (1), ENISA colaborează cu toate părțile interesate relevante, inclusiv reprezentanți ai statelor membre, ai Comisiei sau ai altor instituții, organisme și agenții relevante ale UE, furnizori de servicii de securitate gestionate și utilizatori de servicii de securitate cibernetică. După caz, ENISA colaborează și cu entitățile afectate de incidente de securitate cibernetică semnificative sau de mare amploare***, inclusiv cu operatorii de transport***. Pentru a sprijini evaluarea, ENISA poate consulta și alte tipuri de părți interesate. Reprezentanții consultați comunică orice potențial conflict de interese.

Amendamentul 26

Propunere de regulament
Articolul 19 – paragraful 1 – punctul 1 – litera b
Regulamentul (UE) 2021/694
Articolul 6 – alineatul 2a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Având în vedere interesele Uniunii aflate în joc, în ceea ce privește responsabilitățile sale pentru pregătirea propunerilor de sisteme de certificare în temeiul Regulamentului (UE) 2019/881, responsabilitățile sale de a revizui și de a evalua amenințările cibernetice, vulnerabilitățile și atenuarea acestora, de a pregăti un raport de evaluare a incidentelor pentru mecanismul de evaluare a incidentelor de securitate cibernetică, precum și de a oferi formare împotriva atacurilor și a incidentelor cibernetice operatorilor de infrastructură critică și având în vedere responsabilitățile sale recent atribuite în cadrul propunerii de regulament privind reziliența cibernetică, ENISA i se vor pune la dispoziție resursele necesare în cadrul bugetului Uniunii, în conformitate cu legislația aplicabilă.

Amendamentul 27

Propunere de regulament
Articolul 19 – paragraful 1 – punctul 1 a (nou)
Regulamentul (UE) 2021/694
Articolul 7 – alineatul 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(1a) Articolul 7 se modifică după cum urmează:
	(a) alineatul (1) se modifică după cum urmează:
	(1) se introduce următoarea literă (ca):
	(ca) sprijinirea formării de înaltă calitate a operatorilor de transport și a administratorilor și forței de muncă ale infrastructurii critice de transport,

inclusiv cu scopul de a partaja și de a pune în aplicare în mod eficace practici de atenuare în fața atacurilor cibernetice sau a incidentelor la adresa infrastructurii critice, cum ar fi cele furnizate de setul de instrumente pentru securitatea cibernetică a transporturilor.

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Stabilirea 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
Referințe	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Comisie competentă Data anunțului în plen	ITRE 1.6.2023
Aviz emis de către Data anunțului în plen	TRAN 1.6.2023
Raportor/Raportoare pentru aviz Data numirii	Gheorghe Falcă 7.7.2023
Data adoptării	25.10.2023
Rezultatul votului final	+: 38 –: 0 0: 0
Membri titulari prezenți la votul final	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Membri supleanți prezenți la votul final	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

VOT FINAL PRIN APEL NOMINAL ÎN COMISIA SESIZATĂ PENTRU AVIZ

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri

PROCEDURA COMISIEI COMPETENTE

Titlu	Stabilirea 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			
Referințe	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Data prezentării în PE	19.4.2023			
Comisie competentă Data anunțului în plen	ITRE 1.6.2023			
Comisii sesizate pentru aviz Data anunțului în plen	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Avize care nu au fost emise Data deciziei	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Raportori Data numirii	Lina Gálvez Muñoz 2.5.2023			
Examinare în comisie	19.9.2023			
Data adoptării	7.12.2023			
Rezultatul votului final	+: –: 0:	43 10 1		
Membri titulari prezenți la votul final	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Membri supleanți prezenți la votul final	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Data depunerii	8.12.2023			

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA COMPETENTĂ

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri