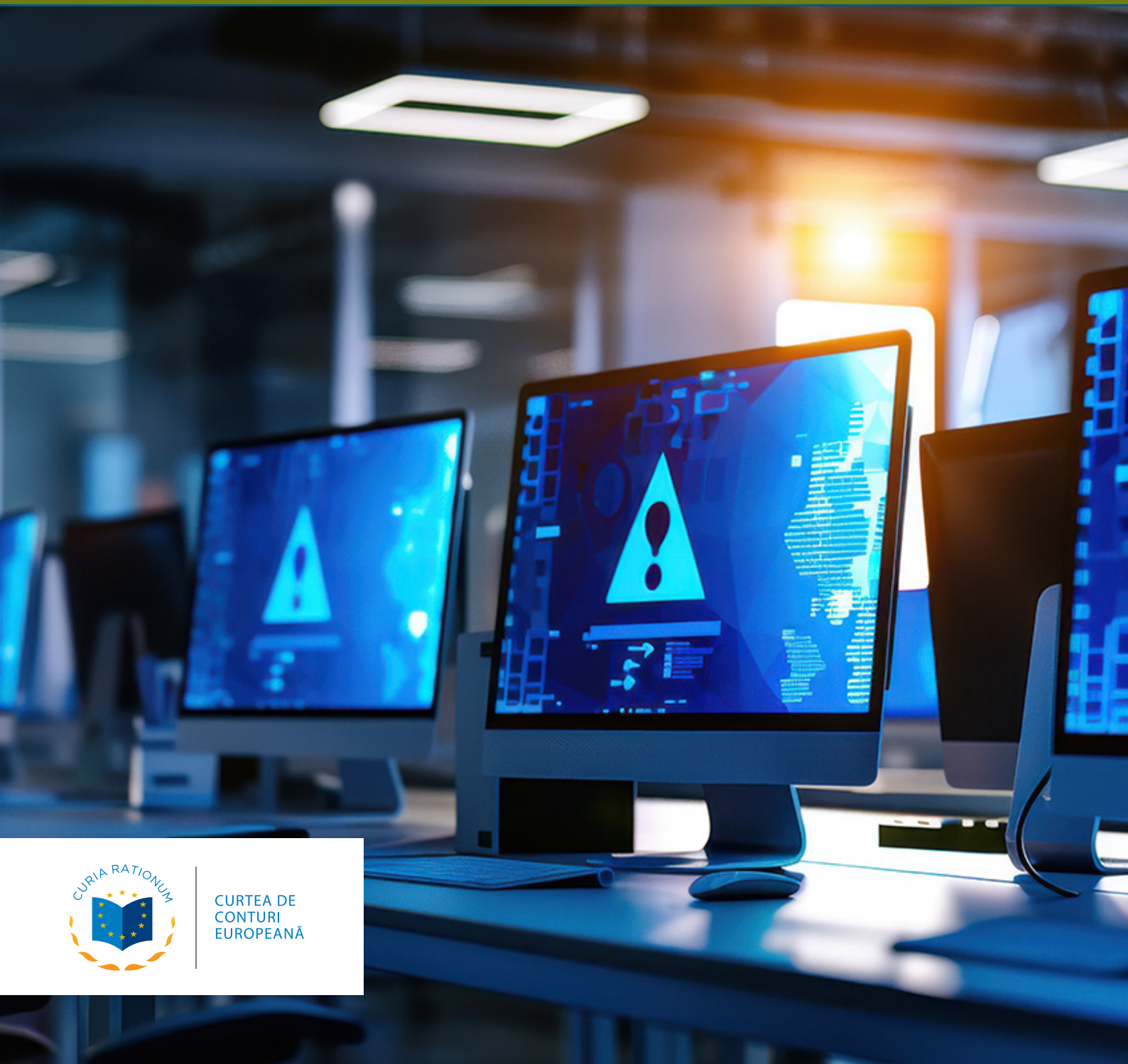
RAPORTUL SPECIAL 19/2026 **RO**

Detectarea incidentelor de securitate cibernetică și răspunsul la acestea

Cadrul de cooperare al UE înregistrează progrese, dar, din cauza întârzierilor în punerea în aplicare și a schimbului limitat de informații, nu este decât parțial eficace



CURIA RATIONUM
CURTEA DE CONTURI EUROPEANĂ

Cuprins

Puncte

01-23 | Mesajele principale 01

01-07 | De ce este important acest domeniu

08-23 | Ce a constatat și ce recomandă Curtea

24-01 | Observațiile Curții, în detaliu 02

24-74 | Rețelele și mecanismele de securitate cibernetică ale UE sprijină cooperarea și răspunsul, însă eficacitatea lor este redusă din cauza schimbului limitat de informații și a punerii în aplicare incomplete

24-51 | Rețelele UE facilitează cooperarea între statele membre, dar schimbul limitat de informații le reduce valoarea adăugată

52-61 | Rezerva UE pentru securitate cibernetică facilitează mobilizarea rapidă a serviciilor de răspuns la incidente

62-74 | Sistemul european de alertă în materie de securitate cibernetică urmărește să consolideze capacitățile de detectare a amenințărilor, dar nu este operațional

75-01 | Proiectele finanțate de UE prin programul „Europa digitală” vizează consolidarea securității cibernetice, dar întâmpină provocări legate de punerea în aplicare și de raportare

75-81 | Din cauza întârzierilor la înființare, Comunitatea de competențe în materie de securitate cibernetică nu a reușit să modeleze programele de lucru ale „Europa digitală” în funcție de propriile nevoi

82-96 | Proiectele finanțate de UE urmăresc obiective relevante, dar multe dintre ele se confruntă cu probleme operaționale

97-01 | Majoritatea proiectelor finanțate de UE au cadre de performanță inadecvate, iar datele privind performanța componentei de securitate cibernetică a programului „Europa digitală” nu sunt exacte

Anexe

Anexa I – Informații despre audit

Anexa II – Peisajul securității cibernetice din UE

Anexa III – Acțiunile în materie de securitate cibernetică selectate

Anexa IV – Evaluarea Curții de Conturi Europene cu privire la proiectele de securitate cibernetică finanțate de UE

Acronime

Glosar

Răspunsurile Comisiei

Răspunsurile Centrului european de competențe în materie de securitate cibernetică (ECCC)

Răspunsurile Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA)

Calendar

Echipa de audit

01

Mesajele principale

De ce este important acest domeniu

01 Pe măsură ce economia și viața noastră de zi cu zi devin mai digitalizate, cresc și riscurile de atacuri cibernetice. Securitatea cibernetică desemnează „activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice”[1]. Este nevoie de o abordare holistică pentru a preveni și a detecta amenințările cibernetice, pentru a răspunde la acestea și pentru a se redresa în urma lor.

02 Peisajul securității cibernetice din UE reunește numeroși actori civili publici și privați de la nivel regional, național și de la nivelul UE. În același timp, securitatea cibernetică este un element-cheie al securității și apărării naționale.

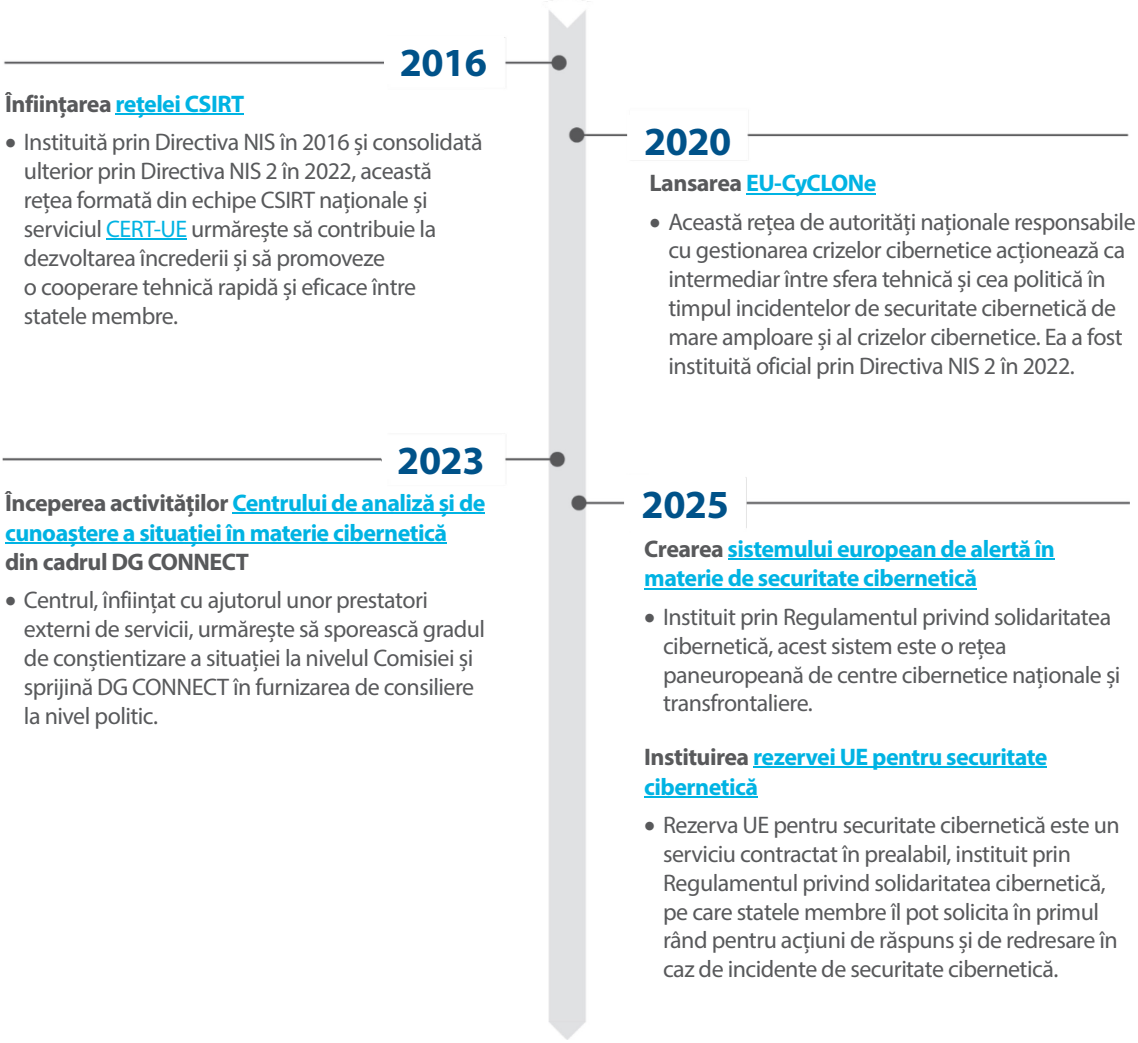
03 Statele membre sunt cele cărora le revine responsabilitatea principală pentru prevenirea, pregătirea și răspunsul în caz de incidente și crize cibernetice care le afectează. Dat fiind că aceste evenimente pot afecta buna funcționare a pieței interne, UE joacă și ea un rol important în cazul unui incident semnificativ sau al unei crize. În ultimii ani, ea și-a consolidat cadrul de reglementare în materie de securitate cibernetică, aflat în continuă evoluție[2], și a instituit rețele și mecanisme, astfel cum se ilustrează în ***figura 1*** de mai jos și în ***anexa II***.

---

[1] Regulamentul (UE) 2019/881 (Regulamentul privind securitatea cibernetică).

[2] De exemplu, Comisia a propus Regulamentul omnibus în domeniul digital în noiembrie 2025 și o versiune revizuită a Regulamentului UE privind securitatea cibernetică în ianuarie 2026.

Figura 1 | Rețelele și mecanismele de securitate cibernetică ale UE în perioada 2016-2025



CSIRT: echipe de intervenție în caz de incidente de securitate informatică
DG CONNECT: Direcția Generală Rețele de Comunicare, Conținut și Tehnologie
EU-CyCLONe: Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice
Directiva NIS: Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune
Directiva NIS 2: Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune

Sursa: Curtea de Conturi Europeană.

04 În actualul cadru financiar multianual 2021-2027, principala sursă de finanțare pentru securitatea cibernetică este programul „Europa digitală”. Acesta dispune de un buget total de 8,1 miliarde de euro, din care 1,4 miliarde sunt alocate consolidării securității cibernetice.

05 Obiectivul auditului Curții de Conturi Europene a fost de a evalua dacă acțiunile UE reușesc să faciliteze detectarea incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsul la acestea. Curtea a verificat dacă acest lucru era valabil pentru:

- rețelele și mecanismele de la nivelul UE [și anume, rețeaua echipelor de intervenție în caz de incidente de securitate informatică (rețeaua CSIRT), Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), sistemul european de alertă în materie de securitate cibernetică, Centrul de analiză și de cunoaștere a situației în materie cibernetică (*cyber situation centre*) și rezerva UE pentru securitate cibernetică];
- acțiunile finanțate în cadrul programului „Europa digitală”.

06 Curtea se așteaptă ca observațiile sale să contribuie la consolidarea rezilienței cibernetice a UE prin îmbunătățirea eficacității și eficienței rețelelor și mecanismelor UE, precum și a modului în care sunt selectate și monitorizate acțiunile finanțate de UE.

07 Auditul acoperă perioada cuprinsă între 2022 și 2025. El se bazează pe: verificare documentară, o analiză a documentelor relevante, vizite de audit în trei state membre (Irlanda, Grecia și Italia), chestionare scrise și interviuri cu părțile interesate relevante. În ***anexa I*** sunt prezentate informații generale suplimentare și detalii privind sfera și abordarea auditului.

Ce a constatat și ce recomandă Curtea

08 În general, Curtea concluzionează că acțiunile UE facilitează doar parțial detectarea incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsul la acestea. A fost instituit treptat un cadru de cooperare, dar se depun în continuare eforturi pentru ca acesta să devină pe deplin operațional. Schimbul limitat de informații, deficiențele de raportare și întârzierile semnificative în punerea în aplicare împiedică rețelele și mecanismele UE să își atingă întregul potențial. Proiectele finanțate prin programul „Europa digitală” urmăresc obiective relevante, dar mai multe dintre ele se confruntă cu provocări operaționale și cu întârzieri și există deficiențe în cadrul general de monitorizare a performanței.

09 Cadrul actual al rețelelor și mecanismelor UE de facilitare a detectării incidentelor de securitate cibernetică semnificative și a răspunsului la acestea a fost dezvoltat treptat. În 2025, Consiliul a adoptat Planul de acțiune pentru gestionarea crizelor cibernetice, care stabilește cadrul UE în acest domeniu. Curtea a constatat că planul respectiv clarifică în mare măsură rolurile și responsabilitățile în materie de gestionare a crizelor cibernetice la nivelul UE. Cu toate acestea, nu s-au stabilit încă în mod formal aranjamentele procedurale care să reglementeze cooperarea dintre rețeaua CSIRT (înființată în 2016) și EU-CyCLONe (instituită oficial în 2023) (punctele ***24***-***30***).

10 Curtea a constatat că schimbul de informații prin intermediul acestor rețele este limitat, din mai multe motive: în principal întârzieri în transpunerea Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2), dificultăți în a stabili dacă un incident are sau nu un impact transfrontalier și legislații în materie de securitate națională care împiedică schimbul de informații. Valoarea adăugată a rețelelor se reduce în mod semnificativ dacă statele membre nu sunt dispuse să facă schimb în timp util de informații cu caracter operațional (punctele ***31***-***44***).

Recomandarea 1

Să se consolideze schimbul de informații între statele membre

Pentru a îmbunătăți detectarea incidentelor de securitate cibernetică și răspunsul la acestea, Comisia, cu sprijinul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), ar trebui:

(a) să propună Grupului de cooperare privind securitatea rețelelor și a informațiilor să efectueze o analiză detaliată a restricțiilor de securitate națională care limitează schimbul de informații și care afectează reziliența cibernetică a UE și să identifice soluții juridice și tehnice pentru a îmbunătăți schimbul de informații, cu respectarea, în același timp, a limitelor impuse de securitatea națională;

(b) fără a aduce atingere deciziilor colegiuitorilor, să se asigure, în colaborare cu statele membre, că punctul unic de contact pentru raportarea incidentelor propus de Regulamentul Omnibus în domeniul digital poate detecta potențialele incidente transfrontaliere;

(c) să depună eforturi pentru găsirea unor soluții care să permită raportarea în timp real a incidentelor către ENISA.

Data-țintă pentru punerea în aplicare a recomandării: 2027 pentru literele (a) și (b) și 2028 pentru litera (c).

11 În 2022, Comisia și-a înființat propriul „Centru de analiză și de cunoaștere a situației în materie cibernetică” pentru a-și îmbunătăți capacitatea de înțelegere a contextului cibernetic, cu scopul de a-și sprijini responsabilitățile instituționale în materie de gestionare a crizelor. Funcționarea centrului este sprijinită în mare măsură printr-un contract cu prestatori externi de servicii. Curtea a constatat că activitatea desfășurată de aceștia se suprapune, parțial, cu cea a Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) în ceea ce privește conștientizarea situației și monitorizarea amenințărilor. Curtea consideră că, în stabilirea arhitecturii acestui centru, nu s-a valorificat suficient potențialul de raționalizare, prin utilizarea informațiilor deja disponibile la nivelul Comisiei și al ENISA. În plus, lipsa unui plan cuprinzător și detaliat pentru perioada de după expirarea contractului reprezintă un risc la adresa funcționării centrului după 2026 (punctele ***45***-***51***).

Recomandarea 2

Să se raționalizeze capacitățile UE de conștientizare a situației în materie de securitate cibernetică și să se optimizeze diseminarea informațiilor

Pentru a îmbunătăți eficiența, Comisia ar trebui ca, în colaborare cu ENISA, să evalueze fezabilitatea achiziției și analizei comune de informații necesare pentru conștientizarea situației. Ea ar trebui, de asemenea, să pună aceste informații și rapoartele conexe privind amenințările cibernetice la dispoziția tuturor serviciilor și agențiilor relevante ale UE.

Data-țintă pentru punerea în aplicare a recomandării: 2027.

12 Regulamentul privind solidaritatea cibernetică din 2024 înființează rezerva UE pentru securitate cibernetică, cu rolul de a ajuta statele membre să răspundă la incidentele majore de securitate cibernetică și să se redreseze în urma acestora. Rezerva constă într-un grup de prestatori de servicii selectați pentru fiecare stat membru, capabili să răspundă la incidente în permanență. Această abordare contribuie la abordarea cerințelor specifice ale statelor membre și ajută la consolidarea încrederii, însă bugetul disponibil este împărțit în mod egal între acestea și nu ține seama de nevoile specifice ale fiecărei țări (punctele ***52***-***57***).

13 Curtea consideră că utilizarea de furnizori contractați în prealabil permite o mobilizare rapidă a serviciilor de răspuns la incidente. Rezerva UE pentru securitate cibernetică are drept prim scop să sprijine răspunsul și redresarea, însă, atunci când nu este utilizată pentru răspunsul la incidente, ea poate fi utilizată pentru pregătire. Această abordare flexibilă poate preveni situațiile în care servicii preplătite să nu fie utilizate. Pe de altă parte însă, rezerva riscă să fie utilizată în principal pentru pregătire, contrar scopului său preconizat, și anume de răspuns (punctele ***58***-***61***).

14 Sistemul european de alertă în materie de securitate cibernetică este o rețea de centre cibernetice naționale și transfrontaliere cu rolul de a îmbunătăți detectarea și analiza amenințărilor cibernetice, precum și răspunsul la acestea. Curtea a constatat că, la momentul auditului, din cauza unor întârzieri importante în achiziționarea de instrumente și servicii, cele două centre (ATHENA și ENSOC) nu erau de fapt operaționale încă, iar sistemul european de alertă în materie de securitate cibernetică nu începuse nici el să funcționeze (punctele ***62***-***70***).

15 Unul dintre obiectivele-cheie ale sistemului european de alertă în materie de securitate cibernetică este de a încuraja schimbul de informații utile între clustere de state membre. Acest sistem este capabil să soluționeze unele dintre problemele legate de schimbul de informații, însă integrarea centrelor cibernetice într-un peisaj al securității cibernetice deja complex rămâne o mare provocare. Curtea a constatat că nu se instituiseră încă acordurile de cooperare, taxonomia comună și standardele de interoperabilitate necesare pentru ca sistemul european de alertă în materie de securitate cibernetică să funcționeze pe deplin (punctele ***71***-***74***).

Recomandarea 3

Să se integreze sistemul european de alertă în materie de securitate cibernetică în peisajul securității cibernetice din UE

Comisia, împreună cu ENISA și cu statele membre, ar trebui să se asigure că sunt instituite mecanisme de cooperare și standarde de interoperabilitate pentru a facilita schimbul de informații între centrele transfrontaliere care fac parte din sistemul european de alertă în materie de securitate cibernetică, rețeaua CSIRT și EU-CyCLONe.

Data-țintă pentru punerea în aplicare a recomandării: 2028.

16 În 2018, Comisia a propus crearea Centrului european de competențe în materie de securitate cibernetică (ECCC), care să gestioneze, începând din 2021, componenta de securitate cibernetică a programului „Europa digitală”. Regulamentul privind ECCC a solicitat crearea unei Comunități de competențe în materie de securitate cibernetică, alcătuită din reprezentanți ai industriei și ai organizațiilor universitare și de cercetare. Mai mulți membri selectați din cadrul acestei comunități urmau să formeze un grup consultativ strategic (punctele ***75***-***76***).

17 Curtea a constatat întârzieri atât în dobândirea autonomiei financiare a ECCC, cât și în instituirea Comunității de competențe în materie de securitate cibernetică și a grupului consultativ strategic. Altfel spus, Comunitatea de competențe în materie de securitate cibernetică și grupul consultativ strategic nu au fost în măsură să contribuie la elaborarea programelor de lucru din cadrul „Europa digitală”. Curtea este de părere că aceasta a fost o oportunitate ratată (punctele ***77***-***81***).

18 Curtea a constatat că toate proiectele examinate urmăreau obiective relevante care contribuie la atingerea obiectivelor în materie de securitate cibernetică ale programului „Europa digitală”. S-au identificat însă cazuri în care calitatea sau rezultatele obținute nu erau satisfăcătoare, în principal din cauza întârzierilor în punerea în aplicare (punctele ***82***-***87***).

19 Regulamentul „Europa digitală” prevede că, din motive de securitate, finanțarea pentru securitatea cibernetică poate fi limitată la entități stabilite în statele membre și controlate de acestea sau de resortisanți ai acestora. Serviciul central de validare din cadrul Agenției Executive Europene pentru Cercetare efectuează, în numele ECCC, această evaluare privind proprietatea și controlul (punctele ***88***-***91***).

20 În cazul sprijinului financiar pentru terți, evaluarea referitoare la proprietate și la control se află în responsabilitatea beneficiarilor proiectului, care se bazează pe propria abordare și metodologie. Curtea a constatat că ECCC nu validează metodologia acestora și nici nu efectuează verificări pentru a se asigura că părțile terțe selectate sunt deținute și controlate de UE. Curtea este de părere că există un risc semnificativ ca beneficiarii să nu aibă capacitatea de a efectua aceste controale în mod corespunzător. Acest risc nu a fost atenuat în mod adecvat și ar putea duce la expunerea unor infrastructuri sensibile, a unor date operaționale și a unor tehnologii critice din punctul de vedere al securității (punctele ***92***-***96***).

Recomandarea 4

Să se asigure o evaluare solidă privind proprietatea și controlul entităților care primesc finanțare din partea UE în cadrul programului „Europa digitală”

Centrul european de competențe în materie de securitate cibernetică ar trebui:

(a) să obțină o asigurare rezonabilă că beneficiarii responsabili de acordarea de sprijin financiar către terți dispun de capacitatea administrativă și tehnică necesară pentru a efectua, pe baza metodologiei existente puse la dispoziția beneficiarilor care implementează acest tip de sprijin, evaluări adecvate privind proprietatea și controlul;

(b) să verifice, pe bază de eșantion, dacă doar entitățile eligibile au primit finanțare din partea UE.

Data-țintă pentru punerea în aplicare a recomandării: 2026 pentru litera (a) și 2027 pentru litera (b).

21 Beneficiarii care gestionează proiecte finanțate de UE trebuie să raporteze către ECCC cu privire la progresele și rezultatele lor, utilizând jaloane și livrabile. Acestea sunt esențiale pentru monitorizarea proiectelor și ar trebui definite în mod corespunzător. Curtea a constatat că aproape niciunul dintre proiectele din eșantionul său nu respecta instrucțiunile referitoare la modul de elaborare a jaloanelor și a livrabilelor și că multe dintre acestea nu erau utile pentru urmărirea progreselor (punctele ***97***-***99***).

22 S-a constatat că mulți dintre indicatorii de performanță utilizați de beneficiari nu sunt relevanți sau măsurabili și nu sunt însoțiți de valori-țintă sau de valori de referință. În plus, raportarea cu privire la acești indicatori nu era adecvată și, prin urmare, nu poate servi drept bază pentru evaluarea performanței proiectelor (punctele ***100***-***102***).

23 Pentru a monitoriza realizările programului „Europa digitală” în ansamblu, toate proiectele trebuie să raporteze cu privire la indicatori specifici ai programului, care sunt integrați în fișele anuale de performanță a programului întocmite de Comisie. ECCC este responsabil de colectarea și verificarea datelor furnizate în legătură cu acești indicatori. Curtea a identificat mai multe probleme legate de modul în care au fost colectate datele, precum și de calitatea generală a acestora. Nu s-au identificat dovezi care să ateste că ECCC a verificat exactitatea datelor raportate. Pe baza verificărilor pe care le-a realizat pe eșantionul său, Curtea consideră că datele raportate nu reflectă cu acuratețe rezultatele obținute (punctele ***103***-***106***).

Recomandarea 5

Să se consolideze cadrul de monitorizare a performanței aferent componentei de securitate cibernetică a programului „Europa digitală”

Pentru a permite o monitorizare adecvată a progreselor și a performanței, Centrul european de competențe în materie de securitate cibernetică ar trebui:

(a) să se asigure, înainte de semnarea unui grant, că toate proiectele au definit jaloane, livrabile și indicatori de performanță care respectă instrucțiunile furnizate în formularul de cerere;

(b) să conceapă și să pună în aplicare un sistem solid de colectare, trasabilitate, verificare și agregare a datelor pentru indicatorii de performanță ai componentei de securitate cibernetică a programului „Europa digitală”, urmărind să se asigure că indicatorii reflectă cu acuratețe rezultatele obținute.

Data-țintă pentru punerea în aplicare a recomandării: 2027.

02

Observațiile Curții, în detaliu

Rețelele și mecanismele de securitate cibernetică ale UE sprijină cooperarea și răspunsul, însă eficacitatea lor este redusă din cauza schimbului limitat de informații și a punerii în aplicare incomplete

Rețelele UE facilitează cooperarea între statele membre, dar schimbul limitat de informații le reduce valoarea adăugată

24 Cadrul actual al UE privind rețelele și mecanismele de facilitare a detectării incidentelor semnificative de securitate cibernetică, precum și a răspunsului la acestea a fost dezvoltat treptat. Primul pas în acest sens a fost Directiva privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune[3] (Directiva NIS), care a intrat în vigoare în august 2016. Peisajul actual de la nivelul UE este ilustrat în ***anexa II***.

[3] Directiva (UE) 2016/1148.

Rețelele UE facilitează cooperarea statelor membre la nivel tehnic și operațional

25 Directiva NIS a instituit rețeaua CSIRT, care reunește CERT-UE (Serviciul de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii) și echipele CSIRT desemnate de statele membre. Această rețea urmărește să consolideze încrederea între echipele CSIRT naționale și să promoveze o cooperare operațională rapidă și eficace între statele membre.

26 EU-CyCLONe a fost înființată în 2020 ca rețea informală de cooperare pentru autoritățile naționale responsabile cu gestionarea crizelor cibernetice. Ea servește drept punte între nivelul tehnic, la care funcționează rețeaua CSIRT, și nivelul politic al Consiliului Uniunii Europene, care acționează prin mecanismul său integrat pentru un răspuns politic la crize. Intrarea în vigoare a Directivei NIS 2 în 2023 a formalizat rolul EU-CyCLONe și i-a conferit un mandat clar.

27 Curtea a evaluat dacă rolurile și responsabilitățile acestor rețele de la nivelul UE sunt bine definite și dacă ele facilitează cooperarea între statele membre.

28 ENISA acționează în calitate de secretariat al rețelelor CSIRT și EU-CyCLONe și le oferă acestora resurse, expertiză, infrastructură și instrumentele informatice necesare pentru cooperare și pentru o comunicare securizată în scopul schimbului de informații. În sondajul său de la începutul anului 2025 privind satisfacția părților interesate[4], ENISA a primit punctaje bune pentru performanța sa în calitate de secretariat al acestor rețele. Acest feedback pozitiv a fost confirmat și în cursul vizitelor de audit ale Curții, unde autoritățile naționale din domeniul securității cibernetice și-au exprimat aprecierea față de agenție.

[4] Raportul anual de activitate consolidat pe 2024 al ENISA, p. 33 și 36.

29 În 2025, Consiliul a adoptat Planul de acțiune al UE pentru gestionarea crizelor cibernetice, care definește rolurile și responsabilitățile actorilor-cheie (inclusiv ale rețelelor CSIRT și EU-CyCLONe) și mecanismele mobilizate pe parcursul incidentelor de securitate cibernetică de mare amploare sau al crizelor cibernetice. Curtea a constatat că acest plan clarifică în mare măsură rolurile și responsabilitățile în ceea ce privește gestionarea crizelor cibernetice la nivelul UE și ține seama de schimbările survenite în peisaj de la primul plan de acțiune adoptat în 2017. Planul definește trei niveluri de cooperare: tehnică, operațională și politică. El detaliază noile rețele și structuri instituite începând din 2017 – cum ar fi EU-CyCLONe, echipele UE de răspuns rapid în caz de amenințări hibride și sistemul european de alertă în materie de securitate cibernetică – și abordează modul în care gestionarea crizelor cibernetice ar trebui integrată în cadrul mai larg al UE de răspuns la crize.

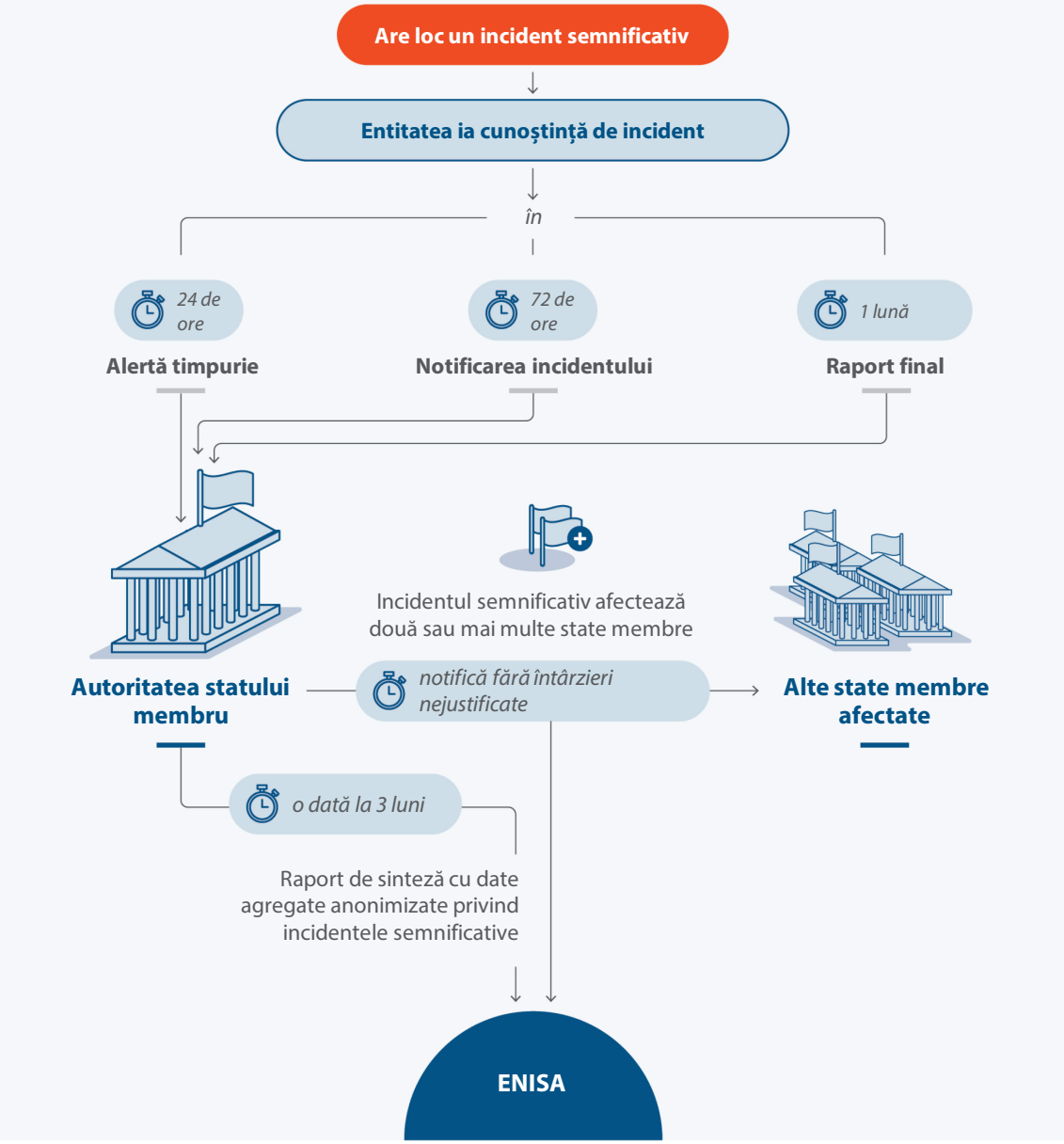
30 Cu toate acestea, în pofida instituirii oficiale a rețelei CSIRT în 2016 și a EU-CyCLONe în 2023, cele două rețele nu au stabilit încă în mod formal aranjamentele procedurale care să reglementeze cooperarea dintre ele. Ele nu au convenit nici asupra criteriilor pe baza cărora rețeaua CSIRT ar trebui să avertizeze EU-CyCLONe că un incident de securitate cibernetică observat constituie un incident de securitate cibernetică de mare amploare, potențial sau în desfășurare. Cele două rețele trebuie, de asemenea, să convină asupra unei taxonomii comune a nivelurilor de gravitate a incidentelor și a conceptelor-cheie – cum ar fi „amenințare”, „actor care generează amenințări”, „incident” sau „impact” –, necesară pentru a permite schimbul automatizat de informații. În prezent, criteriile în funcție de care un incident este considerat semnificativ sau de mare amploare lasă loc de interpretări. Autoritățile din domeniul securității cibernetice din toate cele trei state membre vizitate de Curte au menționat că nu există o taxonomie comună.

Schimbul limitat de informații și raportarea insuficientă reduc semnificativ valoarea adăugată a acestor rețele

31 Frontierele geografice nu împiedică apariția și răspândirea incidentelor și atacurilor cibernetice. Schimbul de informații între statele membre cu privire, de exemplu, la tacticile și tehnicile utilizate de actorii care generează amenințări, precum și la semnele digitale care indică faptul că o rețea sau un sistem informatic a fost compromis(ă) („indicatori de compromitere”) poate contribui în mod semnificativ la consolidarea securității cibernetice.

32 Curtea a constatat că schimbul de informații era limitat, ceea ce reduce considerabil valoarea adăugată a acestor rețele. Limitările observate se referă în principal la întârzieri în transpunerea Directivei NIS 2, la probleme legate de a stabili dacă un incident are sau nu un impact transfrontalier, la legislațiile în materie de securitate națională care îngrădesc schimbul de informații, precum și la o lipsă de încredere. Directiva NIS 2 introduce mai multe cerințe de raportare pentru entitățile care intră în sfera sa de aplicare și pentru autoritățile statelor membre, astfel cum se ilustrează în ***figura 2***.

Figura 2 | Calendarul de raportare a incidentelor în temeiul Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în UE (Directiva NIS 2)



Sursa: Curtea de Conturi Europeană, pe baza ENISA.

33 Statele membre au avut termen până în octombrie 2024 pentru a transpune Directiva NIS 2 în legislația națională, dar numai două dintre ele au respectat termenul. Întârzierile în transpunere au un impact semnificativ asupra schimbului de informații, deoarece, până la transpunere, entitățile care intră sub incidența Directivei NIS 2 nu au obligația legală de a raporta incidentele. Comisia a estimat[5] că sub incidența Directivei NIS intrau 15 500 de entități, în timp ce numărul celor care se încadrează în sfera de aplicare a Directivei NIS 2 se ridică la peste 110 000. De exemplu, administrația publică – sectorul cel mai vizat din UE, potrivit raportului privind situația amenințărilor publicat de ENISA în 2025 – nu avea obligația de a raporta incidentele în temeiul Directivei NIS.

34 Pentru că datele privind incidentele se transmit către ENISA o dată la trei luni (adică la mult timp după ce este posibil să fi avut loc un incident), valoarea adăugată a acestei raportări este limitată. Datele respective servesc în principal unor scopuri statistice și de raportare a tendințelor istorice, nu pentru a îmbunătăți detectarea și răspunsul. ENISA pune la dispoziția statelor membre un instrument online pentru prezentarea rapoartelor. Modelul de raportare conține un set minim de date care trebuie furnizate, cum ar fi tipul de incident și sectorul implicat. În plus, ENISA sugerează ca statele membre să furnizeze informații suplimentare pentru a permite o analiză mai aprofundată a datelor, de exemplu prin corelarea incidentelor cu vulnerabilități specifice. Nu toate statele membre aleg însă să furnizeze aceste informații, ceea ce reduce semnificativ calitatea și valoarea adăugată a datelor colectate.

35 În raportul său din 2024 privind situația securității cibernetice în UE, ENISA a afirmat că incidentele sunt probabil subraportate, deoarece numărul incidentelor declarate pare să fie scăzut. În perioada 2018-2021, statele membre au raportat în fiecare an agenției ENISA între 100 și 500 de incidente. Acest număr a crescut treptat, ajungând la 1 276 în 2024[6].

---

[5] Comisia Europeană, raportul din 2020 privind evaluarea impactului.

[6] Potrivit datelor din CIRAS pentru 2024.

36 În raportul său din 2025 privind situația amenințărilor, care acoperă perioada iunie 2024-iunie 2025, ENISA a identificat aproximativ 4 800 de incidente de securitate cibernetică[7] prin intermediul informațiilor din surse deschise, cum ar fi articolele de știri. Atunci când colectează datele, ENISA acoperă un spectru mai larg de incidente, deci nu toate aceste incidente ar fi fost raportabile în temeiul Directivei NIS 2. În schimb, multe incidente semnificative nu sunt raportate în informațiile din surse deschise. Dat fiind că datele raportate de statele membre sunt anonimizate, ENISA nu poate corela incidentele identificate de ea cu cele raportate de statele membre. Prin urmare, nu este posibil să se determine cu precizie amploarea subraportării, dar Curtea consideră că diferența dintre numărul de incidente raportate de statele membre și cel indicat în raportul privind situația amenințărilor arată că nu toate incidentele semnificative sunt raportate.

37 Un alt element care sugerează o subraportare a incidentelor este numărul de notificări transmise către alte state membre afectate și către ENISA cu privire la incidente transfrontaliere semnificative. Directiva NIS prevedea și ea o cerință similară, care a fost însă considerată ineficace, deoarece, în 2020, Comisia a concluzionat[8] că, în pofida obligației existente, rareori se trimiteau astfel de notificări. Ea a pus acest fapt pe seama lipsei unor aranjamente clare pentru schimbul de informații și a faptului că nu existau obiective comune care să stimuleze un astfel de schimb.

38 Obligația de a informa alte state membre este esențială pentru a preveni propagarea incidentelor. Nerespectarea sa afectează negativ securitatea cibernetică a UE. În 2025, nu s-au raportat decât 14 incidente transfrontaliere semnificative (de către șapte state membre). În 2024, s-au raportat două incidente cu un posibil impact transfrontalier, în 2023, niciunul, iar în 2022, trei. Rezultă de aici că doar foarte puține incidente transfrontaliere semnificative sunt raportate, numărul acestora nereflectând amploarea reală a unor astfel de atacuri. Pentru a oferi un termen de comparație, în raportul său din 2024 privind situația amenințărilor, ENISA a identificat 322 de incidente care au vizat în mod specific două sau mai multe state membre. Incidentul care a vizat *Collins Aerospace* (a se vedea ***caseta 1***) este un exemplu de situație în care statele membre nu au raportat un incident cu un impact transfrontalier semnificativ.

---

[7] Raportul ENISA din 2025 privind situația amenințărilor.

[8] Comisia Europeană, raportul din 2020 privind evaluarea impactului.

Caseta 1

Incident cibernetic ce a perturbat operațiunile aeroportuare

În septembrie 2025, *Collins Aerospace*, un important furnizor de tehnologie pentru industria aeronautică, a fost victima unui atac semnificativ de tip *ransomware* care a vizat software-ul său de prelucrare a datelor cu privire la pasageri. Din această cauză, principalele aeroporturi europene s-au văzut obligate să revină la operațiuni manuale, ceea ce a cauzat numeroase întârzieri și anulări ale zborurilor. Cele mai afectate au fost aeroportul Heathrow din Londra, aeroportul din Bruxelles, aeroportul Berlin Brandenburg și aeroportul din Dublin.

În conformitate cu Directiva NIS 2, un incident este considerat „semnificativ” dacă, printre altele, provoacă perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză. Or, niciun stat membru nu a tratat acest incident ca pe un incident transfrontalier semnificativ sau de mare amploare. Prin urmare, niciunul dintre statele membre afectate nu a notificat în mod oficial ENISA sau alte state membre cu privire la acest atac. Rețeaua CSIRT nu a informat EU-CyCLONe, care, deci, nu a sprijinit gestionarea coordonată a incidentului.

Sursa: analiza Curții de Conturi Europene, pe baza interviurilor cu ENISA.

39 Raportarea limitată a incidentelor transfrontaliere se explică și prin faptul că responsabilitatea de a stabili dacă un incident raportat are sau nu un impact transfrontalier și de a identifica celelalte state membre afectate revine autorității competente din statul membru în cauză. Este posibil ca, pe baza informațiilor de care dispune, entitatea raportoare sau autoritatea națională respectivă să nu fie conștientă de caracterul transfrontalier al anumitor atacuri. În prezent, nu există nicio platformă la nivelul UE care să colecteze în timp real raportări privind incidentele din partea tuturor statelor membre și care să poată corela informații privind sectoarele sau indicatorii de compromitere pentru a detecta incidentele transfrontaliere. Există astfel un risc important ca unele astfel de incidente să nu fie identificate și raportate ca atare.

40 Din 2016, niciun stat membru nu a considerat vreun incident cibernetic drept „incident de mare amploare”. În principiu, orice incident care afectează în mod semnificativ cel puțin două state membre se încadrează în această definiție. Cu toate acestea, nici măcar incidentele cibernetice care au cauzat pane la nivel mondial și daune semnificative, precum cele prezentate în ***figura 3***, nu au fost considerate incidente de mare amploare. Prin urmare, procedura de escaladare către EU-CyCLONe nu a fost niciodată pe deplin activată ca urmare a unui incident de securitate cibernetică de mare amploare.

Figura 3 | Exemple de incidente de securitate cibernetică majore

WannaCry

2017

Un atac de tip *ransomware*, la nivel mondial

A infectat peste 200 000 de calculatoare din mai mult de 150 de țări, paralizând operatori de infrastructură critică; atacatorii au criptat datele de pe sistemele afectate și au cerut o răscumpărare pentru decriptarea acestora.

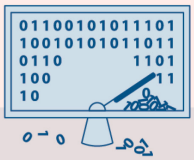


NotPetya

2017

Un program *malware* distructiv care se prezintă ca *ransomware*

A fost conceput pentru ștergerea permanentă a datelor; a vizat în principal Ucraina, dar s-a răspândit ulterior rapid în întreaga lume, paralizând corporații multinaționale și cauzând daune la nivel mondial.



Pană informatică legată de CrowdStrike

iulie 2024

O pană informatică masivă, la nivel mondial

A fost cauzată de o actualizare de software defectuoasă realizată de compania de securitate cibernetică CrowdStrike, care a afectat funcționarea a milioane de calculatoare.



Sursa: Curtea de Conturi Europeană, adaptare pe baza informațiilor publicate de Cloudflare, ENISA, Europol, Wired, IBM, CrowdStrike.

41 Pe lângă obligația de raportare impusă entităților și statelor membre, a fost creată rețeaua CSIRT, menită să faciliteze schimbul de informații. Încrederea între statele membre reprezintă fundamentul acestei rețele, în cadrul căreia informațiile sunt partajate pe bază voluntară. Valoarea adăugată a rețelei se reduce în mod semnificativ dacă statele membre nu sunt dispuse să facă în timp util schimb de informații cu caracter operațional.

42 Schimbul de informații la nivelul UE este restricționat de legislația în materie de securitate națională a fiecărui stat membru. În cazul în care consideră că informațiile legate de un atac cibernetic asupra unei entități critice sunt clasificate sau că raportarea cu privire la un anumit incident ar fi în detrimentul securității lor naționale, statele membre nu au obligația de a partaja respectivele informații. În cursul vizitelor Curții în statele membre, reprezentanți ai rețelelor CSIRT și EU-CyCLONe au afirmat că schimbul de date se poate realiza numai în limitele legislațiilor în materie de securitate națională. Nu s-a efectuat nicio analiză la nivelul UE a cadrelor juridice naționale ale statelor membre și a impactului acestora asupra schimbului de informații.

43 În 2016, rețeaua CSIRT cuprindea 28 de echipe CSIRT naționale, cu câte doi reprezentanți pentru fiecare stat membru. Lipsa schimbului de informații este o problemă persistentă, iar Comisia a recunoscut în evaluarea Directivei NIS că „statele membre nu fac în mod sistematic schimb de informații între ele”, ceea ce afectează în special eficacitatea măsurilor de securitate cibernetică și nivelul de conștientizare comună a situației în ansamblul UE. În temeiul Directivei NIS 2, multe state membre au desemnat, pe lângă echipa CSIRT națională, și echipe CSIRT specifice unui sector, rețeaua extinzându-se deci considerabil. La momentul auditului, ea cuprindea 42 de echipe CSIRT, cu peste 700 de participanți în total. O rețea atât de mare face și mai dificilă consolidarea încrederii, deoarece este greu să se mențină legături strânse între toți membrii.

44 Rețeaua CSIRT este conștientă de problema schimbului de informații și are în vedere diverse acțiuni menite să consolideze încrederea într-o rețea în continuă creștere. Crearea unor clustere mai mici de state membre, organizate în centre transfrontaliere, astfel cum se detaliază la punctele ***62-74***, reprezintă o soluție alternativă la o rețea la nivelul UE, care poate contribui la abordarea acestei provocări.

Serviciile contractate de Centrul de analiză și de cunoaștere a situației în materie cibernetică se suprapun parțial peste capacități existente, iar funcționarea viitoare a centrului nu este clar definită

45 În temeiul Directivei NIS 2, în cazurile în care un incident de securitate cibernetică de mare amploare potențial sau în curs are sau este probabil să aibă un impact semnificativ, Comisia devine membru al EU-CyCLONe[9]. Acest nou rol și evoluția peisajului amenințărilor au determinat Comisia să instituie un grup operativ de coordonare cibernetică în cadrul DG CONNECT în 2022. Grupul include un Centru de analiză și de cunoaștere a situației în materie cibernetică (denumit în continuare „centrul pentru cunoașterea situației cibernetice”), menit să ajute Comisia să își consolideze capacitatea de înțelegere a situației amenințărilor la adresa securității cibernetice, în vederea sprijinirii responsabilităților sale instituționale în materie de gestionare a crizelor. Centrul ar trebui, de asemenea, să ajute DG CONNECT să ofere consiliere la nivel politic.

46 Pentru activitatea acestui centru, Comisia se bazează în mare măsură pe prestatori externi de servicii contractați în decembrie 2022 în schimbul a aproape 18 milioane de euro pentru o perioadă de patru ani. Curtea a evaluat arhitectura centrului, realizările obținute și planurile Comisiei pentru funcționarea viitoare a acestuia.

[9] Articolul 16 alineatul (2) din Directiva NIS 2.

47 Ca parte a serviciilor pe care le asigură, contractanții au creat un tablou de bord bazat pe fluxuri comerciale de informații privind amenințările cibernetice pentru a prezenta și a face schimb de informații în materie. De asemenea, ei elaborează diverse rapoarte cu date operative privind amenințările cibernetice, inclusiv rapoarte zilnice și săptămânale, precum și rapoarte tematice referitoare la anumite țări sau sectoare economice. Sediul fizic al centrului pentru cunoașterea situației cibernetice constă într-o sală dotată cu stații de lucru conectate de la distanță la tabloul de bord găzduit de contractanți și se află într-una dintre clădirile Comisiei. La momentul auditului, centrul era format dintr-un număr redus de membri ai personalului Comisiei, sprijiniți de numeroși analiști proveniți de la contractanți, precum și de experți din cadrul ENISA.

48 Curtea a constatat că activitatea desfășurată pentru acest centru de prestatorii externi de servicii se suprapune, parțial, cu cea desfășurată de ENISA. ENISA dispune de capacități permanente de conștientizare a situației și de monitorizare a amenințărilor. Ea publică periodic rapoarte privind amenințările cibernetice, inclusiv rapoarte-fulger legate de incidente specifice, precum și rapoarte săptămânale care oferă o imagine de ansamblu a amenințărilor. Rapoartele se bazează pe informații din surse deschise și sunt similare cu cele elaborate de contractanți. În plus, ENISA elaborează sau contribuie la informări la nivel înalt pentru factorii de decizie în perioade de criză, informări care sunt și ele comparabile cu cele emise de centrul pentru cunoașterea situației cibernetice.

49 Un alt aspect, datele utilizate de centru pentru a elabora aceste rapoarte se bazează pe fluxuri comerciale de informații privind amenințările cibernetice și sunt similare cu datele utilizate de alte servicii ale Comisiei, cum ar fi Direcția Generală pentru Servicii Digitale și CERT-UE. Curtea consideră că, în stabilirea arhitecturii acestui centru, nu s-a valorificat suficient potențialul de raționalizare, prin utilizarea informațiilor deja disponibile la nivelul Comisiei și al ENISA.

50 Contractul expiră în decembrie 2026. După această dată, contractanții nu vor mai furniza servicii centrului. Este vorba, printre altele, despre servicii precum punerea la dispoziție a datelor din tabloul de bord, elaborarea de rapoarte privind amenințările și asigurarea majorității capacităților centrului. Tabloul de bord va fi predat Comisiei, dar își va pierde valoarea adăugată dacă nu va fi actualizat în permanență cu informații privind amenințările cibernetice.

51 La momentul auditului, Comisia nu elaborase planuri referitoare la continuarea sprijinului din partea prestatorilor externi de servicii pentru funcționarea centrului după expirarea contractului. Curtea consideră că lipsa unui astfel de plan cuprinzător și detaliat reprezintă un risc la adresa funcționării centrului după 2026.

Rezerva UE pentru securitate cibernetică facilitează mobilizarea rapidă a serviciilor de răspuns la incidente

52 În 2022, imediat după ce a început agresiunea militară a Rusiei împotriva Ucrainei, Comisia, recunoscând că atacurile cibernetice de mare amploare au devenit mai răspândite, a acordat ENISA o finanțare excepțională de 15 milioane de euro pentru a implementa în regim pilot Acțiunea de sprijin în materie de securitate cibernetică, lansată ulterior în 2023. Tot în 2023, Comisia a furnizat fonduri suplimentare (aproximativ 20 de milioane de euro) pentru a prelungi programul până la sfârșitul anului 2026.

53 Comisia a propus, de asemenea, Regulamentul privind solidaritatea cibernetică – adoptat în decembrie 2024 –, pentru a se pregăti să răspundă în cazul unor eventuale incidente de securitate cibernetică de mare amploare. Regulamentul instituie o rezervă a UE pentru securitate cibernetică, ce constă în servicii de răspuns la incidente, furnizate de prestatori de încredere. Dotată cu un buget de 36 de milioane de euro pentru perioada 2025-2027, rezerva a devenit treptat operațională în 2025.

54 Curtea a evaluat modul în care a fost organizată Acțiunea de sprijin în materie de securitate cibernetică, program care stă la baza rezervei UE pentru securitate cibernetică. S-a verificat, de asemenea, dacă învățămintele desprinse începând din 2022 au fost utilizate pentru conceperea rezervei.

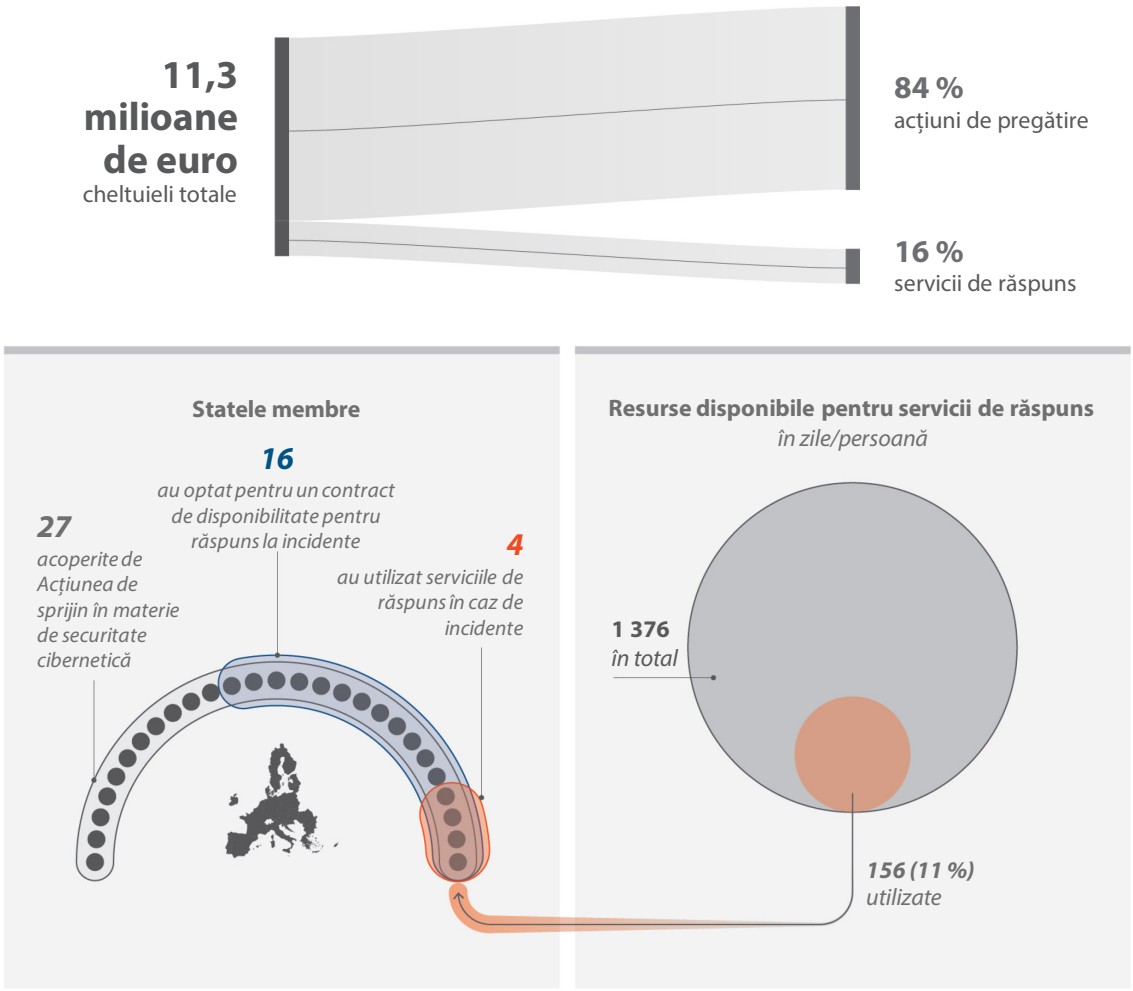
55 ENISA a conceput Acțiunea de sprijin în materie de securitate cibernetică drept mecanism de furnizare de servicii în sprijinul acțiunilor statelor membre de pregătire și de răspuns în caz de incidente de securitate cibernetică de mare amploare sau de crize cibernetice. Toate serviciile sunt contractate în prealabil de ENISA, ceea ce înseamnă că prestatorii pot răspunde imediat eventualelor solicitări din partea statelor membre. Acest lucru este posibil și datorită structurii de organizare a ENISA, care asigură un sistem de permanență, cu un responsabil disponibil în orice moment pentru a trata cererile statelor membre.

56 ENISA a ales să aloce bugetul disponibil în mod egal între statele membre. În practică, agenția a lansat o procedură de licitație deschisă împărțită în 27 de loturi, câte unul pentru fiecare stat membru, pentru a selecta până la trei furnizori de securitate privați care să asigure servicii până la sfârșitul anului 2026. În plus, ENISA a selectat, în cadrul unui lot paneuropean, furnizori care să asigure servicii pentru țările terțe eligibile, precum și pentru instituțiile, organele și agențiile UE sau care să sprijine răspunsul la incidente transfrontaliere.

57 Această abordare a permis ENISA să țină seama de cerințele naționale specifice, inclusiv legate de limbă, de autorizațiile de securitate națională sau de prezența operațională deja existentă în statele membre. Pe de altă parte, întrucât furnizorii nu au fost selectați pentru a opera la nivelul întregii UE, această abordare prezintă dezavantajul major că, în cazul în care un anumit stat membru nu recurge la serviciile contractate în prealabil, bugetul angajat pentru aceste servicii pentru respectivul stat nu poate fi redirecționat pentru a sprijini un alt stat membru.

58 În ceea ce privește Acțiunea de sprijin în materie de securitate cibernetică, statele membre pot alege între servicii de pregătire sau servicii de răspuns ori o combinație între cele două. În principal, statele membre au ales să utilizeze fondurile disponibile pentru a-și îmbunătăți gradul de pregătire (84 % din cheltuieli în 2023). Cele care au optat pentru un contract de disponibilitate pentru răspuns la incidente (adică un acord predefinit cu un furnizor, care asigură faptul că, la cerere, statul membru poate beneficia de serviciile acestuia pentru a oferi un răspuns rapid la incidente de securitate cibernetică) nu au utilizat acest mecanism decât în mod limitat, astfel cum se arată în ***figura 4***. În cele trei state membre vizitate, autoritățile și-au exprimat aprecierea față de modul în care ENISA gestionează Acțiunea de sprijin în materie de securitate cibernetică.

Figura 4 | Acțiunea de sprijin în materie de securitate cibernetică a ENISA, până în 2023



Sursa: Curtea de Conturi Europeană, pe baza datelor de la ENISA.

59 Pentru perioada 2024-2026, doar nouă state membre au solicitat un contract de disponibilitate pentru răspuns la incidente. Interviurile desfășurate de Curte cu ENISA și cu autorități din trei state membre au confirmat o preferință clară pentru activitățile de pregătire.

60 Rezerva UE pentru securitate cibernetică urmărește în primul rând să sprijine răspunsul la incidente majore de securitate cibernetică și redresarea în urma acestora, însă serviciile precontractate din această rezervă care nu sunt utilizate pentru răspunsul la incidente pot fi convertite în servicii de pregătire. Această abordare flexibilă poate preveni situațiile în care servicii preplătite să nu fie utilizate.

61 Curtea consideră că modelul ales pentru rezerva UE pentru securitate cibernetică se bazează pe învățămintele desprinse din Acțiunea de sprijin în materie de securitate cibernetică. Datele privind utilizarea acestei acțiuni indică însă riscul ca rezerva să fie utilizată în principal pentru pregătire, și nu pentru răspuns, contrar scopului prevăzut în Regulamentul privind solidaritatea cibernetică.

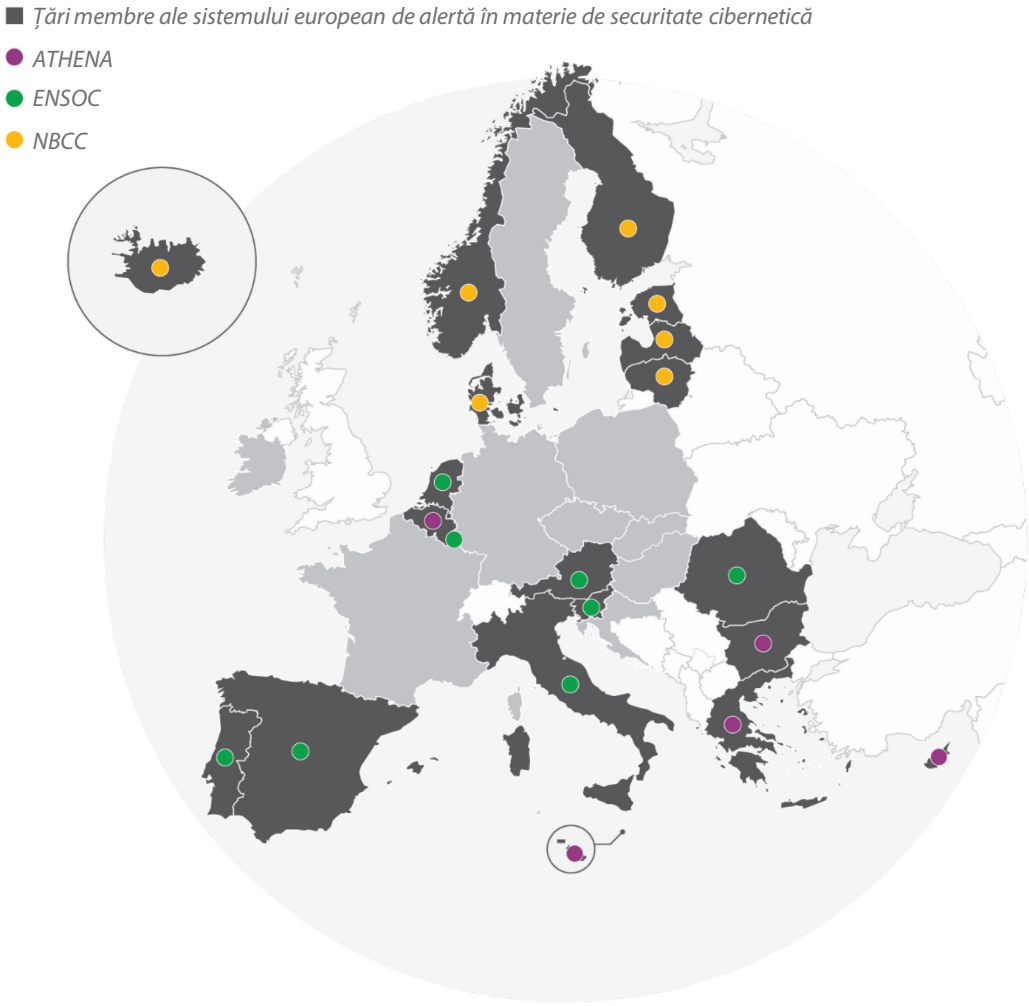
Sistemul european de alertă în materie de securitate cibernetică urmărește să consolideze capacitățile de detectare a amenințărilor, dar nu este operațional

62 Unul dintre obiectivele-cheie ale sistemului european de alertă în materie de securitate cibernetică este de a încuraja schimbul de informații pertinente, pentru a îmbunătăți detectarea și analiza amenințărilor cibernetice și răspunsul la acestea. Participarea la sistemul de alertă este voluntară, dar statele membre care aleg să se alăture unui centru cibernetic transfrontalier trebuie să se angajeze să facă schimb de informații relevante cu ceilalți membri. Lucrând împreună în clustere într-un mediu sigur și de încredere, ele ar putea evita unele dintre problemele legate de schimbul de informații identificate la punctele ***31***-***44***.

63 La momentul auditului, 13 state membre optaseră să facă parte din sistemul european de alertă în materie de securitate cibernetică, instituind două centre transfrontaliere: ATHENA și ENSOC. În 2026 s-au alocat fonduri pentru înființarea unui al treilea centru cibernetic transfrontalier, NBCC. Numărul total de membri ai rețelei ajunge astfel la 20 de țări (18 state membre plus Islanda și Norvegia[10]), astfel cum se arată în ***figura 5***.

[10] Țări terțe asociate în conformitate cu articolul 10 alineatul (1) litera (a) din Regulamentul (UE) 2021/694.

Figura 5 | Țările care fac parte din sistemul european de alertă în materie de securitate cibernetică



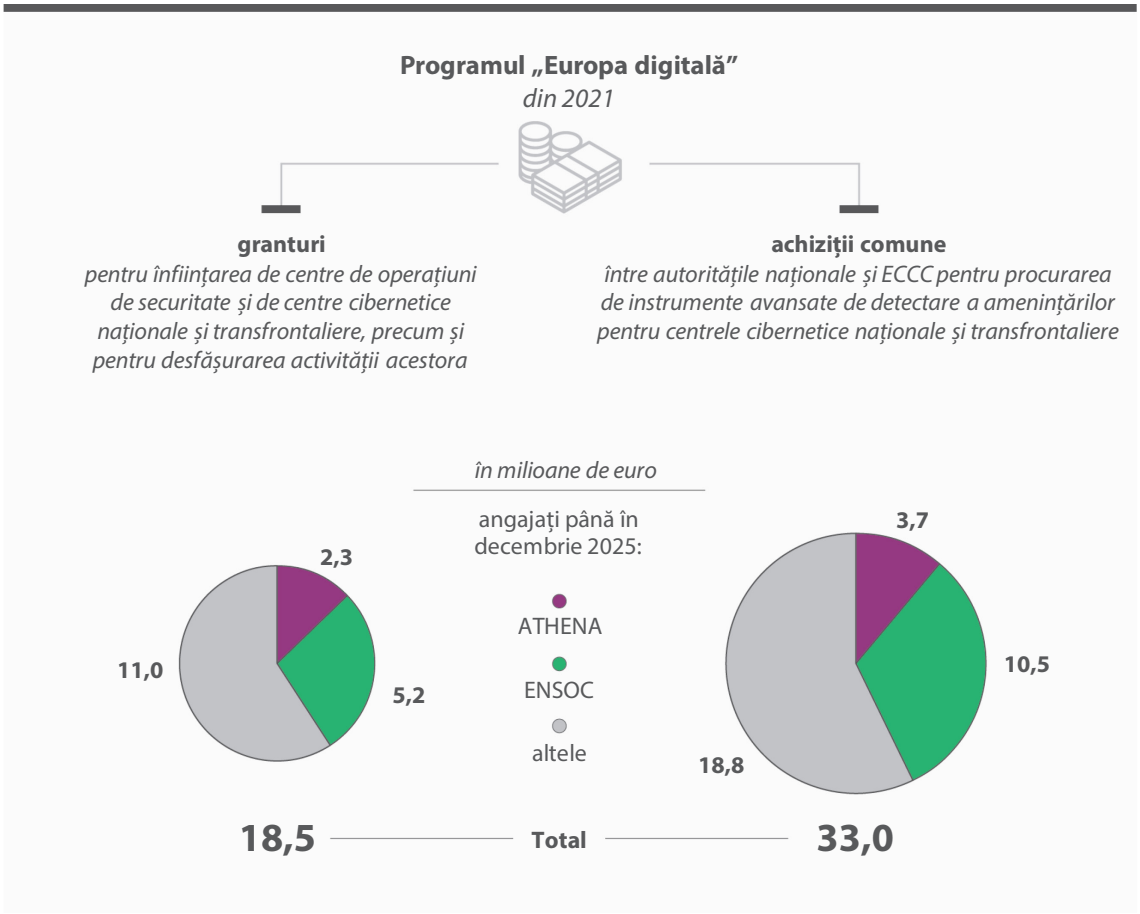
Sursa: Curtea de Conturi Europeană.

64 Curtea a evaluat modul în care au fost înființate primele două centre cibernetice transfrontaliere, precum și progresele acestora în direcția îndeplinirii obiectivelor sistemului european de alertă în materie de securitate cibernetică. S-a examinat, de asemenea, cum se încadrează centrele cibernetice transfrontaliere în peisajul mai larg al securității cibernetice și cum interacționează ele cu rețelele și structurile existente.

Până în prezent, nu s-au obținut rezultate concrete, din cauza întârzierilor semnificative în achizițiile publice

65 Din 2021, sunt disponibile, prin programul „Europa digitală”, fonduri pentru sprijinirea înființării de centre cibernetice naționale și transfrontaliere. Această finanțare este acordată printr-o procedură complexă, cu două fluxuri paralele: granturi tradiționale menite să sprijine înființarea și funcționarea centrelor, precum și achiziții comune pentru instrumente avansate de detectare a amenințărilor, astfel cum se arată în ***figura 6***. În urma unei cereri de propuneri lansate în noiembrie 2022, ATHENA și ENSOC și-au început activitatea în ianuarie 2024.

Figura 6 | Finanțarea acordată pentru centre cibernetice prin programul „Europa digitală”



Sursa: Curtea de Conturi Europeană, pe baza datelor ECCC.

66 Procedurile de achiziții restrânse[11], desfășurate în două etape, au fost organizate de membrii ATHENA și ai ENSOC, împreună cu DG CONNECT (prima etapă) și cu centrul ECCC nou înființat (a doua etapă). Abordarea în două etape vizează să limiteze circulația informațiilor sensibile, prin furnizarea specificațiilor tehnice detaliate numai candidaților selectați în prima etapă.

67 Prima etapă a fost lansată în mai 2024 pentru ENSOC și în iulie 2024 pentru ATHENA. Societățile interesate au avut la dispoziție o lună pentru a-și depune candidatura. Candidații aleși nu au fost însă informați cu privire la faptul că au fost selectați decât în aprilie 2025, la aproape un an de la lansarea procedurii.

68 În plus, nici procedura de achiziții aferentă ENSOC, nici cea pentru ATHENA nu au putut trece la a doua etapă la momentul respectiv, din cauză că membrii centrelor și ECCC nu au fost în măsură să furnizeze întreprinderilor preselectate specificațiile tehnice necesare pentru ca acestea să depună o ofertă, deoarece încă lucrau la finalizarea lor.

69 A doua etapă a procedurilor de achiziții publice a început abia în august 2025 pentru unele loturi ENSOC și a fost planificată pentru începutul anului 2026 în cazul ATHENA. La momentul auditului, la 18 luni de la lansarea procedurilor de achiziții, nu se semnase încă niciun contract pentru niciunul dintre loturi. Curtea consideră că procedurile de achiziții nu au putut fi finalizate la timp din cauza complexității lor, dar și pentru că nu a existat o pregătire corespunzătoare.

70 Acestea fiind spuse, Curtea a constatat că centrele transfrontaliere nu sunt pe cale să își atingă obiectivele. În lipsa instrumentelor necesare pentru detectarea amenințărilor și pentru partajarea informațiilor, ele nu sunt utilizabile în practică, iar sistemul european de alertă în materie de securitate cibernetică nu poate funcționa deocamdată, ceea ce întârzie dezvoltarea eficace a unor capacități avansate de detectare și prevenire a amenințărilor și a incidentelor cibernetice. S-au semnat acte adiționale la acordurile de grant pentru prelungirea duratei acestora, astfel încât să se reflecte întârzierile înregistrate până în prezent în procedurile de achiziții (15 luni pentru ATHENA și 18 luni pentru ENSOC).

[11] Procedura de ofertare ENSOC și procedura de ofertare ATHENA.

Centrele cibernetice transfrontaliere creează canale de comunicare suplimentare care cresc și mai mult complexitatea

71 Una dintre sarcinile esențiale ale centrelor cibernetice transfrontaliere este de a face schimb de informații relevante pentru a îmbunătăți detectarea amenințărilor și răspunsul la acestea. Este vorba, printre altele, despre informații privind amenințările cibernetice, vulnerabilitățile, indicatorii de compromitere și actorii care generează amenințări. Sarcinile centrelor cibernetice transfrontaliere se suprapun parțial cu cele ale echipelor CSIRT naționale și ale rețelei CSIRT, în special în ceea ce privește schimbul de informații privind amenințările cibernetice și vulnerabilitățile în materie. Nu există o limită clară între rolul centrelor cibernetice transfrontaliere și cel al echipelor CSIRT. Potrivit Planului de acțiune din 2025 al UE pentru gestionarea crizelor cibernetice (punctul ***29***), centrele cibernetice transfrontaliere sunt menite să funcționeze atât la nivel tehnic (cum ar fi echipele CSIRT naționale și rețeaua CSIRT), cât și la nivel operațional (cum ar fi EU-CyCLONe).

72 Regulamentul privind solidaritatea cibernetică impune centrelor cibernetice transfrontaliere să semneze acorduri de cooperare între ele pentru a facilita schimbul de informații. Tot în temeiul regulamentului, ENISA ar fi trebuit ca, până în februarie 2026, să emită orientări privind interoperabilitatea dintre centrele cibernetice transfrontaliere. Între timp, în decembrie 2025, ECCC a acordat un grant unui consorțiu (care includea și anumiți membri ai ENSOC și ai ATHENA) pentru a defini un cadru tehnic de interoperabilitate între centrele cibernetice transfrontaliere. Orientările și cadrul nu vor fi însă finalizate decât după ce centrele cibernetice transfrontaliere vor deveni operaționale. După cum a subliniat Curtea în avizul său din 2023 referitor la propunerea de regulament privind solidaritatea cibernetică[12], există riscul ca, fără un acord rapid, să se dezvolte sisteme incompatibile între ele, ceea ce ar duce la creșterea costurilor.

[12] Avizul nr. 02/2023 referitor la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor, punctul 26.

73 Centrele cibernetice transfrontaliere au, de asemenea, obligația de a face schimb de informații relevante privind incidentele de securitate cibernetică de mare amploare cu EU-CyCLONe și cu rețeaua CSIRT, fără întârzieri nejustificate. La nivelul statelor membre, înființarea de centre cibernetice naționale și participarea la centre cibernetice transfrontaliere creează niveluri suplimentare de comunicare. Coordonarea cu țări participante din afara UE[13], care nu sunt membre ale rețelei CSIRT sau ale EU-CyCLONe, crește, de asemenea, complexitatea.

74 Sunt necesare acorduri de cooperare clare pentru a conveni asupra unei taxonomii comune și asupra modalităților de schimb de informații, precum și pentru a asigura interoperabilitatea. Lecțiile desprinse din funcționarea rețelei CSIRT arată că este vorba despre o provocare majoră. Curtea a constatat că, la momentul auditului, nu se conveniseră aranjamente procedurale privind cooperarea și schimbul de informații. În opinia sa, înființarea de centre cibernetice naționale și transfrontaliere ar putea promova un schimb de informații mai eficace. Integrarea centrelor transfrontaliere în peisajul deja complex al securității cibernetice va fi însă dificilă și necesită canale de comunicare și mecanisme de cooperare suplimentare.

[13] Islanda și Norvegia.

Proiectele finanțate de UE prin programul „Europa digitală” vizează consolidarea securității cibernetice, dar întâmpină provocări legate de punerea în aplicare și de raportare

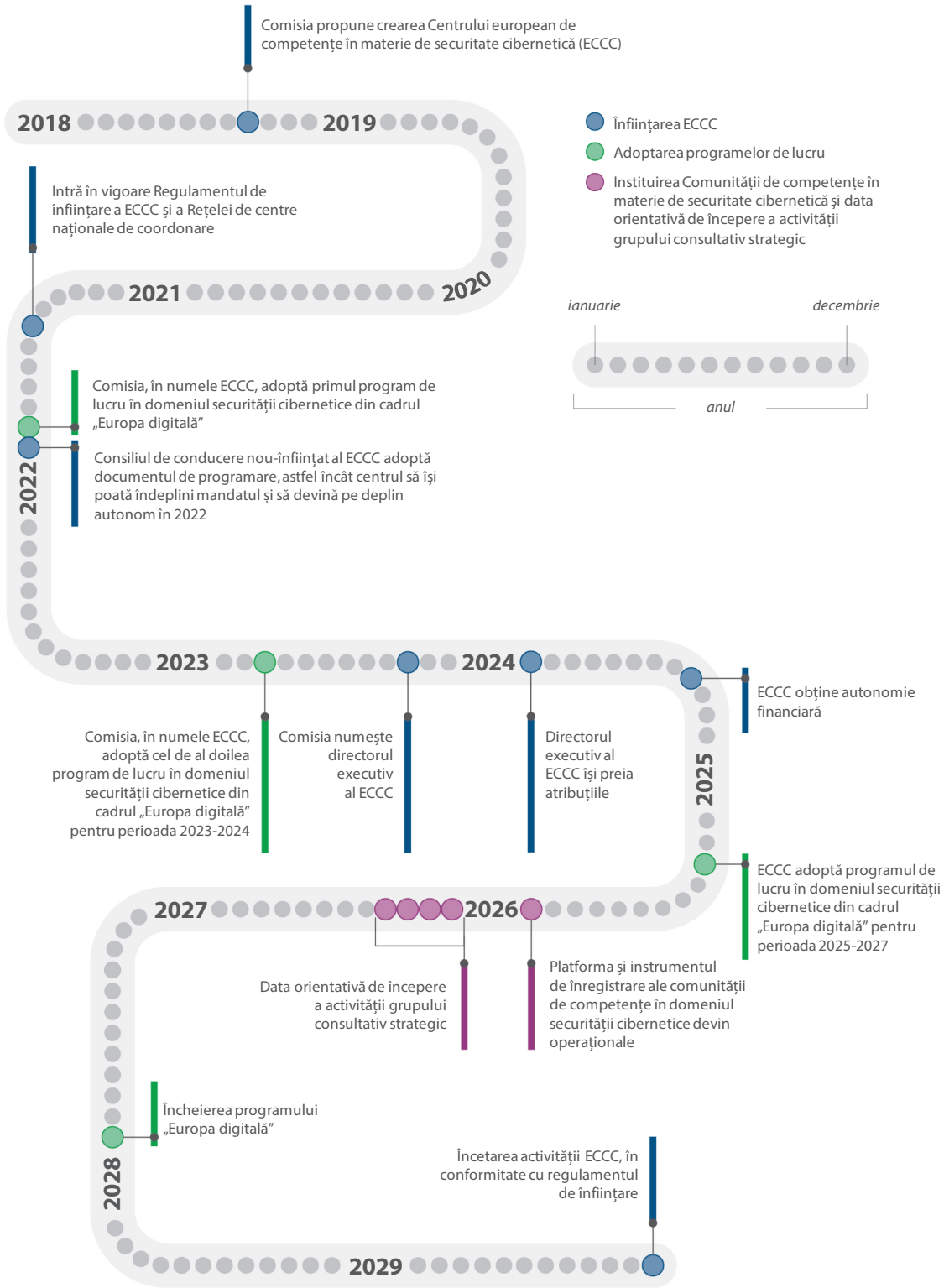
Din cauza întârzierilor la înființare, Comunitatea de competențe în materie de securitate cibernetică nu a reușit să modeleze programele de lucru ale „Europa digitală” în funcție de propriile nevoi

75 Pentru gestionarea componentei de securitate cibernetică a programului „Europa digitală”, Comisia a propus în 2018 crearea Centrului european de competențe în materie de securitate cibernetică (ECCC). Regulamentul privind ECCC prevedea ca acest centru să fie sprijinit de o rețea de 29 de centre naționale de coordonare (CNC) – câte unul pentru fiecare stat membru, pentru Islanda și pentru Norvegia. Regulamentul solicita, de asemenea, crearea Comunității de competențe în materie de securitate cibernetică (denumită în continuare „comunitatea”), formată din reprezentanți ai industriei, ai organizațiilor universitare și de cercetare, precum și ai altor asociații relevante ale societății civile.

76 Cel mult 20 de membri ai comunității urmau să fie numiți în grupul consultativ strategic, care este una dintre cele trei componente din structura ECCC. Una dintre sarcinile principale ale acestui grup este de a organiza consultări publice care să contribuie la agenda ECCC și la programele de lucru ale „Europa digitală”.

77 Curtea a evaluat dacă „Europa digitală” și programele de lucru aferente au fost adoptate pe baza unei analize solide a nevoilor, precum și cum au contribuit ECCC, Rețeaua de centre naționale de coordonare, comunitatea și grupul consultativ strategic la programele de lucru. În practică, ECCC, rețeaua de centre naționale de coordonare, comunitatea și grupul consultativ strategic au fost înființate treptat de-a lungul mai multor ani (a se vedea ***figura 7***).

Figura 7 | Calendarul înființării Centrului european de competențe în materie de securitate cibernetică, a Rețelei de centre naționale de coordonare, a comunității și a grupului consultativ strategic



Sursa: Curtea de Conturi Europeană.

78 Dat fiind că ECCC a devenit pe deplin operațional abia în septembrie 2024, Comisia a adoptat, în numele acestuia, programele de lucru pentru perioadele 2021-2022 și 2023-2024. Aceste două programe nu au putut beneficia de contribuții din partea comunității.

79 Între timp, statele membre au început să își înființeze propriile centre naționale de coordonare, care acționează ca puncte de contact la nivel național pentru comunitate. Înființarea și funcționarea acestora sunt cofinanțate prin programul „Europa digitală”. Până la momentul auditului, UE acordase peste 90 de milioane de euro, inclusiv aproximativ 44 de milioane care vor fi distribuite mai departe sub formă de sprijin financiar către terți. O sumă suplimentară de 38 de milioane de euro a fost înscrisă în buget până în 2027 pentru a sprijini centrele naționale de coordonare.

80 Curtea a constatat că, în decembrie 2025, la patru ani de la înființarea ECCC și a Rețelei de centre naționale de coordonare, comunitatea nu fusese încă înființată, iar grupul consultativ strategic nu fusese încă numit. La 14 martie 2025, ECCC a adoptat cel mai recent program de lucru în domeniul securității cibernetice din cadrul „Europa digitală” pentru perioada 2025-2027. ECCC și-a pregătit și adoptat programul de lucru în urma unor consultări ample cu statele membre și cu Rețeaua de centre naționale de coordonare, însă nu a putut beneficia de contribuții și de consiliere din partea comunității sau a grupului consultativ strategic, ceea ce contravine dispozițiilor prevăzute de regulamentul său de instituire. Curtea consideră că aceasta este o oportunitate ratată.

81 Programul „Europa digitală” este prevăzut să se încheie în 2027, iar ECCC, în lipsa unei prelungiri a mandatului, ar urma să își înceteze activitatea în 2029. Prin urmare, este posibil ca sprijinul Rețelei de centre naționale de coordonare, al comunității și al grupului consultativ strategic, odată instituite, să nu fie relevant decât pentru o perioadă scurtă de timp.

Proiectele finanțate de UE urmăresc obiective relevante, dar multe dintre ele se confruntă cu probleme operaționale

82 Curtea a selectat un eșantion de 11 proiecte relevante pentru detectarea incidentelor de securitate cibernetică și pentru răspunsul la acestea. Este vorba de proiecte finanțate în cadrul programului „Europa digitală” în perioada 2022-2025 (a se vedea ***figura 5*** din ***anexa I*** și ***anexa III***). Curtea a evaluat dacă:

- obiectivele proiectelor erau în concordanță cu rezultatele preconizate exprimate în cererile de propuneri și cu obiectivele programului „Europa digitală” în ansamblu;
- până în prezent, proiectele și-au atins realizările și rezultatele planificate;
- realizările proiectelor au fost livrate la timp.

Curtea prezintă rezultatele acestei evaluări în ***anexa IV***.

Unele proiecte au dat rapid rezultate, dar multe dintre ele se confruntă cu provocări operaționale și cu întârzieri

83 Curtea a constatat că toate proiectele urmăresc obiective care contribuie la atingerea obiectivelor în materie de securitate cibernetică ale programului „Europa digitală”[14] și că ele abordează majoritatea obiectivelor prevăzute în cererile de propuneri[15].

84 Dintre cele 11 proiecte incluse în eșantionul Curții, 2 se aflau într-un stadiu incipient de punere în aplicare și, prin urmare, Curtea nu a putut formula o concluzie cu privire la performanța lor. 4 au fost evaluate ca fiind satisfăcătoare în ceea ce privește obținerea realizărilor și a rezultatelor planificate. 2 proiecte prezentau unele deficiențe, iar 3 au fost evaluate drept nesatisfăcătoare (a se vedea ***anexa IV***).

85 Programul „Europa digitală” are drept obiectiv explicit să crească nivelul de securitate cibernetică al întreprinderilor mici și mijlocii (IMM-uri). În acest sens, mai multe proiecte oferă soluții concrete pentru IMM-uri (a se vedea ***caseta 2***).

---

[14] Articolul 6 din Regulamentul (UE) 2021/694 de instituire a programului „Europa digitală”.

[15] Cererile de propuneri: Consolidarea capacităților centrelor de operațiuni de securitate; Implementarea Rețelei de centre naționale de coordonare împreună cu statele membre; Sprijin pentru pregătire și asistență reciprocă; și Noi aplicații ale IA și alte tehnologii generice pentru centrele de operațiuni de securitate.

Caseta 2

Exemple de proiecte care aduc rezultate tangibile pentru IMM-uri

Proiectul GR-SME-SOC (proiectul 6 din ***anexa III***) urmărește să furnizeze instrumente și servicii de securitate cibernetică IMM-urilor din Grecia prin înființarea unui centru de operațiuni de securitate (SOC) adaptat nevoilor acestora. El a început în ianuarie 2024 și este pus în aplicare de un consorțiu format din cinci organizații elene. Obiectivul este de a oferi servicii de securitate cibernetică, gratuit, unui număr de 120 de IMM-uri timp de un an, după care serviciile vor deveni disponibile pe piață. Proiectul oferă IMM-urilor servicii avansate, cum ar fi monitorizarea în timp real, detectarea amenințărilor pe baza IA și răspunsul flexibil și rapid la incidente.

Prin proiectul NCC-IE (proiectul 3 din ***anexa III***), coordonatorul a acordat granturi în valoare de aproximativ 1,8 milioane de euro unui număr de peste 50 de IMM-uri irlandeze în scopul îmbunătățirii securității cibernetice. De schema de granturi au beneficiat întreprinderi cu între 2 și circa 200 de angajați, inclusiv întreprinderi familiale, întreprinderi nou-înființate și exportatori mondiali din diferite sectoare. Granturile s-au acordat exclusiv pentru întreprinderi care au fost supuse anterior unei analize de securitate cibernetică gestionate de agenția guvernamentală Enterprise Ireland. Grantul a acoperit 80 % din costurile (până la 60 000 de euro) necesare pentru punerea în aplicare a recomandărilor formulate în urma analizei.

Sursa: Curtea de Conturi Europeană.

86 Multe proiecte din eșantionul Curții întâmpină dificultăți în a respecta termenele sau se confruntă cu provocări operaționale (a se vedea ***anexa IV***). Curtea a constatat că patru proiecte înregistrează întârzieri considerabile. Printre acestea se numără ENSOC și ATHENA, astfel cum se detaliază la punctele ***65***-***70***. În ***caseta 3*** sunt prezentate alte exemple.

Caseta 3

Exemple de proiecte care se confruntă cu provocări operaționale și cu întârzieri

În Irlanda, Autoritatea de gestionare a administrației publice locale (LGMA) este singurul beneficiar al grantului acordat pentru proiectul ILG-SOC (proiectul 8 din ***anexa III***). Obiectivul proiectului este de a înființa un centru principal de operațiuni de securitate pentru 31 de autorități locale, care să utilizeze instrumente avansate de detectare a amenințărilor și de răspuns la acestea. Proiectul, planificat să se desfășoare pe parcursul a trei ani, a început în octombrie 2023. În urma evaluării la jumătatea perioadei, toate livrabilele au fost respinse. Proiectul include mai multe proceduri de achiziții publice care au eșuat sau care au suferit întârzieri. Durata proiectului va fi prelungită (fără nicio finanțare suplimentară), ceea ce ar putea oferi suficient timp pentru ca acesta să se încheie cu succes.

În Grecia, proiectul EL-SOC (proiectul 5 din ***anexa III***) urmărește să instituie un SOC consolidat, la nivel național, care să reunească informații de la SOC sectoriale. S-ar putea obține astfel o imagine de ansamblu cuprinzătoare și în timp real asupra situației în materie de securitate cibernetică. Proiectul se desfășoară în perioada ianuarie 2024-decembrie 2026. Achiziția planificată de hardware și de servicii a fost întârziată din cauza unor probleme legate de finalizarea și publicarea specificațiilor tehnice pentru procedura de ofertare. Drept motive pentru întârziere, coordonatorul de proiect a menționat, de asemenea, probleme legate de asigurarea cofinanțării naționale și de disponibilitatea limitată a personalului din domeniul achizițiilor publice.

Sursa: Curtea de Conturi Europeană.

87 Alte două proiecte din eșantionul Curții se confruntă cu întârzieri moderate. Trei proiecte au furnizat realizările la timp. Două proiecte se află într-un stadiu incipient de punere în aplicare și Curtea nu poate, deci, să tragă o concluzie.

Restricțiile de securitate generează provocări operaționale și există riscuri semnificative atunci când controalele sunt efectuate de beneficiari

88 Regulamentul „Europa digitală” prevede că, din motive de securitate, finanțarea pentru securitatea cibernetică poate fi limitată la entități stabilite în UE și controlate de statele membre sau de cetățeni ai statelor membre. Această restricție urmărește să atenueze riscul de intruziune sau influență din partea țărilor terțe și să împiedice schimbul de informații sensibile în materie de securitate cu autorități din afara UE.

89 Obligația ca entitățile să fie stabilite în UE și controlate din UE se aplică nu numai beneficiarilor de granturi, ci și subcontractanților acestora și oricăror beneficiari de sprijin financiar pentru terți. Cu excepția acestei din urmă categorii (a se vedea punctele ***92***-***96***), evaluarea este efectuată de Serviciul central de validare al Agenției Executive Europene pentru Cercetare. Decizia finală privind eligibilitatea pentru participarea la cereri de propuneri restrânse rămâne însă la latitudinea autorității care acordă grantul, și anume DG CONNECT sau ECCC.

90 În cursul activității de audit a Curții, beneficiarii au menționat în mod repetat provocările practice generate de evaluările privind proprietatea și controlul UE. O astfel de evaluare poate fi un proces complex și îndelungat: trebuie să se analizeze structura completă de proprietate și întregul lanț de control al fiecărei organizații, inclusiv toate nivelurile de proprietate până la proprietarii finali. Serviciul central de validare impune ca fiecare entitate să furnizeze probe documentare detaliate privind structura sa de proprietate și drepturile specifice aferente, guvernanța corporativă, precum și orice legături comerciale, financiare sau de altă natură care conferă control.

91 În cazul a trei proiecte finanțate de UE incluse în eșantionul Curții, cel puțin un beneficiar din cadrul unui consorțiu a fost ulterior exclus deoarece s-a considerat că era deținut sau controlat din afara UE. Excluderea unor membri din consorțiu arată că noțiunea de proprietate și control din UE nu este pe deplin înțeleasă de toți participanții la programul „Europa digitală”. În ansamblu, pe baza datelor furnizate de Serviciul central de validare, 7 % dintre solicitanții de granturi în domeniul securității cibernetice din cadrul programului „Europa digitală” sau subcontractanții acestora nu au trecut evaluarea în perioada 2022-2025. Faptul că participanți neeligibili depun candidaturi în cadrul cererilor de propuneri cauzează întârzieri, după cum se arată în ***caseta 4***.

Caseta 4

Exemplu de caz în care unii beneficiari au fost excluși din cauză că nu au trecut controalele de securitate

Doi dintre membrii consorțiului din cadrul proiectului NG-SOC (proiectul 7 din ***anexa III***) au fost respinși în urma evaluărilor privind proprietatea și controlul. Rezultatul a fost anunțat cu aproximativ o lună înainte de termenul-limită pentru semnarea acordului de grant. Coordonatorul de proiect a fost nevoit să accepte să preia activitatea care fusese atribuită celor doi membri excluși, deoarece nu era suficient timp pentru a găsi un nou partener. Unul dintre membrii excluși activa într-o industrie specifică, în care urma să se testeze soluția dezvoltată. Prin urmare, o parte semnificativă a proiectului, care viza testarea soluțiilor în practică, nu a putut continua așa cum fusese prevăzut. Această situație a fost remediată ulterior prin modificarea acordului de grant pentru a include noi membri.

Sursa: Curtea de Conturi Europeană.

92 Două dintre proiectele examinate de Curte (NCC-IE și CYberSynchrony) oferă așa-numitul „sprijin financiar pentru terți”. Acest mecanism de finanțare permite beneficiarilor de granturi să utilizeze o parte din fondurile obținute pe această cale pentru a finanța alte entități prin cereri deschise de propuneri. Sprijinul financiar pentru terți poate facilita accesul la finanțare din partea UE. În acest caz, beneficiarii sunt singurii responsabili pentru efectuarea evaluărilor privind proprietatea și controlul, iar Serviciul central de validare nu este implicat.

93 În 2021, Comisia a publicat orientări generale pentru solicitanții cererilor restrânse de propuneri, orientări actualizate ulterior în 2026. Mecanismul de sprijin financiar pentru terți este în vigoare din 2021 pentru cererile de propuneri din cadrul programului „Europa digitală”, însă nici Comisia, nici ECCC nu au pus la dispoziția beneficiarilor o metodologie detaliată cu privire la modul de efectuare a verificărilor privind proprietatea și controlul atunci când evaluează părțile terțe cărora le acordă sprijin financiar. În iulie 2025, ECCC a furnizat orientări fără caracter obligatoriu, oferind Rețelei de centre naționale de coordonare o abordare structurată cu privire la realizarea acestui tip de verificări. Documentul de orientare conține principii generale și măsuri care ar putea fi luate. El nu specifică însă modul în care ar trebui efectuate verificările, lăsând beneficiarilor responsabilitatea de a-și dezvolta propria abordare.

94 Curtea a constatat că ECCC nici nu validează metodologia adoptată de beneficiari, nici nu efectuează controale bazate pe eșantioane pentru a se asigura că metodologia este suficient de solidă și că destinatarii selectați ai sprijinului financiar sunt într-adevăr deținuți și controlați din UE.

95 În raportul său anual pe 2024, Curtea a constatat că beneficiarii însărcinați de Comisie să gestioneze sprijinul financiar acordat unor părți terțe (în domeniul cercetării) nu erau obligați să demonstreze că controalele realizate de ei permit garantarea cu eficacitate a regularității cheltuielilor UE. Nici ECCC nu evaluează dacă beneficiarii dispun de capacitatea administrativă și tehnică necesară pentru a gestiona în mod corespunzător evaluările privind proprietatea și controlul. Astfel cum se detaliază la punctul ***90***, o astfel de evaluare poate fi complexă și se realizează la nivelul UE de către un serviciu specific cu expertiză în domeniu.

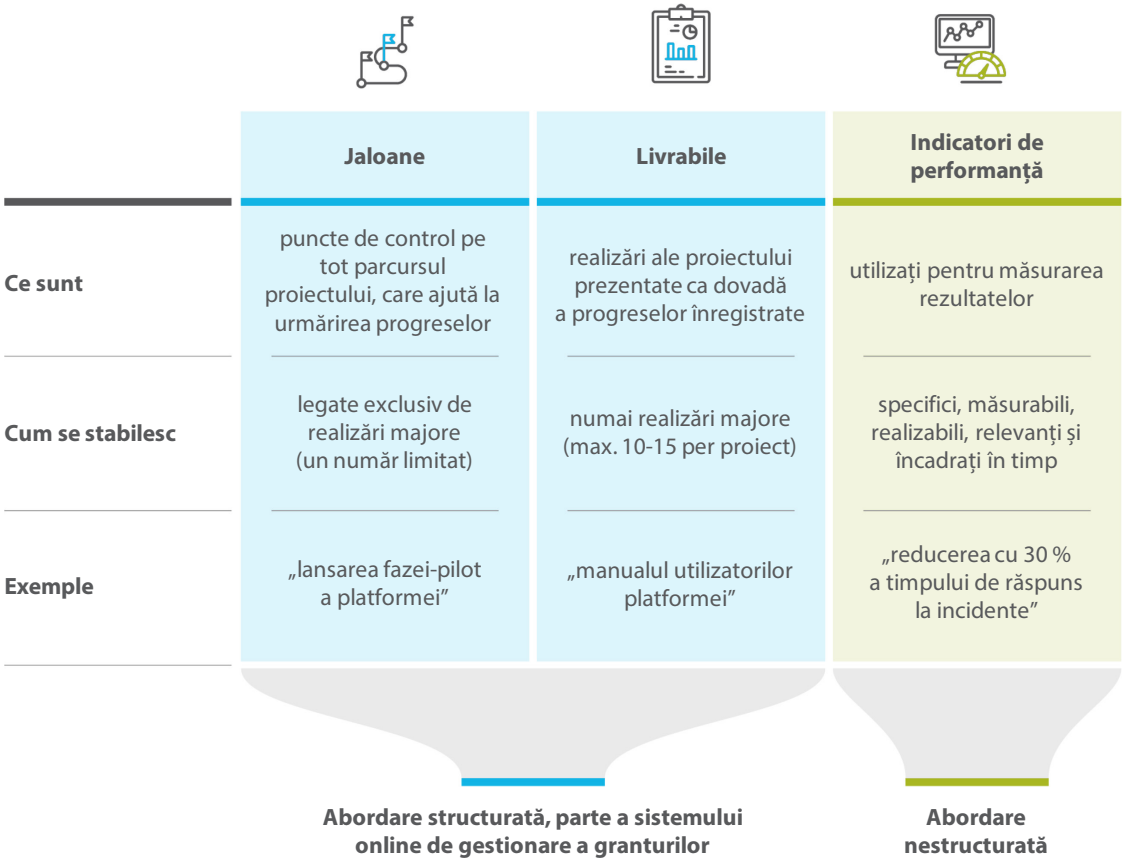
96 În acest context, Curtea consideră că există un risc semnificativ ca beneficiarii, care sunt responsabili de efectuarea verificărilor privind proprietatea și controlul, să nu dispună de capacitatea necesară pentru a se achita în mod corespunzător de această sarcină. Având în vedere natura activităților finanțate, această deficiență ar putea duce la expunerea unor infrastructuri sensibile, a unor date operaționale și a unor tehnologii critice din punctul de vedere al securității.

Majoritatea proiectelor finanțate de UE au cadre de performanță inadecvate, iar datele privind performanța componentei de securitate cibernetică a programului „Europa digitală” nu sunt exacte

Majoritatea proiectelor finanțate de UE au cadre de performanță inadecvate

97 Beneficiarii care gestionează proiecte finanțate de UE trebuie să raporteze către ECCC cu privire la progresele și rezultatele lor, utilizând jaloane, livrabile și indicatori, astfel cum se ilustrează în ***figura 8***. Curtea a evaluat dacă jaloanele și livrabilele stabilite pentru fiecare proiect permit o monitorizare adecvată. S-a evaluat, de asemenea, dacă indicatorii de performanță ai acestora sunt relevanți și măsurabili și dacă sunt însoțiți de o valoare de referință și de o valoare-țintă.

Figura 8 | Jaloane, livrabile și indicatori de performanță pentru proiectele din cadrul programului „Europa digitală”



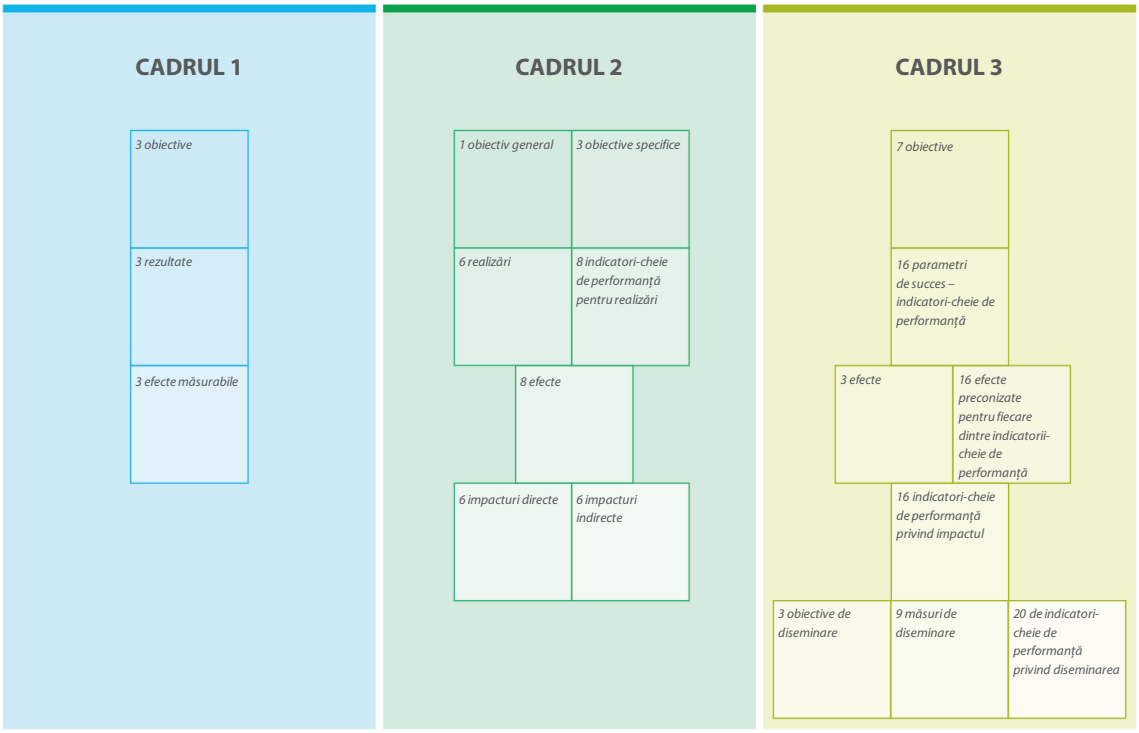
Sursa: Curtea de Conturi Europeană, pe baza formularului de cerere de grant.

98 În propunerea de proiect, beneficiarii trebuie să stabilească o serie de jaloane și de livrabile, urmând o abordare structurată specificată în instrucțiunile pentru solicitanți. Toate jaloanele și livrabilele sunt introduse în sistemul online de gestionare a granturilor, pentru a facilita monitorizarea lor. De obicei, ECCC examinează fiecare proiect de două ori: o dată la jumătatea perioadei de desfășurare a proiectului și o dată după finalizarea acestuia. În cursul examinărilor, experți externi verifică îndeplinirea jaloanelor și a livrabilelor, iar ECCC le validează. Jaloanele și livrabilele sunt deci esențiale pentru monitorizarea proiectelor și ar trebui stabilite în mod corespunzător.

99 Curtea a constatat că aproape niciunul dintre proiectele din eșantionul său nu a respectat instrucțiunile privind numărul de jaloane și de livrabile: numărul de jaloane per proiect variază între 8 și 39, iar numărul de livrabile între 8 și 45. Multe dintre jaloane și livrabile nu respectă instrucțiunile privind modul în care ar trebui definite și, prin urmare, nu sunt utile pentru urmărirea progreselor (de exemplu, „reuniune pentru începerea elaborării cererii de propuneri în domeniul cercetării” sau „proces-verbal oficial al reuniunii privind proiectul”). În cazul a trei proiecte, comitetul de evaluare identificase aceste probleme înainte de semnarea acordului de grant. În două cazuri, beneficiarii au propus doar modificări minore (de exemplu, cu privire la termenele-limită), fără a aborda problemele esențiale, iar în cel de-al treilea caz nu s-a efectuat nicio modificare. Pentru alte șase proiecte din eșantion, analiza Curții arată că jaloanele sau livrabilele nu sunt conforme cu instrucțiunile și nu sunt întotdeauna adecvate. În opinia Curții, dacă jaloanele și livrabilele nu sunt definite corespunzător sau dacă există prea multe jaloane și livrabile, este dificil să se urmărească progresele.

100 Spre deosebire de jaloane și de livrabile, indicatorii de performanță nu urmează o abordare structurată și nu sunt consolidați într-un tabel din sistemul de gestionare a granturilor, ci pot fi găsiți în diferite secțiuni ale propunerii. Această abordare a dus la o mare diversitate de cadre de performanță propuse de beneficiari. Unii au definit doar obiective ale proiectului corelate cu indicatori de performanță, în timp ce alții au stabilit cadre de performanță mult mai complexe. În ***figura 9*** de mai jos sunt prezentate câteva exemple.

Figura 9 | Exemplu care ilustrează varietatea de cadre de performanță definite pentru proiecte



Sursa: Curtea de Conturi Europeană.

101 Analiza Curții arată că mulți dintre indicatorii de performanță utilizați pentru proiecte nu sunt relevanți sau măsurabili și nu sunt însoțiți de valori-țintă sau de valori de referință (a se vedea ***caseta 5***). În plus, șapte proiecte au definit câte cel puțin 20 de indicatori, unul chiar 52. Curtea prezintă rezultatele acestei evaluări în ***anexa IV***.

Caseta 5

Exemple de indicatori de performanță necorespunzători

Nu pot fi măsurați:

- „Indicatorii de compromitere și alte servicii furnizate consolidează capacitățile IMM-urilor în materie de securitate cibernetică”
- „Furnizarea de instrumente și metode de răspuns la incidente care permit integrarea cu canalele de comunicare EU-CyCLONe”

Nu sunt însoțiți de o valoare de referință sau de o valoare-țintă:

- „O îmbunătățire de cel puțin 20 % a nivelului de pregătire a personalului”
- „O reducere de cel puțin 20 % a efortului necesar pentru alinierea la inițiativele relevante ale UE în materie de securitate cibernetică și pentru asigurarea conformității cu acestea”

Nu sunt legați de performanță:

- „Raport final privind proiectul la sfârșitul fazei de finanțare”
- „Numărul de stagiari care vor participa la toate sesiunile de formare”

Sursa: Curtea de Conturi Europeană, pe baza documentației proiectului.

102 În ansamblu, Curtea consideră că marea varietate de cadre de performanță, definirea deficitară a indicatorilor și numărul excesiv al acestora complică în mod substanțial monitorizarea performanței. Prin urmare, nu este posibil să se evalueze în mod corespunzător performanța proiectelor. Situația este complicată și mai mult de faptul că modelul de raportare nu conține o secțiune specifică privind indicatorii de performanță ai proiectelor și, prin urmare, majoritatea proiectelor din eșantionul Curții nu au raportat cu privire la aceștia.

Datele privind performanța componentei de securitate cibernetică a programului „Europa digitală” nu sunt exacte

103 Pentru a monitoriza realizările programului „Europa digitală”, regulamentul de instituire a acestuia prevede indicatori la nivel de program cu privire la care toate proiectele trebuie să raporteze, astfel cum se detaliază în ***caseta 6***.

Caseta 6

Indicatorii programului „Europa digitală” pentru componenta referitoare la securitatea cibernetică

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

1.b. Numărul de infrastructuri de securitate cibernetică sau de instrumente achiziționate în comun

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

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

Sursa: anexa II la Regulamentul (UE) 2021/694 de instituire a programului „Europa digitală”; cadrul de monitorizare și de evaluare pentru programul „Europa digitală” [SWD(2024) 37].

104 Curtea a evaluat dacă proiectele din eșantionul său raportaseră cu privire la acești indicatori și a examinat modul în care ECCC colectează și verifică datele respective.

105 Înainte de evaluarea lor intermediară și de cea finală, toate proiectele trebuie să raporteze, în sistemul de gestionare a granturilor, cu privire la indicatorii programului „Europa digitală”. Curtea a constatat că, din șapte proiecte care, la momentul auditului, se aflau la jumătatea calendarului lor și care ar fi trebuit deci să raporteze cu privire la acești indicatori, doar trei s-au achitat de această obligație. Dintre acestea, două nu raportaseră informații exacte: unul raportase cu privire la un indicator greșit, iar celălalt a indicat valori-țintă, nu rezultatele obținute.

106 În fiecare an, Comisia raportează cu privire la acești indicatori în fișele sale de performanță a programelor. Acest lucru le permite părților interesate să evalueze dacă programul își îndeplinește obiectivele. Potrivit fișei de performanță a programului pentru 2024, indicatorii programului „Europa digitală” pentru componenta referitoare la securitatea cibernetică sunt pe drumul cel bun. ECCC a explicat Curții că, pentru a compila acești indicatori, a utilizat o serie de sondaje trimise beneficiarilor proiectelor și nu s-a bazat pe sistemul de gestionare a granturilor. Curtea a examinat datele dezagregate furnizate de ECCC și a identificat numeroase probleme în ceea ce privește atât modul în care au fost colectate datele, cât și calitatea generală a acestora. S-a constatat că datele colectate nu corespund valorilor prezentate în fișa de performanță a programului, nefiind deci clar modul în care au fost calculate valorile raportate. Nu s-au identificat dovezi care să ateste că ECCC a verificat exactitatea datelor raportate. Pe baza verificărilor pe care le-a efectuat cu privire la proiectele din eșantionul său, întrucât majoritatea valorilor lipsesc sau sunt inexacte, Curtea consideră că datele raportate nu reflectă în mod corespunzător rezultatele obținute.

Prezentul raport a fost adoptat de Camera III, condusă de domnul George-Marius Hyzler, membru al Curții de Conturi, la Luxemburg, în ședința sa din 16 iunie 2026.

Pentru Curtea de Conturi

Tony Murphy
Președinte

Anexe

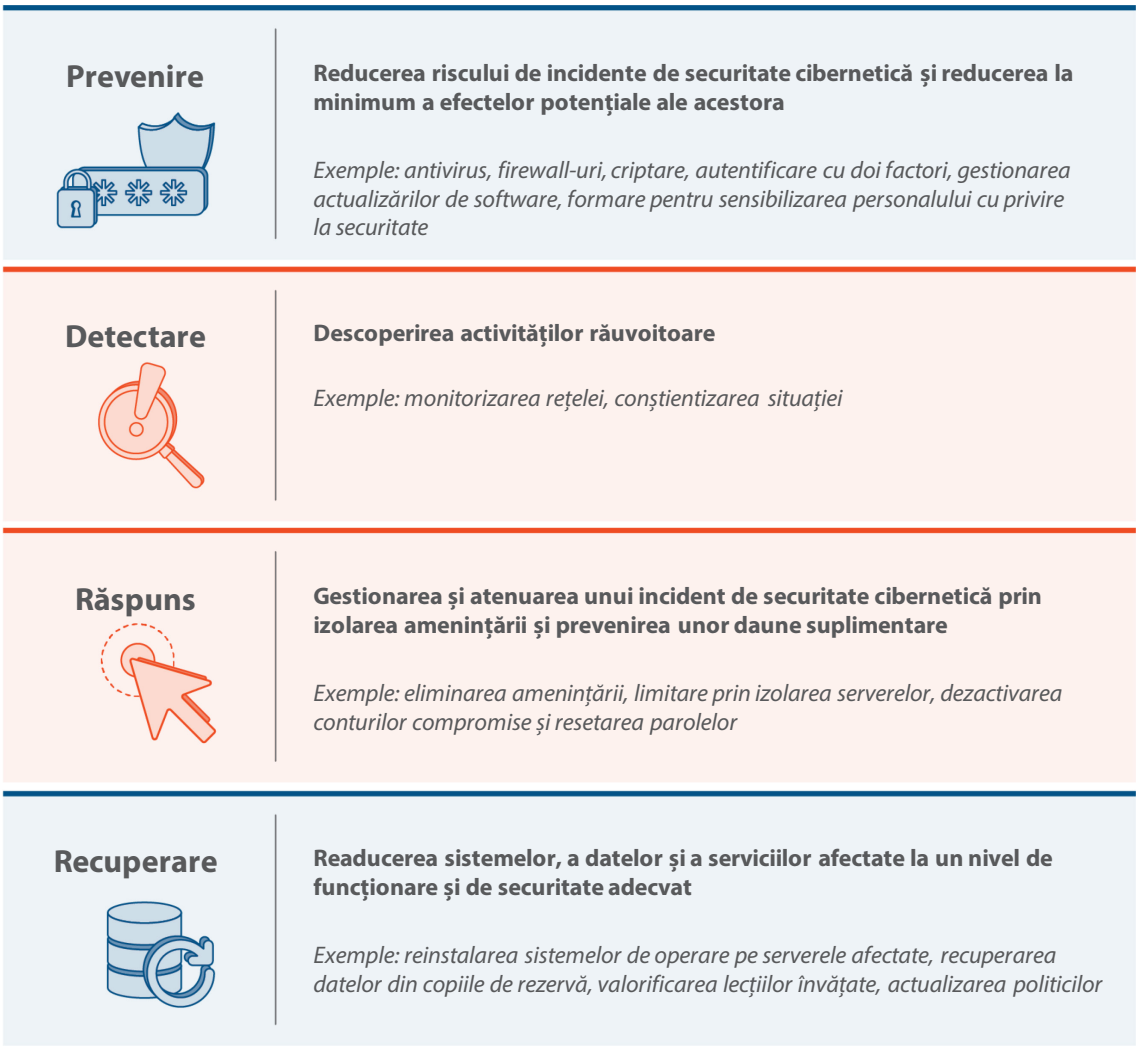
Anexa I – Informații despre audit

01 Securitatea cibernetică desemnează „activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice”[1]. O amenințare cibernetică este „orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora”[2]. Securitatea cibernetică necesită o abordare holistică, bazată pe o serie de activități interconectate de prevenire și detectare a amenințărilor cibernetice, de răspuns la acestea și de redresare în urma lor, astfel cum se arată în ***figura 1*** de mai jos.

[1] Regulamentul (UE) 2019/881 (Regulamentul privind securitatea cibernetică).

[2] Articolul 2 din Regulamentul privind securitatea cibernetică.

Figura 1 | Exemple de activități de securitate cibernetică

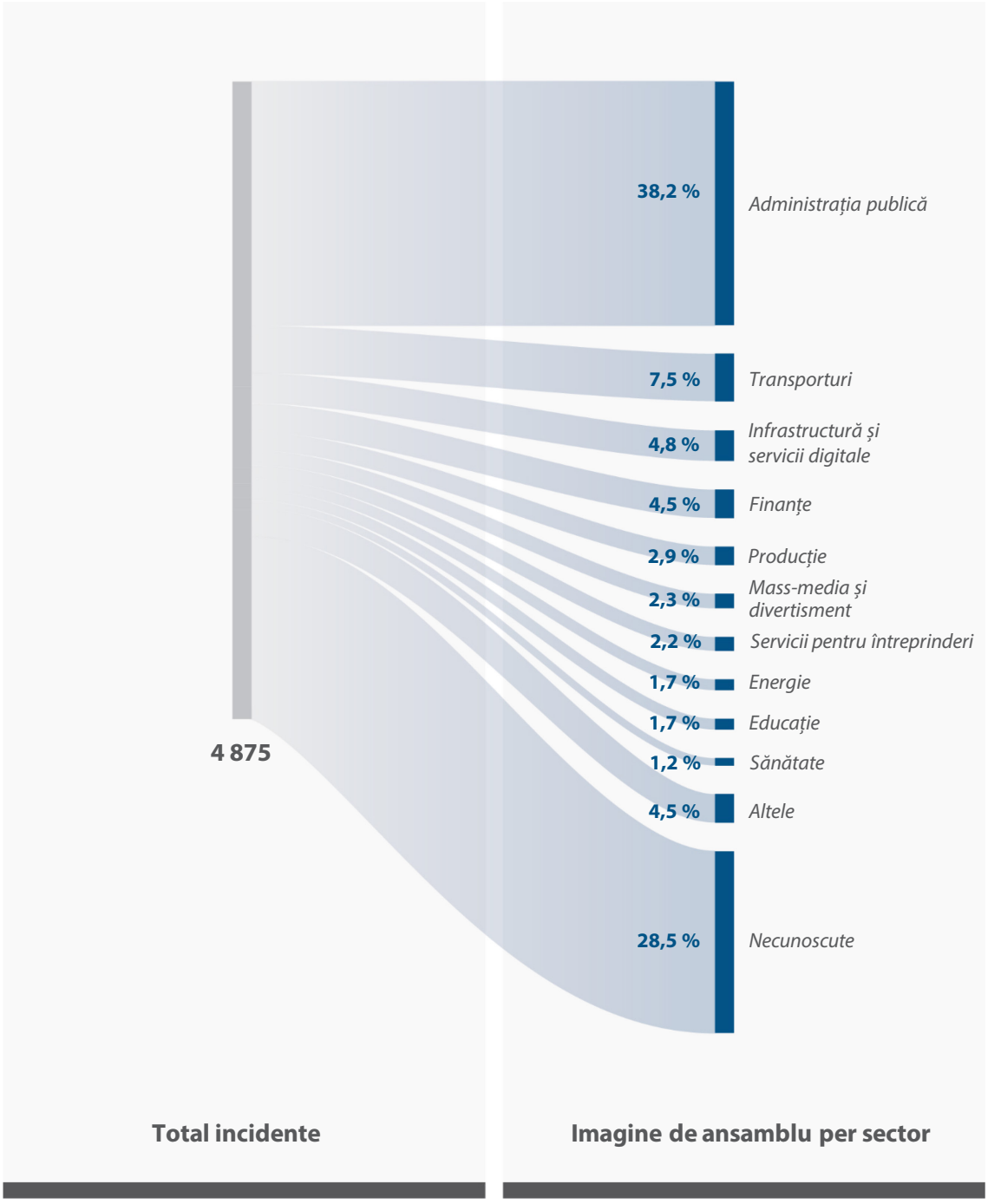


Sursa: Curtea de Conturi Europeană, pe baza considerentului 78 al Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică (Directiva NIS 2).

02 Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) consideră că nivelul amenințărilor la adresa securității cibernetice este substanțial, remarcând, în același timp, că peisajul amenințărilor cibernetice a devenit și este în continuare mult mai complex[3]. Aceste amenințări subliniază importanța vitală a securității cibernetice în economiile și societățile din ce în ce mai digitalizate. În raportul său din 2025 privind situația amenințărilor, ENISA a identificat *ransomware*-ul ca fiind cea mai critică amenințare din UE. ***Figura 2*** prezintă sectoarele vizate.

[3] *2024 report on the state of cybersecurity in the Union*, ENISA.

Figura 2 | Sectoare vizate de atacuri cibernetice



Sursa: Curtea de Conturi Europeană, pe baza ENISA.

Incidente de securitate cibernetică semnificative și de mare amploare

03 Incidentele de securitate cibernetică, ce includ atât amenințări cibernetice, cât și evenimente neintenționate (cum ar fi cele menționate în ***figura 3*** și la punctul ***40***), „pot [să împiedice] furnizarea serviciilor publice [și] desfășurarea activităților economice, […] să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei și sistemelor democratice ale Uniunii și ar putea avea chiar consecințe asupra sănătății sau asupra vieții”[4]. Un incident de securitate cibernetică este considerat[5]:

- **semnificativ**, dacă a provocat sau poate provoca perturbări operaționale grave ale serviciilor sau pierderi financiare pentru entitatea în cauză sau dacă a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile;

- **de mare amploare**, dacă a provocat un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre.

04 Un incident de securitate cibernetică de mare amploare poate escalada într-o **criză cibernetică** de sine stătătoare **la nivelul UE** dacă împiedică buna funcționare a pieței interne sau dacă prezintă riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni, în mai multe state membre sau în UE în ansamblul său[6].

---

[4] Considerentul 2 al Regulamentului (UE) 2025/38 (Regulamentul privind solidaritatea cibernetică).

[5] Articolele 6 și 23 din Directiva NIS 2; detaliate în Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei pentru o serie de furnizori din sectorul infrastructurii digitale.

[6] Considerentul 69 al Directivei NIS 2.

Cadrul politic al UE

05 Ecosistemul cibernetic al UE este complex și compus din mai multe niveluri, intersectându-se cu o serie de domenii de politică internă, cum ar fi justiția și afacerile interne, piața unică digitală și politicile de cercetare[7]. În cadrul politicii externe, securitatea cibernetică este prezentă în diplomație și devine o parte din ce în ce mai importantă a politicii emergente de apărare a UE[8].

06 În ultimii ani, UE și-a consolidat cadrul de reglementare în materie de securitate cibernetică. ***Figura 3*** de mai jos prezintă cele mai relevante acte legislative și instrumente de politică de la nivelul UE. În conformitate cu sfera auditului său (a se vedea punctele ***13***-***14***), Curtea s-a axat pe instrumentele care vizează detectarea incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsul la acestea.

[7] Documentul de informare al Curții de Conturi Europene intitulat „Provocări pentru o politică eficace a UE în domeniul securității cibernetice”, p. 12.

[8] De exemplu, poziția cibernetică a Uniunii Europene (2022), cadrul pentru un răspuns coordonat al UE la campaniile hibride (2022), politica UE în domeniul apărării cibernetice (2023) și setul de instrumente pentru diplomația cibernetică revizuit (2023).

Figura 3 | Legislația și instrumentele de politică relevante ale UE



Sursa: Curtea de Conturi Europeană.

Roluri și responsabilități

07 Peisajul securității cibernetice din UE reunește numeroși actori civili publici și privați de la nivel regional, național și de la nivelul UE, inclusiv autorități de asigurare a respectării legii. În același timp, securitatea cibernetică este un element-cheie al securității și apărării naționale[9]. Peisajul actual de la nivelul UE este ilustrat în ***anexa II***.

08 Statele membre sunt cele cărora le revine responsabilitatea principală pentru prevenirea, pregătirea și răspunsul în caz de incidente și crize cibernetice care le afectează. În conformitate cu articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană, securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru. Dat fiind că incidentele de securitate cibernetică pot perturba și afecta infrastructurile critice de informații de care depinde buna funcționare a pieței interne, UE joacă și ea un rol important în cazul unui incident semnificativ sau al unei crize[10]. Principalele entități din domeniul securității cibernetice de la nivelul UE sunt prezentate în ***figura 4*** de mai jos.

[9] Avizul nr. 02/2023 referitor la propunerea de regulament privind solidaritatea cibernetică.

[10] Planul de acțiune al UE pentru gestionarea crizelor cibernetice.

Figura 4 | Entitățile de la nivelul UE cu un rol esențial în securitatea cibernetică

Direcția Generală Rețele de Comunicare, Conținut și Tehnologie (DG CONNECT)

elaborează și pune în aplicare politica UE privind securitatea cibernetică, inclusiv prin formularea legislației relevante și consolidarea capacităților UE în materie de securitate cibernetică

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

are un mandat amplu, dar obiectivul său principal este de a asigura un nivel comun ridicat de securitate cibernetică în întreaga UE

Centrul european de competențe în materie de securitate cibernetică(ECCC)

înființat în 2021, este responsabil de punerea în aplicare a componentei de securitate cibernetică a programului „Europa digitală” și a proiectelor relevante din cadrul programului Orizont Europa

Consiliul Uniunii Europene

poate activa mecanismele integrate pentru un răspuns politic la crize, cu scopul de a coordona răspunsul politic la crize majore de la nivelul UE

Sursa: Curtea de Conturi Europeană.

Finanțarea din partea UE

09 În actualul cadru financiar multianual 2021-2027, principala sursă de finanțare pentru securitatea cibernetică este programul „Europa digitală”. Lansat în 2021, acesta este primul program al UE care urmărește în mod specific să stimuleze transformarea digitală a UE. El dispune de un buget total de 8,1 miliarde de euro[11].

10 „Europa digitală” finanțează acțiuni în materie de securitate cibernetică în cadrul obiectivului său specific nr. 3 – „Securitatea cibernetică și încrederea”. Mai exact, s-a prevăzut un buget de 1,4 miliarde de euro pentru:

- consolidarea coordonării în materie de securitate cibernetică între instrumentele și infrastructurile de date ale statelor membre;
- sprijinirea implementării pe scară largă a unor soluții de securitate cibernetică în toate sectoarele economiei.

11 Cea mai mare parte a finanțării alocate prin programul „Europa digitală” pentru securitatea cibernetică este furnizată prin intermediul cererilor de propuneri. În perioada noiembrie 2021-decembrie 2025, s-au lansat 12 astfel de cereri. Finanțarea din partea UE disponibilă pentru acestea se ridică la 825 de milioane de euro. Pentru 2026 și 2027 sunt planificate noi cereri de propuneri, prin care se urmărește să se acorde granturi suplimentare în valoare de 212 milioane de euro.

12 Un alt program important al UE de sprijinire a securității cibernetice este Orizont Europa. Proiectele în domeniul securității cibernetice sunt finanțate în principal în cadrul clusterului 3 – „Securitatea civilă pentru societate” – și se află, de obicei, într-un stadiu incipient de maturitate, ceea ce se explică prin faptul că programul Orizont Europa pune accentul pe cercetare și inovare. Mecanismul de redresare și reziliență oferă și el finanțare pentru măsuri de securitate cibernetică.

[11] Programul „Europa digitală”.

Sfera și abordarea auditului

13 Înmulțirea amenințărilor cibernetice și impactul potențial al acestora au evidențiat necesitatea de a ne consolida reziliența cibernetică colectivă. Obiectivul auditului Curții de Conturi Europene a fost de a evalua dacă acțiunile UE reușesc să faciliteze detectarea incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsul la acestea. Curtea a verificat în special dacă acest lucru era valabil pentru:

- rețelele și mecanismele de la nivelul UE (și anume rețeaua CSIRT, EU-CyCLONe, sistemul european de alertă în materie de securitate cibernetică, Centrul de analiză și cunoaștere a situației în materie cibernetică și rezerva UE pentru securitate cibernetică);
- acțiunile finanțate în cadrul programului „Europa digitală”.

Curtea nu a acoperit cooperarea în materie de asigurare a respectării legii la nivelul UE și nici acțiunile de disuasiune în spațiul cibernetic întreprinse în UE prin măsuri diplomatice sau activități de apărare.

14 Auditul acoperă perioada cuprinsă între 2022 și 2025. El se bazează pe: verificare documentară, o analiză a documentelor relevante, vizite de audit în trei state membre (Irlanda, Grecia și Italia), chestionare scrise și interviuri cu părțile interesate relevante. ***Figura 5*** prezintă modul în care Curtea a obținut probe pentru observațiile sale.

Figura 5 | Activitățile de audit desfășurate

Curtea a examinat

- **Cadrul juridic** aplicabil detectării incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsului la acestea
- **Rolurile și responsabilitățile** rețelelor și structurilor înființate la nivelul UE

Curtea a analizat

- Documente privind funcționarea **rețelelor CSIRT** și a **EU-CyCLONe**
- Documentație privind **cadrul de programare și de monitorizare a performanței aferent programului „Europa digitală”**
- Documentație privind **13 acțiuni finanțate de UE selectate** (11 granturi și 2 contracte – a se vedea lista detaliată din anexa III)

* Curtea a selectat acțiuni finanțate de UE în trei țări (Irlanda, Grecia și Italia) în care finanțarea relevantă prin programul „Europa digitală” era mai substanțială. Cele 11 granturi au fost selectate dintr-o listă de 137 de proiecte finanțate de UE relevante pentru detectarea amenințărilor și răspunsul la acestea, cu scopul de a acoperi o combinație diversificată de proiecte.

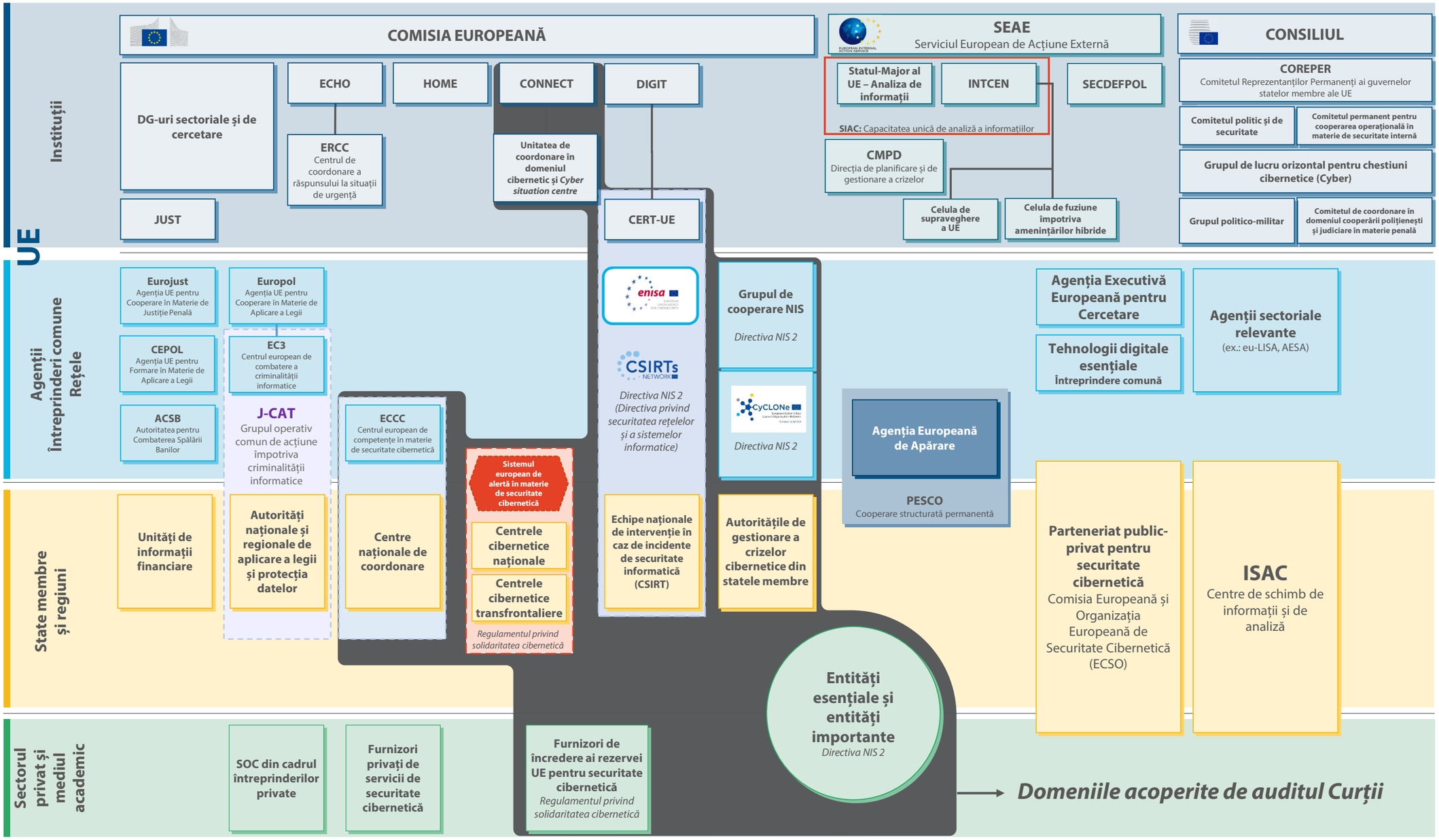
Curtea a intervievat

- Beneficiarii celor **11 granturi finanțate de UE incluse în eșantion**
- Reprezentanți ai autorităților naționale de securitate cibernetică din **trei state membre** (Irlanda, Grecia și Italia)
- Reprezentanți ai Comisiei Europene (**DG CONNECT**), ai **ENISA** și ai **ECCC**

Sursa: Curtea de Conturi Europeană.

15 Curtea se așteaptă ca observațiile sale să contribuie la îmbunătățirea eficacității și eficienței atât a detectării de către UE a incidentelor de securitate cibernetică semnificative și de mare amploare, cât și a răspunsului UE la acestea, precum și la îmbunătățirea modului în care sunt selectate și monitorizate acțiunile finanțate de UE. Metodologia de audit a Curții este conformă cu standardele internaționale de audit adoptate de Organizația Internațională a Instituțiilor Supreme de Audit (*International Organization of Supreme Audit Institutions* – INTOSAI).

Anexa II – Peisajul securității cibernetice din UE



DG CONNECT: Direcția Generală Rețele de Comunicare, Conținut și Tehnologie
DG ECHO: Direcția Generală Protecție Civilă și Operațiuni Umanitare Europene
DG HOME: Direcția Generală Migrație și Afaceri Interne
DG JUST: Direcția Generală Justiție și Consumatori
DIGIT: Direcția Generală pentru Servicii Digitale
AESA: Agenția Uniunii Europene pentru Siguranța Aviației
EU-CyCLONe: Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice
eu-LISA: Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție
INTCEN: Centrul de situații și de analiză a informațiilor al UE
SECDEFPOL: Politica de securitate și apărare
SOC: Centru de operațiuni de securitate

Anexa III – Acțiunile în materie de securitate cibernetică selectate

Nr.	Titlu	Țări	Data de începere	Data de încheiere	Costul total (în milioane de euro) și contribuția UE (în %)	Link către portalul UE pentru oportunități de finanțare și ofertare
Granturi pentru centrele cibernetice transfrontaliere care fac parte din sistemul european de alertă în materie de securitate cibernetică						
1	**Instituirea de SOC transfrontaliere (ATHENA)**	Bulgaria, Grecia, Cipru, Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	**PLATFORMA TRANSFRONTALIERĂ ENSOC (ENSOC)**	Spania, Italia, Luxemburg, Țările de Jos, Austria, Portugalia, România	1.1.2024	30.6.2028	10,4 (50 %)	
Granturi pentru implementarea Rețelei de centre naționale de coordonare în statele membre						
3	**Dezvoltarea și implementarea Centrului național de coordonare și dezvoltare în materie de securitate cibernetică pentru Irlanda (NCC-IE)**	Irlanda	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Centrul național de coordonare din Italia (NCC-IT)**	Italia	1.11.2023	31.10.2025	2,0 (50 %)	

Nr.	Titlu	Țări	Data de începere	Data de încheiere	Costul total (în milioane de euro) și contribuția UE (în %)	Link către portalul UE pentru oportunități de finanțare și ofertare
Granturi pentru consolidarea capacității centrelor de operațiuni de securitate (SOC), promovarea de noi aplicații ale IA și de alte tehnologii generice pentru SOC și furnizarea de sprijin pentru pregătire și de asistență reciprocă						
5	**Creșterea capacității Centrului consolidat de operațiuni de securitate al Greciei (EL-SOC)**	Grecia, Cipru	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Centrul elen de operațiuni de securitate pentru întreprinderile mici și mijlocii (GR-SME-SOC)**	Grecia	1.1.2024	31.12.2026	12,1 (50 %)	
7	**Centre operaționale de securitate de generație următoare (NG-SOC)**	Grecia, Spania, Cipru, Luxemburg, Slovenia, Norvegia	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Centrul de operațiuni de securitate al administrației locale irlandeze (ILG-SOC)**	Irlanda	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Un ecosistem interconectat al rețelelor de coordonare și răspuns în materie de securitate cibernetică (Cyber-CORE-Network)**	Irlanda	1.1.2024	31.12.2026	3,6 (50 %)	
10	**Armonizarea factorului uman, a proceselor și a tehnologiei pentru o securitate cibernetică solidă (CYberSynchrony)**	Belgia, Grecia, Italia, Cipru, Țările de jos	1.6.2024	31.5.2027	7,0 (100 %)	
11	**Centre avansate de operațiuni cooperative de securitate (ACSOC)**	Grecia, Italia, România	1.1.2025	31.12.2027	3,0 (50 %)	

Nr.	Titlu	Țări	Data de începere	Data de încheiere	Costul total (în milioane de euro) și contribuția UE (în %)	Link către portalul UE pentru oportunități de finanțare și ofertare
Contract-cadru pentru acțiunea ENISA de sprijin în materie de securitate cibernetică						
12	**Sprijinirea ENISA pentru furnizarea de servicii în cadrul acțiunii de sprijin în materie de securitate cibernetică (28 de loturi)**	27 de loturi pentru statele membre 1 lot paneuropean	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Contract de servicii pentru Centrul de analiză și cunoaștere a situației în materie cibernetică al DG CONNECT						
13	**Serviciul personalizat de sprijinire a Centrului de analiză și de cunoaștere a situației în materie cibernetică al Comisiei Europene**	-	30.12.2022	30.12.2026	18,0 (100 %)	

Sursa: Curtea de Conturi Europeană.

[1] Mai multe contracte semnate în decembrie 2022.

Anexa IV – Evaluarea Curții de Conturi Europene cu privire la proiectele de securitate cibernetică finanțate de UE

Satisfăcătoare *Anumite deficiențe*
Nesatisfăcătoare *Nu se poate formula nicio concluzie (este prea devreme)*

Nr.	Proiect	Proiectul răspunde majorității nevoilor identificate în cererea de propuneri	Până în prezent, proiectul și-a atins realizările și rezultatele planificate	Realizările proiectului au fost livrate în termenul prevăzut	Indicatorii de performanță ai proiectului sunt relevanți și măsurabili și sunt însoțiți de o valoare de referință și de o valoare-țintă
1	Instituirea de SOC transfrontaliere (ATHENA)	Satisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare
2	PLATFORMA TRANSFRONTALIERĂ ENSOC (ENSOC)	Satisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare
3	Dezvoltarea și implementarea Centrului național de coordonare și dezvoltare în materie de securitate cibernetică pentru Irlanda (NCC-IE)	Satisfăcătoare	Satisfăcătoare	Anumite deficiențe	Anumite deficiențe
4	Centrul național de coordonare din Italia (NCC-IT)	Satisfăcătoare	Satisfăcătoare	Satisfăcătoare	Anumite deficiențe
5	Creșterea capacității Centrului consolidat de operațiuni de securitate al Greciei (EL-SOC)	Satisfăcătoare	Anumite deficiențe	Nesatisfăcătoare	Nesatisfăcătoare
6	Centrul elen de operațiuni de securitate pentru întreprinderile mici și mijlocii (GR-SME-SOC)	Satisfăcătoare	Satisfăcătoare	Satisfăcătoare	Anumite deficiențe
7	Centre operaționale de securitate de generație următoare (NG-SOC)	Satisfăcătoare	Satisfăcătoare	Satisfăcătoare	Anumite deficiențe
8	Centrul de operațiuni de securitate al administrației locale irlandeze (ILG-SOC)	Satisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare	Nesatisfăcătoare
9	Un ecosistem interconectat al rețelelor de coordonare și răspuns în materie de securitate cibernetică (Cyber-CORE-Network)	Satisfăcătoare	Anumite deficiențe	Anumite deficiențe	Anumite deficiențe
10	Armonizarea factorului uman, a proceselor și a tehnologiei pentru o securitate cibernetică solidă (CYberSynchrony)	Anumite deficiențe	Nu se poate formula nicio concluzie (este prea devreme)	Nu se poate formula nicio concluzie (este prea devreme)	Anumite deficiențe
11	Centre avansate de operațiuni cooperative de securitate (ACSOC)	Satisfăcătoare	Nu se poate formula nicio concluzie (este prea devreme)	Nu se poate formula nicio concluzie (este prea devreme)	Nesatisfăcătoare

Acronime

Acronim	Definiție/explicație
CSIRT	Echipă de răspuns la incidente de securitate cibernetică
DG CONNECT	Direcția Generală Rețele de Comunicare, Conținut și Tehnologie
ECCC	Centrul european de competențe în materie de securitate cibernetică
ENISA	Agenția Uniunii Europene pentru Securitate Cibernetică
EU-CyCLONe	Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice
IMM	Întreprindere mică sau mijlocie
NCC	Centru național de coordonare (*national coordination centre*)
NIS	Securitate a rețelelor și a informațiilor
SOC	Centru de operațiuni de securitate

Glosar

Termen	Definiție/explicație
Actor care generează amenințări	Persoană sau grup care cauzează în mod intenționat prejudicii, perturbând servicii sau furând date prin exploatarea vulnerabilităților sistemelor, rețelelor și dispozitivelor informatice.
Amenințare cibernetică	Utilizarea potențială a spațiului cibernetic pentru a compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau a sistemelor de informații.
Centru cibernetic	Platformă centrală care reunește diverse servicii, instrumente și profesioniști din domeniul IT pentru a îmbunătăți monitorizarea, detectarea și analiza amenințărilor cibernetice, pentru a preveni incidentele de securitate cibernetică și pentru a sprijini producerea de informații privind amenințările cibernetice.
Centru de operațiuni de securitate	Unitate organizațională care se ocupă cu prevenirea amenințărilor și a incidentelor cibernetice și care colectează informații operative conexe.
Incident de securitate cibernetică de mare amploare	Incident de securitate cibernetică prea disruptiv pentru ca un stat membru să îi poată face față singur sau care are un impact semnificativ asupra a cel puțin două state membre.
Incident de securitate cibernetică semnificativ	Incident de securitate cibernetică ce a cauzat sau poate cauza perturbări grave sau pierderi financiare pentru o organizație ori prejudicii considerabile pentru alte entități sau persoane fizice.
Incident de securitate cibernetică/incident cibernetic	Eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau a sistemelor de informații.
Ransomware	Program *malware* care împiedică accesul victimelor la un sistem informatic sau care criptează fișiere astfel încât acestea să nu mai poată fi citite, forțând victima să plătească o răscumpărare pentru a redobândi accesul.
Taxonomie	În contextul securității cibernetice, un sistem de clasificare utilizat pentru organizarea, clasificarea și structurarea cunoștințelor cu privire la concepte-cheie, cum ar fi amenințările și incidentele.

Răspunsurile Comisiei

https://www.eca.europa.eu/ro/publications/SR-2026-19

Răspunsurile Centrului european de competențe în materie de securitate cibernetică (ECCC)

https://www.eca.europa.eu/ro/publications/SR-2026-19

Răspunsurile Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA)

https://www.eca.europa.eu/ro/publications/SR-2026-19

Calendar

https://www.eca.europa.eu/ro/publications/SR-2026-19

Echipa de audit

Rapoartele speciale ale Curții de Conturi Europene prezintă rezultatele auditurilor sale cu privire la politicile și programele UE sau la diverse aspecte legate de gestiune aferente unor domenii bugetare specifice. Curtea de Conturi Europeană selectează și concepe aceste sarcini de audit astfel încât impactul lor să fie maxim, luând în considerare riscurile la adresa performanței sau a conformității, nivelul de venituri sau de cheltuieli implicat, evoluțiile viitoare și interesul politic și public.

Acest audit al performanței a fost efectuat de Camera de audit III – Acțiuni externe, securitate și justiție, condusă de domnul George-Marius Hyzler, membru al Curții de Conturi Europene. Auditul a fost condus de domnul George-Marius Hyzler, membru al Curții de Conturi Europene, care a beneficiat de sprijinul unei echipe formate din: Romuald Kayibanda, șef de cabinet, și Annette Farrugia, atașată în cadrul cabinetului; Cyril Messein, manager principal; Frédéric Soblet, coordonator; Jurgen Manjé și Flavia Di Marco, auditori. Zoe Amador Martínez a furnizat asistență lingvistică. Dunja Weibel a asigurat sprijin pentru concepția grafică.



De la stânga la dreapta: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

DREPTURI DE AUTOR

© Uniunea Europeană, 2026

Politica Curții de Conturi Europene referitoare la reutilizare este definită în Decizia nr. 6-2019 a Curții de Conturi Europene privind politica în materie de date deschise și reutilizarea documentelor.

Cu excepția cazului în care se precizează altceva (de exemplu, într-o mențiune separată indicând drepturile de autor), conținutul elaborat de Curtea de Conturi Europeană pentru care UE deține drepturile de autor face obiectul licenței Creative Commons Atribuire 4.0 Internațional (CC BY 4.0). Prin urmare, ca regulă generală, reutilizarea este autorizată cu condiția menționării adecvate a autorilor și a indicării eventualelor modificări. Reutilizatorul conținutului elaborat de Curtea de Conturi Europeană nu poate altera sensul sau mesajul inițial. Curtea de Conturi Europeană nu răspunde pentru eventualele consecințe ale reutilizării.

Este necesar să obțineți o permisiune suplimentară în cazul în care un anumit conținut prezintă persoane fizice ce pot fi identificate, de exemplu, în cazul fotografiilor în care apar membri ai personalului Curții de Conturi Europene sau în cazul în care conținutul include lucrări ale unor terți.

Dacă se obține o astfel de permisiune, ea anulează și înlocuiește permisiunea de natură generală menționată mai sus și va indica în mod clar eventualele restricții de utilizare.

Pentru a utiliza sau a reproduce un conținut pentru care UE nu deține drepturile de autor, poate fi necesar să obțineți o permisiune în acest sens direct de la titularii drepturilor de autor.

Fotografia de pe pagina de titlu: © 4AXY – stock.adobe.com.

Figurile 6 și 8 – pictograme: aceste figuri au fost realizate folosind resurse de pe site-ul Flaticon.com. © Freepik Company S.L. Toate drepturile rezervate.

Figura 5 – hărțile: Eurostat.

Programele informatice sau documentele care fac obiectul unor drepturi de proprietate industrială, cum ar fi brevetele, mărcile, desenele și modelele înregistrate, logourile și denumirile, sunt excluse din politica Curții de Conturi Europene referitoare la reutilizare.

Familia site-urilor instituționale ale Uniunii Europene care sunt incluse în domeniul europa.eu oferă linkuri către site-uri terțe. Deoarece Curtea de Conturi Europeană nu are control asupra acestor site-uri, sunteți încurajați să verificați politica aplicată de ele în ceea ce privește respectarea vieții private și drepturile de autor.

Utilizarea logoului Curții de Conturi Europene

Logoul Curții de Conturi Europene nu poate fi utilizat fără acordul prealabil al Curții de Conturi Europene.

HTML	ISBN 978-92-849-7889-2	ISSN 1977-5806	doi:10.2865/1976159	QJ-01-26-032-RO-Q
PDF	ISBN 978-92-849-7890-8	ISSN 1977-5806	doi:10.2865/7474061	QJ-01-26-032-RO-N

REFERINȚA EXACTĂ

Curtea de Conturi Europeană, Raportul special nr. 19/2026 „Detectarea incidentelor de securitate cibernetică și răspunsul la acestea – Cadrul de cooperare al UE înregistrează progrese, dar, din cauza întârzierilor în punerea în aplicare și a schimbului limitat de informații, nu este decât parțial eficace”, Oficiul pentru Publicații al Uniunii Europene, 2026.

În ultimii ani, UE și-a consolidat cadrul de reglementare în materie de securitate cibernetică și a instituit rețele și mecanisme pentru gestionarea incidentelor cibernetice. De asemenea, UE finanțează proiecte în domeniul securității cibernetice prin Programul Europa Digitală.

Curtea de Conturi Europeană concluzionează că acțiunile UE facilitează doar parțial detectarea incidentelor de securitate cibernetică semnificative și de mare amploare și răspunsul la acestea. A fost instituit treptat un cadru de cooperare, dar se depun în continuare eforturi pentru ca acesta să devină pe deplin operațional. Schimbul limitat de informații, deficiențele de raportare și întârzierile semnificative în punerea în aplicare împiedică rețelele și mecanismele UE să își atingă întregul potențial. Proiectele urmăresc obiective relevante, dar mai multe dintre ele se confruntă cu dificultăți operaționale și cu întârzieri. În plus, există deficiențe în cadrul general de monitorizare a performanței. Curtea formulează o serie de recomandări menite să ajute la rezolvarea acestor probleme.

Raport special al Curții de Conturi Europene prezentat în temeiul articolului 287 alineatul (4) al doilea paragraf TFUE.

CURIA RATIONUM
CURTEA DE CONTURI EUROPEANĂ

Oficiul pentru Publicații al Uniunii Europene

CURTEA DE CONTURI EUROPEANĂ
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBURG

Tel. +352 4398-1

Întrebări: eca.europa.eu/ro/contact
Website: eca.europa.eu
Rețele sociale: @EUauditors