COMISIA
EUROPEANĂ

Strasbourg, 18.4.2023
COM(2023) 209 final

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

EXPUNERE DE MOTIVE

1. CONTEXT

• Temeiurile și obiectivele propunerii

Prezenta expunere de motive însoțește propunerea de Regulament privind solidaritatea cibernetică. 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. Această adoptare pe scară mai largă a tehnologiilor digitale face să crească expunerea la incidentele de securitate cibernetică și impactul potențial al acestora. În același timp, statele membre se confruntă cu riscuri tot mai mari în materie de securitate cibernetică și cu un peisaj general complex al amenințărilor, cu un risc clar de propagare rapidă a incidentelor cibernetice de la un stat membru la altul.

În plus, operațiunile cibernetice sunt din ce în ce mai integrate în strategiile hibride și de război, cu efecte semnificative asupra țintei. În special, agresiunea militară a Rusiei împotriva Ucrainei a fost precedată și este însoțită de o strategie de operațiuni cibernetice ostile, care reprezintă un factor de schimbare pentru percepția și evaluarea pregătirii colective a UE pentru gestionarea crizelor în materie de securitate cibernetică și impune adoptarea de acțiuni urgente. Amenințarea unui posibil incident de mare amploare care cauzează perturbări și daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile ecosistemului de securitate cibernetică al UE. Această amenințare depășește agresiunea militară a Rusiei asupra Ucrainei și include amenințări cibernetice continue din partea actorilor statali și nestatali, care sunt susceptibile să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. În ultimii ani, numărul atacurilor cibernetice a crescut dramatic, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware sau perturbări. În 2020, atacul asupra lanțului de aprovizionare SolarWinds a afectat peste 18 000 de organizații la nivel mondial, inclusiv agenții guvernamentale și întreprinderi importante. Incidentele semnificative de securitate cibernetică pot fi prea perturbatoare pentru ca un singur stat membru sau mai multe state membre afectate să poată să le gestioneze la nivel individual. Din acest motiv, este necesară consolidarea solidarității la nivelul Uniunii pentru a detecta mai bine amenințările și incidentele de securitate cibernetică și pentru a se pregăti mai bine și a putea oferi un răspuns mai bun la astfel de situații.

În ceea ce privește detectarea amenințărilor și incidentelor cibernetice, există o nevoie urgentă de a intensifica schimbul de informații și de a ne îmbunătăți capacitățile colective pentru a reduce drastic timpul necesar pentru detectarea amenințărilor cibernetice, înainte ca acestea să poată cauza daune și costuri de mare amploare[1]. Deși multe amenințări și incidente de

[1] Potrivit unui raport întocmit de Ponemon Institute și IBM Security, durata medie de identificare a unei încălcări a securității datelor în 2022 a fost de 207 zile, cu o perioadă suplimentară de 70 de zile pentru izolare. În același timp, în 2022, încălcările securității datelor cu un ciclu de viață de peste 200 de zile au avut un cost mediu de 4,86 milioane EUR, comparativ cu 3,74 milioane EUR atunci când ciclul de

securitate cibernetică au o dimensiune transfrontalieră potențială, din cauza interconectării infrastructurilor digitale, schimbul de informații relevante între statele membre rămâne limitat. Crearea unei rețele de centre transfrontaliere de operațiuni de securitate (SOC) pentru a consolida capacitățile de detectare și de răspuns urmărește să contribuie la soluționarea acestei probleme.

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 octombrie 2021 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 securitatea cibernetică[2].

De asemenea, prezentul regulament pune în aplicare Strategia de securitate cibernetică a UE adoptată în decembrie 2020[3], 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 SOC naționale și transfrontaliere.

Prezentul regulament se bazează pe primele etape deja elaborate în colaborare strânsă cu principalele părți interesate și cu sprijinul programului „Europa digitală” (DEP). În special, în ceea ce privește SOC, în cadrul programului de lucru privind securitatea cibernetică al DEP pentru perioada 2021-2022, au avut loc o cerere de exprimare a interesului pentru achiziționarea în comun de instrumente și infrastructuri pentru crearea de SOC transfrontaliere și o cerere de granturi pentru a permite consolidarea capacităților SOC-urilor care deservesc organizații publice și private. În ceea ce privește pregătirea și răspunsul la incidente, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre, prin fonduri suplimentare alocate Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), cu scopul de a consolida imediat gradul de pregătire și capacitățile de răspuns la incidentele cibernetice majore. Ambele acțiuni au fost pregătite în strânsă coordonare cu statele membre. Prezentul regulament abordează deficiențele și integrează informații din aceste acțiuni.

În cele din urmă, prezenta propunere respectă angajamentul asumat în conformitate cu Comunicarea comună privind apărarea cibernetică[4], adoptată la 10 noiembrie, de a pregăti o propunere de inițiativă a UE privind solidaritatea cibernetică, cu următoarele obiective: de a consolida capabilitățile comune de detectare, de conștientizare a situației și de răspuns la nivelul UE, de a crea treptat o rezervă de securitate cibernetică la nivelul UE cu servicii furnizate de prestatori de servicii privați de încredere și de a sprijini testarea entităților critice.

---

viață este mai mic de 200 de zile. [„Cost of a data breach 2022” (Costul unei încălcări a securității datelor), https://www.ibm.com/reports/data-breach].

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

[3] Comunicare comună către Parlamentul European și Consiliu, Strategia de securitate cibernetică a UE pentru deceniul digital, JOIN(2020) 18 final.

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

În acest context, Comisia prezintă prezentul Regulament privind solidaritatea cibernetică pentru a consolida solidaritatea la nivelul Uniunii în vederea unei mai bune detectări, pregătiri și a unui răspuns mai bun la amenințările și incidentele de securitate cibernetică prin intermediul următoarelor obiective specifice:

- de a consolida detectarea și conștientizarea comună a situației la nivelul UE cu privire la amenințările și incidentele cibernetice, contribuind astfel la suveranitatea tehnologică europeană în domeniul securității cibernetice;
- de a consolida gradul de pregătire al entităților critice din întreaga UE și solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea la dispoziție a sprijinului pentru răspunsul la incidente pentru țările terțe. asociate la programul „Europa digitală”;
- de a spori reziliența Uniunii și de a contribui la un răspuns eficace prin revizuirea și evaluarea incidentelor semnificative sau de mare amploare, inclusiv prin valorificarea lecțiilor învățate și, după caz, prin recomandări.

Aceste obiective sunt puse în aplicare prin intermediul următoarelor acțiuni:

- implementarea unei infrastructuri paneuropene de SOC (Scutul cibernetic european) pentru a construi și a consolida capabilitățile comune de detectare și de conștientizare a situației;
- 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. Sprijin pentru răspunsul la incidente este pus, de asemenea, la dispoziția instituțiilor, organelor, oficiilor și agențiilor Uniunii Europene (IOAUE);
- instituirea unui mecanism european de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice.

Scutul cibernetic european și mecanismul pentru situații de urgență cibernetică vor fi sprijinite prin finanțare din partea DEP, pe care îl va modifica acest instrument legislativ pentru a stabili acțiunile menționate mai sus, pentru a oferi sprijin financiar pentru dezvoltarea acestora și pentru a clarifica condițiile în care se poate beneficia de sprijinul financiar.

•Coerența cu dispozițiile existente în domeniul de politică vizat

Cadrul UE cuprinde mai multe acte legislative deja în vigoare sau propuse la nivelul Uniunii pentru a reduce vulnerabilitățile, a spori reziliența entităților critice împotriva riscurilor de securitate cibernetică și a sprijini gestionarea coordonată a incidentelor și crizelor de securitate cibernetică de mare amploare, în special Directiva privind măsuri pentru un nivel

comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (NIS2)[5], Regulamentul privind securitatea cibernetică[6], Directiva privind atacurile împotriva sistemelor informatice[7] și Recomandarea (UE) 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare[8].

Acțiunile propuse în temeiul Regulamentului privind solidaritatea cibernetică vizează conștientizarea situației, schimbul de informații, precum și sprijinul pentru pregătirea și răspunsul la incidentele cibernetice. Aceste acțiuni sunt în concordanță cu obiectivele cadrului de reglementare în vigoare la nivelul Uniunii, în special în temeiul Directivei (UE) 2022/2555 („Directiva NIS2”), și le sprijină. Regulamentul privind solidaritatea cibernetică se va baza în special pe cadrele existente de cooperare operațională și de gestionare a crizelor în materie de securitate cibernetică și va sprijini aceste cadre, în special Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) și Rețeaua echipelor de intervenție în caz de incidente de securitate informatică (CSIRT).

Platformele 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 instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a suveranității tehnologice ale Uniunii.

În cele din urmă, prezenta propunere este în concordanță cu Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice[9], care 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.

- **Coerența cu alte domenii de politică a Uniunii**

Propunerea este coerentă cu alte mecanisme și protocoale de urgență în situații de criză, cum ar fi–Mecanismul integrat pentru un răspuns politic la crize (IPCR). Regulamentul privind

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

[6] 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).

[7] 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.

[8] Propunere de regulament al Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020, COM(2022) 454 final.

[9] Recomandare a Consiliului din 8 decembrie 2022 privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice (Text cu relevanță pentru SEE), 2023/C 20/01.

solidaritatea cibernetică va completa aceste cadre și protocoale de gestionare a crizelor prin furnizarea de sprijin specific pentru pregătirea și răspunsul la incidentele de securitate cibernetică. De asemenea, propunerea va fi în concordanță cu acțiunea externă a UE ca răspuns la incidentele de mare amploare din cadrul politicii externe și de securitate comune (PESC), inclusiv prin intermediul setului de instrumente al UE pentru diplomația cibernetică. Propunerea va completa acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană sau în situațiile definite la articolul 222 din Tratatul privind funcționarea Uniunii Europene.

De asemenea, aceasta completează mecanismul de protecție civilă al Uniunii (UCPM)[10], instituit în decembrie 2013 și completat cu o nouă legislație adoptată în mai 2021[11], care consolidează pilonii de prevenire, pregătire și răspuns ai UCPM și oferă UE capacități suplimentare de răspuns la noi riscuri în Europa și în lume și consolidează rezerva rescEU.

2. TEMEIUL JURIDIC, SUBSIDIARITATEA ȘI PROPORȚIONALITATEA

• Temeiul juridic

Temeiul juridic al prezentei propuneri este articolul 173 alineatul (3) și articolul 322 alineatul (1) litera (a) din Tratatul privind funcționarea Uniunii Europene (TFUE). Articolul 173 din TFUE prevede că Uniunea și statele membre se asigură că există condițiile necesare competitivității industriei Uniunii. Prezentul regulament vizează consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Europa în cadrul economiei digitalizate și sprijinirea transformării digitale a acestora, prin consolidarea nivelului de securitate cibernetică pe piața unică digitală. În special, acesta vizează creșterea rezilienței cetățenilor, a întreprinderilor și a entităților care își desfășoară activitatea în sectoare critice și deosebit de critice împotriva amenințărilor tot mai mari la adresa securității cibernetice, care pot avea un impact societal și economic devastator.

Propunerea se bazează, de asemenea, pe articolul 322 alineatul (1) litera (a) din TFUE, deoarece conține norme specifice de reportare care derogă de la principiul anualității prevăzut în Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului („Regulamentul financiar”)[12]. În scopul bunei gestiuni financiare și având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice și al amenințărilor cibernetice, mecanismul pentru situații de urgență cibernetică ar trebui să beneficieze de un anumit grad de flexibilitate în ceea ce privește gestiunea bugetară și, în special, permițând reportarea automată în exercițiul financiar următor a creditelor de angajament și de plată neutilizate pentru acțiunile care urmăresc obiectivele stabilite în regulament. Întrucât această

---

10 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).

11 Regulamentul (UE) 2021/836 al Parlamentului European și al Consiliului din 20 mai 2021 de modificare a Deciziei nr. 1313/2013/UE privind un mecanism de protecție civilă al Uniunii (Text cu relevanță pentru SEE).

12 Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii (JO L 193, 30.7.2018, p. 1).

nouă normă ridică probleme legate de Regulamentul financiar, această chestiune ar putea fi abordată în contextul negocierilor actuale privind Regulamentul financiar reformat.

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

Caracterul transfrontalier puternic al amenințărilor cibernetice și numărul tot mai mare de riscuri și incidente care au efecte de propagare dincolo de frontiere, sectoare și produse fac ca obiectivele prezentei intervenții să nu poată fi realizate în mod eficace de către statele membre în mod individual și să necesite o acțiune comună și solidaritate la nivelul Uniunii.

Experiența combaterii amenințărilor cibernetice generate de războiul împotriva Ucrainei, împreună cu învățămintele desprinse în urma unui exercițiu de securitate cibernetică desfășurat sub președinția franceză (EU CyCLES) au arătat că, pentru a realiza solidaritatea la nivelul UE, ar trebui dezvoltate mecanisme concrete de sprijin reciproc, în special cooperarea cu sectorul privat. În acest context, Concluziile Consiliului din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene invită Comisia să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică.

Sprijinul și acțiunile la nivelul Uniunii pentru o mai bună detectare a amenințărilor la adresa securității cibernetice și pentru sporirea capacităților de pregătire și de răspuns oferă valoare adăugată deoarece evită duplicarea eforturilor în întreaga Uniune și în statele membre. Aceasta ar conduce la o mai bună exploatare a activelor existente și la o mai bună coordonare și un schimb de informații îmbunătățit cu privire la învățămintele desprinse. Mecanismul pentru situații de urgență cibernetică are în vedere, de asemenea, acordarea de sprijin din rezerva UE pentru securitate cibernetică țărilor terțe asociate la DEP.

Sprijinul oferit prin intermediul diferitelor inițiative care urmează să fie instituite și finanțate la nivelul Uniunii va completa și nu se va suprapune peste capabilitățile naționale în ceea ce privește detectarea amenințărilor și incidentelor cibernetice, conștientizarea situației, pregătirea pentru aceasta și răspunsul oferit.

- **Proporționalitatea**

Acțiunile nu depășesc ceea ce este necesar pentru atingerea obiectivelor generale și specifice ale regulamentului. Acțiunile prevăzute în prezentul regulament nu afectează responsabilitățile statelor membre în ceea ce privește securitatea națională, siguranța publică, prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor. Acestea nu afectează nici obligațiile legale ale entităților care își desfășoară activitatea în sectoare critice și deosebit de critice de a adopta măsuri de securitate cibernetică, în conformitate cu Directiva NIS 2.

Acțiunile care fac obiectul prezentului regulament sunt complementare acestor eforturi și măsuri, prin sprijinirea creării de infrastructuri pentru o mai bună detectare și analiză a amenințărilor și prin furnizarea de sprijin pentru acțiunile de pregătire și răspuns în cazul unor incidente semnificative sau de mare amploare.

- **Alegerea instrumentului**

Propunerea este sub forma unui regulament al Parlamentului European și al Consiliului. Acesta este instrumentul juridic cel mai adecvat, deoarece numai un regulament, cu dispozițiile sale juridice direct aplicabile, poate oferi gradul de uniformitate necesar pentru instituirea și funcționarea unui Scut cibernetic european și a unui mecanism pentru situații de urgență cibernetică, prevăzând sprijin din partea DEP pentru instituirea lor, precum și condiții clare de utilizare și de alocare a acestui sprijin.

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

- **Consultările cu părțile interesate**

Acțiunile din prezentul regulament vor fi sprijinite de DEP, care a făcut obiectul unei ample consultări. În plus, acestea se vor baza pe primele etape care au fost pregătite în strânsă cooperare cu principalele părți interesate. În ceea ce privește SOC, Comisia a elaborat un document de reflecție privind dezvoltarea platformelor SOC transfrontaliere și o cerere de exprimare a interesului în strânsă cooperare cu statele membre în cadrul Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC). În acest context, a fost realizat un sondaj privind capacitățile SOC naționale și au fost discutate abordări și cerințe tehnice comune în cadrul grupului de lucru tehnic al ECCC, care reunește reprezentanți ai statelor membre. În plus, au avut loc schimburi cu industria, în special prin intermediul grupului de experți privind SOC creat de ENISA și de Organizația Europeană de Securitate Cibernetică (ECSO).

În al doilea rând, în ceea ce privește pregătirea și răspunsul la incidente, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre, prin fonduri suplimentare alocate ENISA din DEP, cu scopul de a consolida imediat gradul de pregătire și capacitățile de răspuns la incidentele cibernetice majore. Feedbackul din partea statelor membre și a industriei, colectat în cursul punerii în aplicare a acestui program pe termen scurt, oferă deja informații valoroase care au contribuit la elaborarea propunerii de regulament pentru a remedia deficiențele identificate. Acesta a fost un prim pas în conformitate cu concluziile Consiliului privind poziția cibernetică, prin care se solicită Comisiei să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică.

În plus, la 16 februarie 2023, a avut loc un atelier cu experți din statele membre cu privire la mecanismul pentru situații de urgență cibernetică, pe baza unui document de dezbatere. La acest atelier au participat toate statele membre, iar 11 state membre au furnizat contribuții suplimentare în scris.

- **Evaluarea impactului**

Având în vedere caracterul urgent al propunerii, nu a fost efectuată o evaluare a impactului. Acțiunile din prezentul regulament vor fi sprijinite de DEP și sunt conforme cu cele stabilite în Regulamentul privind DEP, care a făcut obiectul unei evaluări a impactului specifice. Prezentul regulament nu va avea niciun impact administrativ sau de mediu semnificativ în afara celor deja evaluate în evaluarea impactului Regulamentului privind DEP.

În plus, acesta se bazează pe primele acțiuni elaborate în colaborare strânsă cu principalele părți interesate, astfel cum se prevede mai sus, și dă curs solicitării statelor membre adresate Comisiei de a prezenta o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică până la sfârșitul celui de al treilea trimestru al anului 2022.

În mod specific, în ceea ce privește conștientizarea situației și detectarea în cadrul Scutului cibernetic european, ca parte a programului de lucru privind securitatea cibernetică al DEP pentru perioada 2021-2022, au avut loc o cerere de exprimare a interesului pentru achiziționarea în comun de instrumente și infrastructuri pentru crearea de SOC transfrontaliere și o cerere de granturi pentru a permite consolidarea capacităților SOC-urilor care deservesc organizații publice și private.

În domeniul pregătirii și al răspunsului la incidente, astfel cum s-a menționat mai sus, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre din cadrul DEP, acesta fiind pus în aplicare de ENISA. Prin aceste fonduri se pot finanța acțiuni de pregătire, cum ar fi efectuare de teste de penetrare cibernetică pe entitățile critice pentru a identifica eventualele vulnerabilități. Se consolidează, de asemenea, posibilitățile de a asista statele membre în cazul unui incident major care ar afecta entitățile critice. Punerea în aplicare de către ENISA a acestui program pe termen scurt este în curs și a oferit deja informații relevante care au fost luate în considerare la elaborarea prezentului regulament.

- **Drepturile fundamentale**

Prin contribuția sa la securitatea informațiilor digitale, prezenta propunere va contribui la protejarea dreptului la libertate și securitate în conformitate cu articolul 6 din Carta drepturilor fundamentale a UE, precum și a dreptului la respectarea vieții private și de familie, în conformitate cu articolul 7 din Carta drepturilor fundamentale a UE. Prin protejarea întreprinderilor împotriva atacurilor cibernetice dăunătoare din punct de vedere economic, propunerea va contribui și la libertatea de a desfășura o activitate comercială în conformitate cu articolul 16 din Carta drepturilor fundamentale a UE și la dreptul de proprietate în conformitate cu articolul 17 din Carta drepturilor fundamentale a UE. În cele din urmă, prin protejarea integrității infrastructurii critice în fața atacurilor cibernetice, propunerea va contribui la dreptul la asistență medicală în conformitate cu articolul 35 din Carta drepturilor fundamentale a UE și la dreptul de acces la servicii de interes economic general, în conformitate cu articolul 36 din Carta drepturilor fundamentale a UE.

4. IMPLICAȚII BUGETARE

Acțiunile prevăzute în prezentul regulament vor fi sprijinite prin finanțare în cadrul obiectivului strategic „Securitate cibernetică” al programului „Europa digitală”.

Bugetul total include o creștere de 100 de milioane EUR pe care prezentul 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 de milioane EUR va consolida bugetul gestionat de 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.

O prezentare generală a costurilor implicate este inclusă în „fișa financiară legislativă” care însoțește prezenta propunere.

5. ELEMENTE DIVERSE

- **Planurile de punere în aplicare și mecanismele de monitorizare, evaluare și raportare**

Comisia va monitoriza punerea în practică, aplicarea și respectarea acestor dispoziții noi în vederea evaluării eficacității lor. Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament în termen de patru ani de la data aplicării sale.

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

Obiective generale, obiect și definiții (capitolul I)

Capitolul I stabilește obiectivele regulamentului de a consolida solidaritatea la nivelul Uniunii pentru a detecta mai bine amenințările și incidentele de securitate cibernetică și a se pregăti mai bine în acest sens pentru a oferi un răspuns mai bun la acestea și, în special, de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele cibernetice, de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice în întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități comune de răspuns la incidentele de

securitate cibernetică semnificative sau de mare amploare, precum și de a spori reziliența Uniunii prin revizuirea și evaluarea incidentelor semnificative sau de mare amploare. Acest capitol stabilește și acțiunile prin care vor fi atinse aceste obiective: implementarea unui Scut cibernetic european, crearea unui mecanism pentru situații de urgență cibernetică și instituirea unui mecanism de reexaminare a incidentelor de securitate cibernetică. Acesta stabilește, de asemenea, definițiile utilizate în cadrul instrumentului.

Scutul cibernetic european (capitolul II)

Capitolul II instituie Scutul cibernetic european și stabilește diferitele sale elemente și condițiile de participare. În primul rând, acesta anunță obiectivul general al Scutului cibernetic european, și anume de a dezvolta capabilități avansate pentru ca Uniunea să detecteze, să analizeze și să prelucreze date privind amenințările și incidentele cibernetice din Uniune, precum și obiectivele operaționale specifice. Acesta precizează că finanțarea din partea Uniunii pentru Scutul cibernetic european se execută în conformitate cu Regulamentul privind DEP.

În plus, capitolul descrie tipul de entități care formează Scutul cibernetic european. Scutul este format din centrele naționale de operațiuni de securitate (denumite în continuare „SOC naționale”) și din centrele transfrontaliere de operațiuni de securitate (denumite în continuare „SOC transfrontaliere”). Fiecare stat membru participant desemnează un SOC național. Acesta acționează 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. În urma unei cereri de exprimare a interesului, ECCC poate selecta un SOC național pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC și pentru a primi un grant pentru a finanța funcționarea instrumentelor și a infrastructurilor. În cazul în care un SOC național beneficiază de sprijin din partea Uniunii, acesta se angajează să participe la un SOC transfrontalier în termen de doi ani.

SOC-urile transfrontaliere sunt alcătuite dintr-un consorțiu format din cel puțin trei state membre, reprezentate de SOC naționale, care se angajează să colaboreze pentru a-și coordona activitățile de detectare a incidentelor cibernetice și de monitorizare a amenințărilor. În urma unei cereri inițiale de exprimare a interesului, ECCC poate selecta un consorțiu-gazdă pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC și pentru a primi un grant pentru a finanța funcționarea instrumentelor și a infrastructurilor. Membrii consorțiului-gazdă încheie un acord de consorțiu scris care stabilește procedurile lor interne. Acest capitol detaliază apoi cerințele pentru schimbul de informații între participanții la un SOC transfrontalier și pentru schimbul de informații între un SOC transfrontalier și alte SOC transfrontaliere, precum și cu entitățile relevante ale UE. SOC-urile naționale care participă la un SOC transfrontalier fac schimb reciproc de informații relevante legate de amenințările cibernetice, iar detaliile, inclusiv angajamentul de a partaja un volum semnificativ de date și condițiile aferente ar trebui definite într-un acord de consorțiu. SOC-urile transfrontaliere asigură un nivel ridicat de interoperabilitate între ele. De asemenea, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere, specificând

principiile schimbului de informații. 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 informații relevante către EU-CyCLONe, rețelei CSIRT și Comisiei, având în vedere rolurile lor respective de gestionare a crizelor în conformitate cu Directiva (UE) 2022/2555. Capitolul II se încheie prin specificarea condițiilor de securitate pentru participarea la Scutul cibernetic european.

Mecanismul pentru situații de urgență cibernetică (capitolul III)

Capitolul III instituie mecanismul pentru situații de urgență cibernetică pentru a îmbunătăți reziliența Uniunii la amenințările majore la adresa securității cibernetice și pentru a se pregăti, în spiritul solidarității, pentru impactul pe termen scurt al incidentelor sau al crizelor de securitate cibernetică semnificative și de mare amploare și pentru a-l atenua. Acțiunile de punere în aplicare a mecanismului pentru situații de urgență cibernetică sunt sprijinite prin finanțare din partea DEP. Mecanismul prevede acțiuni de sprijinire a pregătirii, inclusiv testarea coordonată a entităților care își desfășoară activitatea în sectoare deosebit de critice, a răspunsului la incidente de securitate cibernetică semnificative sau de mare amploare și a redresării imediate în urma acestora sau acțiuni de atenuare a amenințărilor cibernetice semnificative, precum și acțiuni de asistență reciprocă.

Acțiunile de pregătire în cadrul mecanismului pentru situații de urgență cibernetică includ testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice. După consultarea ENISA și a Grupului de cooperare NIS, Comisia ar trebui să identifice în mod regulat sectoarele sau subsectoarele relevante din rândul sectoarelor cu o importanță critică ridicată enumerate în anexa I la Directiva (UE) 2022/2555, ale căror entități pot face obiectul testării coordonate a pregătirii la nivelul UE.

În scopul punerii în aplicare a acțiunilor propuse de răspuns la incidente, prezentul regulament instituie o rezervă a UE pentru securitate cibernetică, constând în servicii de răspuns la incidente furnizate de furnizori de încredere, selectați în conformitate cu criteriile prevăzute în prezentul regulament. Printre utilizatorii serviciilor din rezerva UE pentru securitate cibernetică se numără autoritățile de gestionare a crizelor cibernetice din statele membre și CSIRT, precum și instituțiile, organele și agențiile Uniunii. Comisia are responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică și poate încredința ENISA, integral sau parțial, funcționarea și administrarea rezervei UE pentru securitate cibernetică.

Pentru a primi sprijin din rezerva UE pentru securitate cibernetică, utilizatorii ar trebui să ia propriile măsuri pentru a atenua efectele incidentului pentru care se solicită sprijinul. Cererile de sprijin din rezerva UE pentru securitate cibernetică ar trebui să includă informațiile relevante necesare cu privire la incident și la măsurile luate deja de utilizatori. Capitolul descrie și modalitățile de punere în aplicare, inclusiv evaluarea cererilor adresate rezervei UE pentru securitate cibernetică.

Regulamentul prevede, de asemenea, principiile de achiziții publice și criteriile de selecție în ceea ce privește furnizorii de încredere ai rezervei UE pentru securitate cibernetică.

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. Acest capitol descrie condițiile și modalitățile detaliate ale unei astfel de participări.

Mecanismul de reexaminare a incidentelor de securitate cibernetică (capitolul IV)

La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA ar trebui să analizeze și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. Analiza și evaluarea ar trebui să fie furnizate de ENISA sub forma unui raport de evaluare a incidentelor adresat rețelei CSIRT, EU-CyCLONe și Comisiei, pentru a le sprijini în îndeplinirea sarcinilor care le revin. În cazul în care incidentul se referă la o țară terță, raportul ar trebui transmis de către Comisie Înaltului Reprezentant. Raportul ar trebui să includă învățămintele desprinse și, după caz, recomandări pentru îmbunătățirea poziției cibernetice a Uniunii.

Dispoziții finale (capitolul V)

Capitolul V conține modificări la Regulamentul privind DEP și prevede obligația Comisiei de a elabora rapoarte periodice pentru evaluarea și revizuirea regulamentului adresate Parlamentului European și Consiliului. Comisia este împuternicită să adopte acte de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 21 pentru: a preciza condițiile pentru această interoperabilitate între SOC-urile 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 cerințe tehnice pentru a asigura un nivel ridicat de securitate a datelor și de securitate fizică a infrastructurii și pentru a proteja interesele de securitate ale Uniunii atunci când face schimb de informații cu entități care nu sunt organisme publice ale statelor membre; 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.

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

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Curții de Conturi[1],

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

având în vedere avizul Comitetului Regiunilor[3],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(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.

(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

[1] JO C […], […], p. […].
[2] JO C , , p. .
[3] JO C , , p. .

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.

(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[4], 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.

(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[5], Recomandarea (UE) 2017/1584 a Comisiei[6], Directiva 2013/40/UE a Parlamentului European și a Consiliului[7] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[8]. 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 și un răspuns mai bun la astfel de situații. De asemenea, statele membre au invitat Comisia să prezinte o

---

4 https://futureu.europa.eu/ro/?locale=ro.

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

6 Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).

7 Directiva 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).

8 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).

propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică în Concluziile Consiliului privind o poziție cibernetică a UE[9].

(6) Comunicarea comună privind politica UE în domeniul apărării cibernetice[10], 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.

(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”).

(8) Pentru a atinge aceste obiective, este necesar, de asemenea, să se modifice Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului[11] 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 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 Concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene aprobate de Consiliu în cadrul reuniunii sale din 23 mai 2022 (9364/22).

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

11 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).

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

(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 financiar și determină, în special, procedura de stabilire și execuție a bugetului Uniunii și prevăd controale privind responsabilitatea actorilor financiari. Normele adoptate în temeiul articolului 322 din TFUE includ, de asemenea, un regim general de condiționalitate pentru protecția bugetului Uniunii, astfel cum este stabilit în Regulamentul (UE, Euratom) 2020/2092 al Parlamentului European și al Consiliului.

(11) 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.

(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[12].

(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

[12] 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).

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.

(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 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 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.

(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.

(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.

(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 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, 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, 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. 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[13].

(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

[13] 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).

în cadrul comunității de apărare cibernetică, în strânsă cooperare cu Înaltul Reprezentant.

(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 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 normelor Uniunii sau al normelor naționale 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 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 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 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[14] 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.

[14] 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) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[15], IPCR[16,] 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.

(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 și statul membru afectat. Atunci când solicită sprijin în cadrul mecanismului pentru situații de urgență 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 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

---

15 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).

16 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.

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[17]. 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 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 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 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. 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

[17] 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.

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.

(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.

(35) Pentru a sprijini instituirea rezervei UE pentru securitate cibernetică, Comisia ar putea lua în considerare posibilitatea de a solicita 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 cibernetică.

(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 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.

(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.

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

(39) Obiectivul prezentului regulament poate fi realizat mai bine la nivelul Uniunii decât de către statele membre. În consecință, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității și cu principiul proporționalității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. Prezentul regulament nu depășește ceea ce este necesar pentru îndeplinirea 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 infrastructuri 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 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;

(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;

(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.

(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:

1. **„Centru transfrontalier de operațiuni de securitate” („SOC transfrontalier”)** înseamnă o platformă multinațională care reunește într-o structură coordonată de rețea SOC-uri naționale din cel puțin trei state membre care formează un consorțiu-gazdă și care este concepută pentru a preveni amenințările și incidentele de securitate cibernetică și pentru a sprijini producerea de informații de înaltă calitate, în special prin schimbul de date din diferite surse, publice și private, precum și prin utilizarea în comun a instrumentelor de ultimă generație și dezvoltarea în comun a capabilităților de detectare, analiză și prevenire și de protecție cibernetică într-un mediu de încredere**;**

2. **„organism public”** înseamnă un organism de drept public astfel cum este definit la articolul 2 alineatul (1) punctul 4 din Directiva 2014/24/UE a Parlamentului European și a Consiliului[18];

3. **„consorțiu-gazdă”** înseamnă un consorțiu alcătuit din state participante, reprezentate de SOC-urile naționale, care au convenit să înființeze și să contribuie la achiziționarea de instrumente și de infrastructură pentru un SOC transfrontalier și la asigurarea funcționării acestuia;

[18] 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).

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

5. **„entități care își desfășoară activitatea în sectoare critice sau deosebit de critice”** înseamnă tipurile de entități enumerate în anexele I și II la 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;

7. **„incident de securitate cibernetică semnificativ”** înseamnă un incident de securitate cibernetică care 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;

11. **„furnizori de încredere”** înseamnă furnizori de servicii de securitate gestionate, astfel cum sunt definiți la articolul 6 punctul 40 din Directiva (UE) 2022/2555, selectați în conformitate cu articolul 16 din prezentul regulament.

Capitolul II

SCUTUL CIBERNETIC EUROPEAN

Articolul 3

Instituirea Scutului cibernetic european

(1) Se instituie o infrastructură paneuropeană interconectată 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 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;

(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;

(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 participa la Scutul cibernetic european, fiecare stat membru desemnează cel puțin un SOC național. SOC național este un organism public.

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.

(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.

(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.

(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.

(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) vizează prevenirea și detectarea incidentelor, răspunsul la incidente sau redresarea în urma acestora sau atenuarea impactului lor;

(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 un volum semnificativ de date 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, acestea asigură un nivel ridicat de interoperabilitate între ele. Pentru a facilita interoperabilitatea dintre SOC-urile transfrontaliere, Comisia poate să precizeze condițiile acestei interoperabilități prin intermediul unor acte de punere în aplicare, după consultarea ECCC. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament.

(4) SOC-urile transfrontaliere încheie acorduri de cooperare între ele, specificând principiile schimbului de informații între platformele transfrontaliere.

Articolul 7

Cooperarea și schimbul de informații cu entitățile Uniunii

(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 Directiva (UE) 2022/2555.

(2) Prin intermediul unor acte de punere în aplicare, Comisia poate stabili modalitățile procedurale pentru schimbul de informații prevăzut la alineatul (1). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament.

Articolul 8

Securitate

(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.

(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. 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.

Capitolul III

MECANISMUL PENTRU SITUAȚII DE URGENȚĂ CIBERNETICĂ

Articolul 9

Instituirea mecanismului pentru situații de urgență cibernetică

(1) Se instituie un mecanism pentru situații de urgență cibernetică pentru a îmbunătăți reziliența Uniunii la amenințările majore 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 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.

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 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.

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.

(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.

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.

(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.

(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.

(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 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 poate încredința 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, 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.

(8) Comisia poate specifica, prin intermediul unor acte de punere în aplicare, tipurile și numărul de servicii de răspuns necesare pentru rezerva UE pentru securitate cibernetică. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2).

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 poate, prin intermediul unor acte de punere în aplicare, să specifice modalitățile detaliate de alocare a serviciilor de sprijin din rezerva UE pentru securitate cibernetică. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2).

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 fără întârziere un răspuns.

(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) 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.

(4) Acordurile menționate la alineatul (3) se pot baza pe modele elaborate de ENISA, după consultarea statelor membre.

(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.

(6) În termen de o lună de la încheierea acțiunii de sprijin, utilizatorii prezintă Comisiei și ENISA 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.

(7) Comisia raportează periodic Grupului de cooperare NIS cu privire la utilizarea și rezultatele sprijinului.

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[19], sprijinul acordat în temeiul prezentului regulament pentru răspunsul la astfel

[19] 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).

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 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 Tratatul privind Uniunea Europeană sau poate contribui la aceasta.

(4) Sprijinul acordat în cadrul mecanismului pentru situații de urgență cibernetică poate face parte din răspunsul comun al Uniunii și al statelor membre în situațiile menționate la articolul 222 din Tratatul privind funcționarea Uniunii Europene.

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.

(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 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 necesare pentru a sprijini serviciul solicitat;

(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) în care poate furniza serviciul;

(j) odată ce se instituite în cadrul Regulamentului (UE) 2019/881 un sistem UE de certificare pentru serviciul de securitate gestionat, furnizorul este certificat în conformitate cu sistemul respectiv.

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 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 REEXAMINARE A INCIDENTELOR DE SECURITATE CIBERNETICĂ

Articolul 18

Mecanismul de reexaminare 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, 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.

(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.

(4) După caz, raportul formulează recomandări 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:

(1) 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”;

(2) se adaugă următoarea literă (g):

„(g) instituirea și gestionarea unui mecanism pentru situații de urgență 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”;

(a) 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[20], cu excepția acțiunilor de punere în aplicare a rezervei UE pentru securitate cibernetică, care sunt puse în aplicare de către Comisie și ENISA.**”;**

(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) 1 629 566 000 EUR pentru obiectivul specific nr. 3 – Securitatea cibernetică și încrederea;

(d) 482 347 000 EUR pentru obiectivul specific nr. 4 – Competențele digitale avansate;”;

(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 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.”;

[20] 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).

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

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

Atunci când îndeplinirea obiectivului unei acțiuni necesită achiziționarea de bunuri și servicii inovatoare, granturile pot fi acordate doar beneficiarilor care sunt autorități contractante sau entități contractante, astfel cum sunt definite în Directivele 2014/24/UE [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/XX, 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) XXX/XXXX [FR reformat], 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/XX, 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) XXX/XXXX [FR reformat], 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 furniza finanțare sub formă de instrumente financiare în cadrul operațiunilor de finanțare mixtă.”

(4) Se adaugă următorul articol 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/XX. În cazul unui conflict între dispozițiile prezentului regulament și articolele 4 și 5 din Regulamentul (UE) 2023/XX, 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 financiar și pot acoperi până la 100 % din costurile eligibile, fără a aduce atingere principiului cofinanțării prevăzut la articolul 190 din Regulamentul financiar. Astfel de granturi sunt acordate și gestionate astfel cum este specificat pentru fiecare obiectiv specific.

Sprijinul sub formă de granturi poate fi acordat direct de ECCC, fără o cerere de propuneri, către SOC-urile naționale menționate la articolul 4 din Regulamentul XXXX și către consorțiul-gazdă menționat la articolul 5 din Regulamentul XXXX, în conformitate cu articolul 195 alineatul (1) litera (d) din Regulamentul financiar.

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

Pentru acțiunile menționate la articolul 10 alineatul (1) litera (c) din Regulamentul 202X/XXXX, 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 XXXX și în conformitate cu articolul 193 alineatul (2) al doilea paragraf litera (a) din Regulamentul financiar, în cazuri justificate în mod corespunzător, costurile pot fi considerate eligibile chiar dacă au fost suportate înainte de depunerea cererii de grant.”;

(6) Anexele I și II se modifică în conformitate cu anexa la prezentul regulament.

Articolul 20

Evaluarea

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.

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*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică vizat(e)

1.3. Obiectul propunerii/inițiativei

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

1.4.2. Obiectiv(e) specific(e)

1.4.3. Rezultatul (rezultatele) și impactul preconizate

1.4.4. Indicatori de performanță

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii" este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

1.6. Durata și impactul financiar ale propunerii/inițiativei

1.7. Metoda (metodele) de execuție a bugetului planificată (planificate)

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

3.2.2. Realizările preconizate finanțate din credite operaționale

3.2.3. Sinteza impactului estimat asupra creditelor administrative

3.2.3.1. Necesarul de resurse umane estimat

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

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 lorpent

1.2. Domeniul (domeniile) de politică vizat(e)

O Europă pregătită pentru era digitală

Investiții strategice europene

Activitatea: Conturarea viitorului digital al Europei

1.3. Obiectul propunerii/inițiativei

☒ o acțiune nouă

☐ o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare[33]

☐ prelungirea unei acțiuni existente

☐ o fuziune sau o redirecționare a uneia sau mai multor acțiuni către o altă/o nouă acțiune

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Regulamentul privind solidaritatea cibernetică va consolida solidaritatea la nivelul Uniunii pentru a detecta mai bine amenințările și incidentele de securitate cibernetică și pentru a se pregăti mai bine și a putea oferi un răspuns mai bun la astfel de situații. Scopul său este:

(a) de a consolida detectarea și conștientizarea comună a situației la nivelul UE cu privire la amenințările și incidentele cibernetice;

(b) de a consolida gradul de pregătire al entităților critice din întreaga UE și solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau de mare amploare, inclusiv prin punerea la dispoziție a sprijinului pentru răspunsul la incidente pentru țările terțe asociate la programul „Europa digitală”;

(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.

1.4.2. Obiectiv(e) specific(e)

Regulamentul privind solidaritatea cibernetică va atinge setul de obiective prin:

[33] Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

(a) implementarea unei infrastructuri paneuropene a centrelor de operațiuni pentru 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; Sprijin pentru răspunsul la incidente este pus, de asemenea, la dispoziția instituțiilor, organelor, oficiilor și agențiilor Uniunii Europene (IOAUE);

Aceste acțiuni vor fi sprijinite prin finanțare din partea DEP, pe care îl va modifica acest instrument legislativ pentru a stabili acțiunile menționate mai sus, pentru a oferi sprijin financiar pentru dezvoltarea acestora și pentru a clarifica condițiile în care se poate beneficia de sprijinul financiar.

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

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă propunerea/inițiativa asupra beneficiarilor vizați/grupurilor vizate.

Propunerea ar aduce beneficii semnificative diferitelor părți interesate. 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.

Aceste acțiuni vor consolida poziția competitivă a industriei și a activităților din Europa în cadrul economiei digitalizate și vor sprijini transformarea digitală a acestora, prin consolidarea nivelului de securitate cibernetică pe piața unică digitală. În special, acesta vizează creșterea rezilienței cetățenilor, a întreprinderilor și a entităților care își desfășoară activitatea în sectoare critice sau deosebit de critice împotriva amenințărilor tot mai mari la adresa securității cibernetice, care pot avea un impact societal și economic devastator. Acest lucru se va realiza prin investiții în instrumente care vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre vor beneficia 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. Acest lucru ar trebui să sprijine, de asemenea, dotarea Europei cu capacități mai puternice în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică.

1.4.4. Indicatori de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

Pentru a promova solidaritatea la nivelul Uniunii, ar putea fi luați în considerare mai mulți indicatori:

(1) Numărul de infrastructuri de securitate cibernetică sau de instrumente achiziționate în comun

(2) Numărul de acțiuni de sprijinire a pregătirii în vederea incidentelor de securitate cibernetică și a răspunsului la acestea în cadrul mecanismului pentru situații de urgență cibernetică.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

Regulamentul ar urma să devină pe deplin aplicabil la scurt timp după adoptarea sa, și anume în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu mai buna coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii” este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Caracterul transfrontalier puternic al amenințărilor cibernetice în general și numărul tot mai mare de riscuri și incidente care au efecte de propagare dincolo de frontiere, sectoare și produse fac ca obiectivele prezentei intervenții să nu poată fi realizate în mod eficace de către statele membre în mod individual și să necesite o acțiune comună și solidaritate la nivelul Uniunii. Experiența combaterii amenințărilor cibernetice generate de războiul împotriva Ucrainei, împreună cu învățămintele desprinse în urma unui exercițiu de securitate cibernetică desfășurat sub președinția franceză (EU CyCLES) au arătat că, pentru a realiza solidaritatea la nivelul UE, ar trebui dezvoltate mecanisme concrete de sprijin reciproc, în special cooperarea cu sectorul privat. În acest context, Concluziile Consiliului din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene invită Comisia să prezinte o propunere privind un nou Fond de răspuns la situații de urgență legate de securitatea cibernetică. Sprijinul și acțiunile la nivelul Uniunii pentru o mai bună detectare a amenințărilor la adresa securității cibernetice și pentru sporirea capacităților de pregătire și de răspuns oferă valoare adăugată deoarece evită duplicarea eforturilor în întreaga Uniune și în statele membre. Aceasta ar conduce la o mai bună exploatare a activelor existente și la o mai bună coordonare și un schimb de informații îmbunătățit cu privire la învățămintele desprinse.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

În ceea ce privește conștientizarea situației și detectarea în cadrul Scutului cibernetic european, ca parte a programului de lucru privind securitatea cibernetică al DEP pentru perioada 2021-2022, au avut loc o cerere de exprimare a interesului pentru achiziționarea în comun de instrumente și infrastructuri pentru crearea de SOC transfrontaliere și o cerere de granturi pentru a permite consolidarea capacităților SOC-urilor care deservesc organizații publice și private.

În ceea ce privește pregătirea și răspunsul la incidente, Comisia a instituit un program pe termen scurt pentru a sprijini statele membre, prin fonduri suplimentare alocate ENISA, cu scopul de a consolida imediat gradul de pregătire și capacitățile de răspuns la incidentele cibernetice majore. Prin aceste fonduri se pot finanța acțiuni de pregătire, cum ar fi efectuare de teste de penetrare cibernetică pe entitățile critice pentru a identifica eventualele vulnerabilități. Se consolidează, de asemenea, posibilitățile de a asista statele membre în cazul unui incident major care ar afecta entitățile critice. Punerea în aplicare de către ENISA a acestui program pe termen

scurt este în curs și a oferit deja informații valoroase relevante care au fost luate în considerare la elaborarea prezentului regulament.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

Regulamentul privind solidaritatea cibernetică se va baza pe acțiunile sprijinite în prezent de Uniune și de statele membre pentru a spori conștientizarea situației și detectarea amenințărilor cibernetice și pentru a răspunde la incidentele de securitate cibernetică transfrontaliere de mare amploare. În plus, instrumentul este coerent cu alte cadre de gestionare a crizelor, inclusiv cu IPCR, cu politica de securitate și apărare comună, inclusiv prin intermediul echipelor de răspuns rapid în domeniul cibernetic, și cu asistența furnizată de un stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană. De asemenea, noua propunere ar completa și ar sprijini structurile dezvoltate în cadrul altor instrumente de securitate cibernetică, cum ar fi Directiva (UE) 2022/2555 (Directiva NIS 2) sau Regulamentul (UE) 2019/881 (Regulamentul privind securitatea cibernetică).

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de realocare a creditelor

Gestionarea domeniilor de acțiune atribuite ENISA corespunde mandatului și sarcinilor sale generale existente. Aceste domenii de acțiune pot necesita profiluri specifice sau noi sarcini, dar acestea pot fi absorbite de resursele existente ale ENISA și soluționate prin realocarea sau conectarea diferitelor atribuții. ENISA pune în aplicare în prezent un program pe termen scurt care a fost instituit în 2022 de către Comisie pentru a consolida imediat gradul de pregătire și capacitățile de răspuns la incidentele cibernetice majore. Printre serviciile vizate se numără posibilitățile de a asista statele membre în cazul unui incident major care ar afecta entitățile critice. Punerea în aplicare de către ENISA a acestui program pe termen scurt este în curs și a oferit deja informații valoroase relevante care au fost luate în considerare la elaborarea prezentului regulament. Resursele alocate pentru programul pe termen scurt ar putea fi, de asemenea, utilizate în contextul prezentului regulament.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☒ **durată limitată**

– ☒ în vigoare de la data adoptării Propunerii de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii de detectare pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor („Regulamentul privind solidaritatea cibernetică”)

– ☒ Impact financiar din 2023 până în 2027 pentru creditele de angajament și din 2023 până în 2031 pentru creditele de plată[34].

☐ **durată nelimitată**

– punere în aplicare cu o perioadă de creștere în intensitate din AAAA până în AAAA,

– urmată de o perioadă de funcționare la capacitate maximă.

1.7. Metoda (metodele) de execuție a bugetului planificată (planificate)[35]

☒ **Gestiune directă** asigurată de Comisie

– ☒ prin intermediul departamentelor sale, inclusiv al personalului din delegațiile Uniunii;

– ☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☒ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea;

– ☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

– ☐ BEI și Fondului European de Investiții;

– ☒ organismelor menționate la articolele 70 și 71 din Regulamentul financiar;

– ☐ organismelor de drept public;

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să li se furnizeze garanții financiare adecvate;

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care primește garanții financiare adecvate;

– ☐ organismelor sau persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații”.*

---

34 Acțiunile prevăzute în act ar trebui să fie sprijinite de următorul cadru financiar multianual.

35 Explicații detaliate privind metodele de execuție a bugetului, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

Observații

Acțiunile legate de Scutul cibernetic european vor fi puse în aplicare de ECCC. Până când ECCC va avea capacitatea de a-și executa propriul buget, Comisia Europeană va pune în aplicare acțiunile în cadrul gestiunii directe în numele ECCC. ECCC poate selecta entități pe baza cererilor de exprimare a interesului pentru a participa la achiziții publice comune de instrumente. ECCC poate acorda granturi pentru a finanța funcționarea acestor instrumente și infrastructuri. În plus, ECCC poate acorda granturi pentru acțiuni de pregătire în cadrul mecanismului pentru situații de urgență cibernetică. Comisia are responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Comisia poate încredința ENISA funcționarea și administrarea rezervei UE pentru securitate cibernetică, integral sau parțial, prin intermediul unor acorduri de contribuție. Acțiunile atribuite ENISA în temeiul prezentului regulament sunt în conformitate cu mandatul său existent. Printre aceste acțiuni se numără: (i) sprijinirea Grupului de cooperare NIS în elaborarea acțiunilor de pregătire în conformitate cu evaluările riscurilor; (ii) sprijinirea Comisiei în ceea ce privește instituirea și supravegherea punerii în aplicare a rezervei UE pentru securitate cibernetică, inclusiv primirea și prelucrarea cererilor de sprijin; (iii) elaborarea de modele pentru a facilita depunerea cererilor de sprijin și a acordurilor specifice care urmează să fie încheiate între furnizorul de servicii și utilizatorul căruia i se acordă sprijin în cadrul rezervei UE pentru securitate cibernetică; (iv) analizarea și evaluarea amenințărilor, a vulnerabilităților și a acțiunilor de atenuare în ceea ce privește un anumit incident de securitate cibernetică semnificativ sau de mare amploare și pregătirea de rapoarte cu privire la acestea. Toate aceste misiuni sunt estimate la aproximativ 7 ENI din resursele existente ale ENISA, bazându-se deja pe expertiza și lucrările pregătitoare pe care le desfășoară în prezent ENISA în cadrul proiectului-pilot al sprijinului de urgență pentru pregătirea pentru incidente și răspunsul la acestea.

2. MĂSURI DE GESTIUNE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente monitorizării și raportării.

Comisia va monitoriza punerea în practică, aplicarea și respectarea acestor dispoziții noi în vederea evaluării eficacității lor. Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament în termen de patru ani de la data aplicării sale.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Regulamentul introduce un cadru pentru punerea în aplicare a finanțării UE în vederea creșterii rezilienței în materie de securitate cibernetică prin acțiuni de consolidare a capabilităților de detectare, de răspuns și de redresare în cazul unor incidente de securitate cibernetică semnificative și de mare amploare. Unitățile din cadrul DG CNECT responsabile cu domeniul de politică vor gestiona punerea în aplicare a directivei.

Este necesar să se aloce resurse adecvate serviciilor Comisiei pentru a le permite să facă față acestor noi sarcini. Se estimează că punerea în aplicare a noului regulament va necesita 6 ENI (3 AD și 3 CA) pentru a acoperi următoarele sarcini:

- stabilirea acțiunilor de pregătire în conformitate cu evaluările riscurilor;
- asigurarea interoperabilității între platformele SOC transfrontaliere;
- elaborarea unor posibile acte de punere în aplicare (două pentru SOC și două pentru mecanismul pentru situații de urgență cibernetică);
- gestionarea acordurilor de găzduire și de utilizare pentru SOC;
- instituirea și gestionarea rezervei UE pentru securitate cibernetică, direct sau prin intermediul unui acord de contribuție la ENISA. În cazul unui acord de contribuție la ENISA, elaborarea și supravegherea punerii în aplicare a acordului de contribuție pentru sarcinile atribuite ENISA;
- participarea la grupurile de consultare convocate de ENISA pentru a examina și a evalua incidentele de securitate cibernetică semnificative și de mare amploare și pentru a pregăti rapoartele.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Un risc identificat pentru Scutul cibernetic european este acela că statele membre nu partajează un volum suficient de informații relevante privind amenințările cibernetice nici în cadrul platformelor SOC transfrontaliere, nici între platformele transfrontaliere și alte entități relevante la nivelul UE. Pentru a atenua aceste riscuri, alocarea finanțării va urma unei cereri de exprimare a interesului în care statele membre se angajează să comunice o anumită cantitate de informații la nivelul UE. Acest angajament va fi apoi oficializat printr-un acord de găzduire și de utilizare, care va conferi ECCC competența de a efectua audituri pentru a se asigura că

instrumentele și infrastructura achiziționate în comun sunt utilizate în conformitate cu acordul. Angajamentele privind un nivel ridicat de schimb de informații în cadrul SOC-urilor transfrontaliere vor fi formalizate într-un acord de consorțiu.

Un risc identificat pentru mecanismul pentru situații de urgență cibernetică este acela că utilizatorii care participă la mecanism nu iau suficiente măsuri pentru a asigura pregătirea în fața atacurilor cibernetice. Din acest motiv, pentru a putea primi sprijin din rezerva UE pentru securitate cibernetică, utilizatorii sunt obligați să ia astfel de măsuri de pregătire. Atunci când depun cererile de sprijin către rezerva UE pentru securitate cibernetică, utilizatorii trebuie să explice ce măsuri au fost deja luate pentru a răspunde incidentului, acestea fiind avute în vedere la evaluarea cererilor pentru rezerva UE pentru securitate cibernetică.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

Întrucât normele de participare la programul „Europa digitală” aplicabile sprijinului acordat în temeiul Regulamentului privind securitatea cibernetică sunt similare cu cele pe care Comisia le va utiliza în programele sale de lucru și în condițiile unei populații de beneficiari cu un profil de risc similar cu cel al programelor care se află sub gestiune directă, se poate preconiza că marja de eroare va fi similară cu cea prevăzută de Comisie pentru programul „Europa digitală”, și anume de natură să ofere o asigurare rezonabilă că riscul de eroare pe parcursul perioadei de cheltuieli multianuale este cuprins, pe o bază anuală, în intervalul 2-5 %, cu scopul final de a se obține o rată reziduală de eroare cât mai apropiată de 2 % la încheierea programelor multianuale, după ce a fost luat în considerare impactul financiar al tuturor auditurilor și măsurilor corective și de recuperare.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

În cazul Scutului cibernetic european, ECCC va avea competența de a audita, pe baza accesului la informații și a controalelor la fața locului, instrumentele și infrastructurile achiziționate în comun, în conformitate cu acordul de găzduire și de utilizare care urmează să fie semnat între consorțiul-gazdă și ECCC.

Măsurile existente de prevenire a fraudei aplicabile instituțiilor, organelor și agențiilor Uniunii se vor aplica și creditelor suplimentare necesare pentru punerea în aplicare a prezentului regulament.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul de cheltuieli	Contribuție			
	Numărul	Dif./ Nedif.[36]	din partea țărilor AELS[37]	din partea țărilor candidate și a candidaților potențiali[38]	din partea altor țări terțe	alte venituri alocate
1	02 04 01 10 – programul „Europa digitală” – securitate cibernetică	Dif.	DA	DA	NU	NU
1	02 04 01 11 – programul „Europa digitală” – Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică	Dif.	DA	DA	NU	NU
1	02 04 03 – programul „Europa digitală” – inteligență artificială	Dif.	DA	DA	NU	NU
1	02 04 04 – programul „Europa digitală” – Competențe	Dif.	DA	DA	NU	NU
1	02 01 30 - Cheltuieli de sprijin pentru programul „Europa digitală”	Nedif.	DA	DA	NU	NU

[36] Dif. = credite diferențiate / Nedif. = credite nediferențiate.
[37] AELS: Asociația Europeană a Liberului Schimb.
[38] Țările candidate și, după caz, țările potențial candidate.

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☒ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	Numărul	1 **Piața unică, inovare și sectorul digital**

Propunerea nu va crește nivelul total al angajamentelor din cadrul programului „Europa digitală”. Într-adevăr, contribuția la această inițiativă constă într-o redistribuire a angajamentelor care provin din OS2 și OS4 pentru a consolida bugetul pentru OS3 și ECCC. Orice majorare a angajamentelor din cadrul programului „Europa digitală” care rezultă dintr-o revizuire a CFM ar putea fi utilizată în scopul prezentei inițiative.

DG CONNECT			Anul **2025**	Anul **2026**	Anul **2027**	Anul **2028+**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
○ Credite operaționale										
Linia bugetară[39] 02.040110 (redistribuire din 02.0403 și 02.0404)	Angajamente	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Plăți	(2a)	15,000	15,000	6,000					**36,000**
Linia bugetară 02.040111.02 (redistribuire din 02.0403 și 02.0404)	Angajamente	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Plăți	(2b)	8,450	18,200	25,250	12,100				**64,000**
Credite cu caracter administrativ finanțate din bugetul unor programe specifice[40]										
Linia bugetară 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450

[39] În conformitate cu nomenclatura bugetară oficială.

[40] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

TOTAL credite pentru DG CONNECT	Angajamente	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Plăți	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ TOTAL credite operaționale	Angajamente	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Plăți	(5)	23,450	33,200	31,250	12,100				**100,000**
○ TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice		(6)	0,150	0,150	0,150	p.m.				**0,450**
TOTAL credite în cadrul RUBRICII 1 din cadrul financiar multianual	Angajamente	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Plăți	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

<u>În cazul în care propunerea/inițiativa afectează mai multe rubrici operaționale, a se repeta secțiunea de mai sus:</u>

○ TOTAL credite operaționale (toate rubricile operaționale)	Angajamente	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Plăți	(5)	23,450	33,200	31,250	12,100				**100,000**
TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice (toate rubricile operaționale)		(6)	0,150	0,150	0,150					**0,450**
TOTAL credite în cadrul RUBRICILOR 1-6 din cadrul financiar multianual (Suma de referință)	Angajamente	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Plăți	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Rubrica din cadrul financiar multianual	**7**	„Cheltuieli administrative”

Această secțiune ar trebui completată utilizând „datele bugetare cu caracter administrativ” care trebuie introduse mai întâi în anexa la fișa financiară legislativă (anexa 5 la Decizia Comisiei privind normele interne de execuție a secțiunii „Comisia” din bugetul general al Uniunii Europene), încărcată în DECIDE pentru consultarea interservicii.

milioane EUR (cu trei zecimale)

		Anul **2025**	Anul **2026**	Anul **2027**	Anul **2028+**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
DG: CONNECT									
○ Resurse umane		0,786	0,786	0,786	p.m.				**2,358**
○ Alte cheltuieli administrative		0,035	0,035	0,035	p.m.				**0,105**
TOTAL DG CONNECT	Credite	**0,821**	**0,821**	**0,821**					**2,463**

TOTAL credite în cadrul RUBRICII 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	**0,821**	**0,821**	**0,821**					**2,463**

milioane EUR (cu trei zecimale)

		Anul **2025**	Anul **2026**	Anul **2027**	Anul **2028+**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1-7 din cadrul financiar multianual	Angajamente	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Plăți	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Realizările preconizate finanțate din credite operaționale

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul **N**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tip[41]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Total nr.	Total costuri
OBIECTIVUL SPECIFIC NR. 1[42]…																		
- Realizare																		
- Realizare																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2 …																		
- Realizare																		
Subtotal pentru obiectivul specific nr. 2																		
TOTALURI																		

41 Realizările se referă la produsele și serviciile care trebuie furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

42 Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

3.2.3. Sinteza impactului estimat asupra creditelor administrative

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul 2025	Anul r 2026	Anul 2027	Anul N+3	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
RUBRICA 7 din cadrul financiar multianual								
Resurse umane	0,786	0,786	0,786					**2,358**
Alte cheltuieli administrative	0,035	0,035	0,035					**0,105**
Subtotal de la RUBRICA 7 din cadrul financiar multianual	**0,821**	**0,821**	**0,821**					**2,463**

În afara RUBRICII 7[43] din cadrul financiar multianual								
Resurse umane								
Alte cheltuieli cu caracter administrativ	0,150	0,150	0,150					**0,450**
Subtotal în afara RUBRICII 7 din cadrul financiar multianual	**0,150**	**0,150**	**0,150**					**0,450**

TOTAL	**0,971**	**0,971**	**0,971**					**2,913**

Necesarul de credite pentru resursele umane și pentru alte cheltuieli cu caracter administrativ va fi acoperit de creditele direcției generale (DG) respective care sunt deja alocate pentru gestionarea acțiunii și/sau au fost redistribuite intern în cadrul DG-ului respectiv, completate, după caz, cu resurse suplimentare care ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

[43] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.3.1. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ☒ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări în echivalent normă întreagă

		Anul **2025**	Anul **2026**	Anul 2027	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
O Posturi din schema de personal (funcționari și agenți temporari)								
20 01 02 01 (la sediu și în reprezentanțele Comisiei)		3	3	3				
20 01 02 03 (delegații)								
01 01 01 01 (cercetare indirectă)								
01 01 01 11 (cercetare directă)								
Alte linii bugetare (a se preciza)								
O Personal extern (în echivalent normă întreagă: ENI)[44]								
20 02 01 (AC, END, INT din „pachetul global")		3	3	3				
20 02 03 (AC, AL, END, INT și JPD în delegații)								
XX 01 xx **yy zz** [45]	- la sediu							
	- în delegații							
01 01 01 02 (AC, END, INT - cercetare indirectă)								
01 01 01 12 (AC, END, INT – cercetare directă)								
Alte linii bugetare (a se preciza)								
TOTAL		**6**	**6**	**6**				

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar	- stabilirea acțiunilor de pregătire în conformitate cu evaluările riscurilor (art. 11) - elaborarea unor posibile acte de punere în aplicare (două pentru SOC și două pentru mecanismul pentru situații de urgență cibernetică) - gestionarea acordurilor de găzduire și de utilizare pentru SOC; - instituirea și gestionarea rezervei UE pentru securitate cibernetică, direct sau prin intermediul unui acord de contribuție la ENISA.
Personal extern	sub supravegherea unui funcționar oficial - stabilirea acțiunilor de pregătire în conformitate cu evaluările riscurilor (art. 11) - elaborarea unor posibile acte de punere în aplicare (două pentru SOC și două pentru mecanismul pentru situații de urgență cibernetică) - gestionarea acordurilor de găzduire și de utilizare pentru SOC; - instituirea și gestionarea rezervei UE pentru securitate cibernetică, direct sau prin intermediul unui acord de contribuție la ENISA.

[44] AC = agent contractual; AL= agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

[45] Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA").

3.2.4. *Compatibilitatea cu cadrul financiar multianual actual*

Propunerea/inițiativa:

– [X] poate fi finanțată integral prin realocarea creditelor în cadrul rubricii relevante din cadrul financiar multianual (CFM)

A se explica reprogramarea necesară, precizându-se liniile bugetare vizate și sumele aferente. Vă rugăm să furnizați un tabel Excel în cazul unei reprogramări de proporții.

	2023	2024	2025	2026	2027	Total
OS1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
OS2 inițial	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Către inițiativa cibernetică			18 000 000	28 000 000	19 000 000	65 000 000
OS2 NOU	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
OS3 DB 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
De la OS2-OS4			15 000 000	15 000 000	6 000 000	36 000 000
OS3 Nou	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC inițial	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
De la OS2-OS4			13 000 000	23 000 000	28 000 000	64 000 000
ECCC Nou	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
OS4 inițial	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Către inițiativa cibernetică			10 000 000	10 000 000	15 000 000	35 000 000
OS4 NOU	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] necesită utilizarea marjei nealocate din cadrul rubricii corespunzătoare din CFM și/sau utilizarea instrumentelor speciale, astfel cum sunt definite în Regulamentul privind CFM

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, sumele aferente și instrumentele propuse a fi utilizate.

– [ ] necesită revizuirea CFM

A se explica necesitatea efectuării acestei acțiuni, precizând rubricile și liniile bugetare vizate, precum și sumele aferente.

3.2.5. *Contribuțiile terților*

Propunerea/inițiativa:

– [X] nu prevede cofinanțare din partea terților

– [ ] prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu 3 zecimale)

	Anul **N**[46]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

[46] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

3.3. Impactul estimat asupra veniturilor

– ☒ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

  – ☐ asupra resurselor proprii

  – ☐ asupra altor venituri

  – vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli ☐

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[47]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
Articolul …….								

Pentru veniturile alocate, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

[…]

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice alte informații).

[…]

[47] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.