Consiliul
Uniunii Europene

Bruxelles, 6 decembrie 2024
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Subiect:	Concluziile Consiliului privind ENISA

În anexă, se pun la dispoziția delegațiilor Concluziile Consiliului privind ENISA, astfel cum au fost aprobate de Consiliu în cadrul reuniunii sale desfăşurate la 6 decembrie 2024.

ANEXĂ

Proiect de concluzii ale Consiliului privind ENISA

CONSILIUL UNIUNII EUROPENE

1. SUBLINIAZĂ că provocările generate de spațiul cibernetic mondial nu au mai fost niciodată atât de complexe, diverse și grave ca în prezent, fapt cauzat de nivelul de sofisticare al amenințărilor cibernetice emergente, de evoluția în continuă schimbare a mediului de securitate și de tensiunile geopolitice actuale. Prin urmare, UE și statele sale membre ar trebui să își continue eforturile în vederea sporirii rezilienței lor, astfel încât să poată identifica și aborda în mod eficace amenințările și provocările actuale și emergente. ATRAGE ATENȚIA ASUPRA FAPTULUI că ar trebui duse mai departe lucrările vizând un nivel mai ridicat al rezilienței cibernetice, pe baza unei abordări la nivelul întregii societăți. SCOATE ÎN EVIDENȚĂ că, în anii următori, UE și statele sale membre ar trebui să se concentreze pe punerea în aplicare efectivă a inițiativelor legislative și nelegislative în acest sens, pentru susținerea acțiunilor întreprinse până în prezent și pentru a contribui la acestea.

2. REAMINTIND că securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru, RECUNOAȘTE că UE și statele sale membre au colaborat extrem de mult în ultimii ani pentru a stabili structura instituțională și formele de colaborare necesare atât la nivel național, cât și la nivelul UE în domeniul cibernetic. SALUTĂ diversele inițiative legislative și nelegislative care au oferit UE și statelor sale membre un cadru solid și puternic în acest domeniu, sporind reziliența cibernetică globală a Uniunii. Acest cadru a evoluat pentru a acoperi mai multe aspecte ale domeniului cibernetic: securitatea, diplomația, asigurarea respectării legii și apărarea. IA ACT de faptul că din ecosistemul de securitate cibernetică al UE fac parte un număr mare de actori, inclusiv autoritățile de securitate cibernetică ale statelor membre, Grupul de cooperare NIS, rețeaua CSIRT, Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe), Rețeaua de centre naționale de coordonare (CNC), Grupul european pentru certificarea securității cibernetice (ECCG), Comisia, Serviciul European de Acțiune Externă (SEAE), Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Centrul european de competențe în materie de securitate cibernetică (ECCC), CERT-UE, Agenția Europeană de Apărare (AEA) și Centrul european de combatere a criminalității informatice (EC3) al Europolului, fiecare dintre aceștia deținând un rol precis în punerea în aplicare a cadrului de securitate cibernetică la nivelul UE.

3. RECUNOAȘTE că, în ultimele două decenii, ENISA s-a dovedit a fi o entitate de neprețuit în ecosistemul european de securitate cibernetică, jucând un rol esențial în sprijinirea activă a statelor membre și a instituțiilor, organelor, oficiilor și agențiilor UE în punerea în aplicare și dezvoltarea de către acestea a politicilor de securitate cibernetică, în consolidarea capacităților și pregătirea lor, în cooperarea lor și în promovarea de către acestea a conștientizării și certificării în materie de securitate cibernetică.

RECOMANDĂRI GENERALE DE POLITICĂ

4. INVITĂ Comisia să utilizeze **evaluarea Regulamentului privind securitatea cibernetică** drept o oportunitate de a examina modul în care acesta poate contribui la simplificarea ecosistemului complex de securitate cibernetică, sporind astfel eficacitatea și utilizarea eficientă a resurselor. Prin urmare, SOLICITĂ Comisiei să se asigure că mandatul ENISA de a sprijini statele membre și instituțiile, organele, oficiile și agențiile UE este orientat și definit în mod clar, cu obiective strategice concrete și sarcini prioritizate, pe lângă o repartizare mai precisă a sarcinilor și competențelor în raport cu alți actori. În acest sens, INVITĂ Comisia să examineze și să consolideze suplimentar rolul ENISA în sprijinirea cooperării operaționale la nivelul UE și între statele membre în ceea ce privește sporirea rezilienței cibernetice, ținând seama de competențele statelor membre în acest domeniu. În plus, SOLICITĂ Comisiei să consolideze rolul consultativ al ENISA în asigurarea de orientări și recomandări furnizate de experți și bazate pe dovezi, în ceea ce privește punerea în aplicare a inițiativelor legislative și nelegislative actuale și viitoare ale UE, asigurând în același timp un cadru coerent al UE în materie de securitate cibernetică.

5. În același spirit, ÎNCURAJEAZĂ Comisia să ia în considerare raționalizarea rolului ENISA în ceea ce privește sarcinile care nu se află în centrul misiunii sale. SUBLINIAZĂ că **responsabilitățile** ENISA **au fost extinse în mod semnificativ** prin inițiativele legislative recente, inclusiv Directiva NIS 2, Regulamentul privind reziliența cibernetică și Regulamentul privind solidaritatea cibernetică, printre altele. IA ACT de faptul că ENISA a primit resurse suplimentare ca urmare a unora dintre aceste inițiative, totuși SUBLINIAZĂ că extinderea responsabilităților ENISA și complexitatea tot mai mare a amenințărilor și provocărilor cibernetice au condus la o creștere considerabilă a sarcinilor sale, care ar trebui să se reflecte în **resurse adecvate** – umane, financiare și tehnice – pentru a permite agenției să execute pe deplin toate sarcinile care intră în sfera sa de competență, fără a aduce atingere negocierii cadrului financiar multianual. În acest scop, SOLICITĂ Comisiei să stabilească o ordine de prioritate a acțiunilor și să acorde o poziție prioritară sarcinilor legate de sprijinirea statelor membre în sporirea rezilienței lor cibernetice, a cooperării lor operaționale și a dezvoltării și punerii în aplicare a dreptului Uniunii la elaborarea proiectului de buget general al Uniunii.

SPRIJINUL ENISA PENTRU DEZVOLTAREA ȘI PUNEREA ÎN APLICARE A POLITICILOR

6. REAMINTEȘTE că, în temeiul actualului cadru juridic în materie de securitate cibernetică, ENISA are mai multe responsabilități esențiale de sprijin și consiliere în întreaga UE. SALUTĂ în acest sens rolul ENISA în acordarea de **asistență statelor membre** în ceea ce privește punerea în aplicare efectivă a inițiativelor legislative și nelegislative. INVITĂ ENISA, în strânsă legătură cu Grupul de cooperare NIS și cu Comisia, să continue să furnizeze analize și informații generale cu privire la cadrul juridic actual în ceea ce privește securitatea cibernetică. ÎNCURAJEAZĂ ENISA să facă schimb de orientări tehnice și de bune practici și să le promoveze în mod activ, regulat și structurat, sprijinind statele membre în punerea în aplicare a politicii și a legislației în materie de securitate cibernetică.

7. RECUNOAȘTE rolul vital al ENISA în dezvoltarea **sistemelor europene de certificare a securității cibernetice**, consolidând încrederea în produsele, serviciile și procesele TIC și, în plus, în serviciile de securitate gestionate, având în vedere viitoarea modificare specifică a Regulamentului privind securitatea cibernetică. SUBLINIAZĂ preocupările statelor membre și industriei legate de procesul îndelungat de selecție, elaborare și adoptare a sistemelor de certificare a securității cibernetice; prin urmare, ÎNDEAMNĂ Comisia să valorifice oportunitatea oferită de evaluarea Regulamentului privind securitatea cibernetică pentru a găsi căi către o abordare a dezvoltării sistemelor UE de certificare a securității cibernetice care să fie mai flexibilă, bazată pe riscuri, precum și mai transparentă și mai rapidă, SUBLINIIND totodată rolul important al statelor membre în acest proces. În plus, PUNE ACCENT PE importanța atribuirii explicite a responsabilității pentru menținerea fiecărui sistem de certificare. În plus, REAMINTEȘTE că, la elaborarea propunerilor de sisteme, ENISA ar trebui să consulte toate părțile interesate relevante în timp util prin intermediul unui proces formal, deschis, transparent și incluziv și că, la evaluarea eficienței și utilizării sistemelor adoptate, Comisia ar trebui să desfășoare consultări într-un mod deschis, transparent și incluziv. ÎNCURAJEAZĂ ENISA să consolideze suplimentar colaborarea cu comunitatea de protecție a datelor, în special cu Comitetul european pentru protecția datelor, după caz, și cu autoritățile naționale competente, vizând în special promovarea sinergiilor în contextul dezvoltării viitoarelor sisteme europene de certificare a securității cibernetice.

8. Pentru a preveni sarcina administrativă inutilă care ar putea decurge dintr-un cadru de raportare complex, SOLICITĂ ENISA, în cooperare cu Comisia, să continue schimburile cu statele membre cu privire la aspectele practice, simplificarea și raționalizarea procedurii de raportare. În plus, REAMINTEȘTE invitația adresată Comisiei de a elabora, cu sprijinul ENISA și al altor entități relevante ale UE, o cartografiere a obligațiilor de raportare relevante prevăzute în actele legislative corespunzătoare ale UE în domeniul cibernetic și digital. REAMINTEȘTE că schimbul de informații dintre ENISA și statele membre se bazează pe o relație de încredere, în care securitatea și confidențialitatea sunt garantate în conformitate cu Regulamentul privind securitatea cibernetică și cu normele și protocoalele relevante și ar trebui să se limiteze la ceea ce este relevant și proporțional cu obiectivul schimbului. SUBLINIAZĂ necesitatea ca datele și informațiile să fie tratate cu atenția cuvenită.

9. SCOATE ÎN EVIDENȚĂ FAPTUL că ENISA este responsabilă de instituirea și menținerea **platformei unice de raportare în temeiul Regulamentului privind reziliența cibernetică**, aceasta urmând să aibă o valoare adăugată operațională concretă, în special pentru vulnerabilitățile exploatate activ și incidentele grave care afectează securitatea produselor cu elemente digitale. Având în vedere domeniul larg de aplicare al acestei legislații orizontale, platforma unică de raportare ar trebui să fie un instrument eficace și sigur pentru facilitarea schimbului de informații între CSIRT naționale și ENISA. În consecință, ÎNDEAMNĂ ENISA ca, pe lângă alocarea de resurse umane suficiente, să accelereze instituirea platformei ca prioritate-cheie pentru a asigura disponibilitatea acesteia până la termenul stabilit în Regulamentul privind reziliența cibernetică.

10. RECUNOAȘTE rolul ENISA în instituirea unei **baze de date europene a vulnerabilităților**, care vizează asigurarea unei mai mari transparențe în ceea ce privește divulgarea vulnerabilităților, asigurând, în același timp, gestionarea adecvată a datelor sensibile. Având în vedere sfârșitul perioadei de transpunere a Directivei NIS 2, ÎNDEAMNĂ ENISA să intensifice toate activitățile necesare pentru a asigura buna funcționare a acestei baze de date. În paralel, INVITĂ Grupul de cooperare NIS, cu sprijinul ENISA, să facă publice în continuare orientări, politici și proceduri privind divulgarea vulnerabilităților.

11. RECUNOAȘTE beneficiile **acțiunii de sprijin în materie de securitate cibernetică** desfășurate de ENISA, care funcționează ca o rezervă de servicii de securitate cibernetică disponibile pentru statele membre pentru a completa eforturile acestora, precum și experiența ENISA dobândită în urma punerii în aplicare a acțiunii respective. În acest sens, SUBLINIAZĂ că ENISA ar trebui să aibă un rol central în administrarea și operarea rezervei UE pentru securitate cibernetică. INVITĂ ENISA să înceapă cartografierea serviciilor necesare și a disponibilității acestora imediat după intrarea în vigoare a Regulamentului privind solidaritatea cibernetică, astfel încât rezerva UE pentru securitate cibernetică să fie cât mai utilă și adaptată nevoilor utilizatorilor în toate statele membre. INVITĂ ENISA ca, după ce este mandatată, să implice statele membre, în special prin colectarea de contribuții cu privire la criteriile necesare și prin informarea cu privire la viitoarele licitații, încă de la începutul procesului de instituire a rezervei UE pentru securitate cibernetică. INVITĂ ENISA ca, după ce i se încredințează mandatul, să se asigure că procesul de selecție a prestatorilor de servicii de securitate gestionate de încredere este transparent, deschis, echitabil și permite participarea prestatorilor din toate statele membre, indiferent de dimensiuni. În plus, REAMINTEȘTE că ENISA trebuie să emită fără întârzieri nejustificate orientările privind interoperabilitatea pentru centrele cibernetice transfrontaliere.

12. SUBLINIAZĂ că **monitorizarea tendințelor în ceea ce privește tehnologiile emergente** într-un domeniu care evoluează rapid, cum este cel cibernetic, este de o importanță crucială pentru menținerea și consolidarea în continuare a poziției noastre cibernetice. RECUNOAȘTE activitatea desfășurată de ENISA pentru a atrage atenția publicului asupra riscurilor și posibilităților unor tehnologii precum inteligența artificială și informatica cuantică, facilitând astfel o mai bună înțelegere a provocărilor actuale. ÎNCURAJEAZĂ ENISA să contribuie în continuare la aceste sarcini, să pledeze în mod activ pentru punerea în aplicare a recomandărilor sale și să ofere consiliere ECCC și să colaboreze cu acesta, după caz.

SPRIJINUL ACORDAT DE ENISA STATELOR MEMBRE PENTRU A SPORI REZILIENȚA CIBERNETICĂ ȘI COOPERAREA OPERAȚIONALĂ

13. SUBLINIAZĂ că ENISA îndeplinește un rol important **de secretariat al celor două rețele de cooperare cibernetică conduse de statele membre la nivelul UE, rețeaua CSIRT și EU-CyCLONe**. ATRAGE ATENȚIA asupra participării valoroase a ENISA la Grupul de cooperare NIS, în special prin implicarea sa activă și prin contribuțiile sale tehnice în ceea ce privește diferitele direcții de lucru. ÎNCURAJEAZĂ ENISA să sprijine în continuare funcționarea și cooperarea rețelelor respective în viitor, deoarece acestea oferă canale fundamentale pentru ca statele membre să colaboreze la diferite niveluri.

14. REITEREAZĂ necesitatea de a îmbunătăți **conștientizarea comună a situației** la nivelul UE, care contribuie la poziția cibernetică a UE, în legătură cu depistarea incidentelor de securitate cibernetică, prevenirea acestora și răspunsul la acestea. În acest sens, SUBLINIAZĂ importanța unor activități de analiză prospectivă ale ENISA, a unor rapoarte periodice și a unor evaluări ale amenințărilor, care, considerate în ansamblu, contribuie la îmbunătățirea conștientizării situației. ÎNCURAJEAZĂ ENISA să lucreze în strânsă cooperare cu statele membre, pentru a contribui la îmbunătățirea conștientizării situației la nivelul UE. În acest context, RECUNOAȘTE rolul important deținut de ENISA împreună cu CERT-UE și cu Europolul în sprijinirea Consiliului prin informări situaționale în contextul setului de instrumente pentru diplomația cibernetică, care completează conștientizarea situației furnizată de Capacitatea unică de analiză a informațiilor (SIAC), și SUBLINIAZĂ necesitatea de a construi din diferite surse, incluzând sectorul privat, o imagine cuprinzătoare a amenințărilor. ÎNCURAJEAZĂ, în acest sens, dezvoltarea în continuare a cooperării ENISA cu SEAE, în special cu INTCEN, cu respectarea deplină a mandatelor lor respective.

15. SUBLINIAZĂ că centrul de analiză și de cunoaștere a situației în materie cibernetică al Comisiei îndeplinește o funcție internă în cadrul Comisiei și este sprijinit de colaborarea sa cu ENISA și cu CERT-UE. Pentru a crea un potențial maxim pentru sinergii și a reduce complexitatea în cadrul ecosistemului de securitate cibernetică al UE, INVITĂ Comisia să țină seama de rezultatele evaluării Regulamentului privind securitatea cibernetică, precum și de discuțiile privind evaluarea Planului de acțiune în materie de securitate cibernetică, pentru a raționaliza sarcinile centrului de analiză și de cunoaștere a situației în materie cibernetică al Comisiei și sarcinile conexe ale ENISA. ÎNCURAJEAZĂ Comisia să evite suprapunerea inutilă a sarcinilor, protejând în același timp rolul central al ENISA în ceea ce privește contribuția la îmbunătățirea conștientizării comune a situației la nivelul Uniunii în sprijinul statelor membre, cu respectarea corespunzătoare a competențelor naționale ale acestora.

16. SUBLINIAZĂ că îmbunătățirea conștientizării comune a situației este o condiție prealabilă pentru gestionarea promptă și eficace a crizelor în întreaga Uniune. PUNE ACCENT PE FAPTUL că, la nivelul UE, **răspunsul la incidentele cibernetice de mare amploare** implică o varietate de actori-cheie și că, în cazul unor astfel de incidente, cooperarea eficace dintre statele membre este susținută în principal de rețeaua CSIRT și de EU-CyCLONe. ENISA joacă un rol important în gestionarea crizelor cibernetice în calitate de secretariat al rețelei CSIRT și al EU-CyCLONe. INVITĂ Comisia să utilizeze evaluarea Planului de acțiune în materie de securitate cibernetică pentru a reflecta în mod corespunzător sarcinile și responsabilitățile suplimentare destinate să contribuie la elaborarea unui răspuns bazat pe cooperare la incidentele sau crizele cibernetice transfrontaliere de mare amploare, precum și rolul atribuit ENISA în calitate de secretariat al rețelei CSIRT și al EU-CyCLONe și în temeiul recentei legislații în materie de securitate cibernetică.

17. SUBLINIAZĂ importanța organizării unor **exerciții** periodice **de securitate cibernetică**, care să sporească considerabil gradul de pregătire al UE în ceea ce privește răspunsul la incidente și crize. RECUNOAȘTE că ENISA a acumulat o experiență valoroasă și vastă în acest domeniu prin sprijinirea statelor membre. RECUNOAȘTE rolul important al ENISA în fazele de planificare, pregătire, execuție și evaluare a exercițiilor de securitate cibernetică și SUBLINIAZĂ că aceasta ar trebui să rămână în continuare unul dintre actorii centrali la nivelul UE, ținând seama de faptul că astfel de exerciții ar trebui să se desfășoare pe baza unor cadre structurate și a unor terminologii comune. INVITĂ ENISA, rețeaua CSIRT și EU-CyCLONe să utilizeze cât mai eficient exercițiile periodice existente pentru a testa și a îmbunătăți cadrul de răspuns al UE la situații de criză și pentru a asigura valorificarea la maximum a lecțiilor învățate.

COOPERAREA ENISA CU ALȚI ACTORI DIN ECOSISTEMUL DE SECURITATE CIBERNETICĂ

18. REITEREAZĂ faptul că, având în vedere caracterul orizontal al securității cibernetice, este vitală **colaborarea dintre toți actorii de la nivelul statelor membre și de la nivelul Uniunii** și, prin urmare, SUBLINIAZĂ că creșterea rezilienței cibernetice globale la nivel european necesită, de asemenea, o colaborare între ENISA și alte entități relevante din domeniul cibernetic.

19. SUBLINIAZĂ că capacitatea instituțiilor, organelor, oficiilor și agențiilor UE de a rămâne sigure din punct de vedere cibernetic este importantă pentru reziliența cibernetică globală la nivelul UE, iar rolul CERT-UE pentru această reziliență este de neprețuit. În acest sens, SALUTĂ cooperarea structurată instituită între CERT-UE și ENISA și ÎNCURAJEAZĂ cele două părți să își continue cooperarea strânsă în viitor.

20. În urma obținerii autonomiei financiare, ECCC va contribui în mod semnificativ la dezvoltarea unui ecosistem european solid de securitate cibernetică în domeniul cercetării, industrial și tehnologic, care să cuprindă competențe pentru dezvoltarea forței de muncă, în conformitate cu mandatul său. ÎNCURAJEAZĂ ENISA și ECCC să își continue cooperarea strânsă, în special în ceea ce privește nevoile și prioritățile în materie de cercetare și inovare, precum și competențele cibernetice, pentru a spori competitivitatea industriei securității cibernetice a Uniunii. INVITĂ Comisia să examineze modalitățile de optimizare în continuare a sinergiilor în funcționarea ENISA și a ECCC și de raționalizare sporită a activităților, în conformitate cu mandatele lor respective.

21. SUBLINIAZĂ că furnizarea de actualizări periodice cu privire la situația amenințărilor contribuie la o mai bună identificare a măsurilor și instrumentelor necesare pentru a combate în mod eficace criminalitatea informatică. SUBLINIAZĂ valoarea adăugată a rapoartelor privind evaluarea cibernetică comună a UE (J-CAR), care sunt rezultatul colaborării dintre ENISA, EC3 al Europolului și CERT-UE și care au oferit deja o contribuție valoroasă la abordarea diferitelor provocări, inclusiv combaterea criminalității informatice. INVITĂ ENISA și Europolul să continue colaborarea într-un mod structurat în viitor.

22. SUBLINIAZĂ că apărarea cibernetică constituie o parte importantă și în continuă dezvoltare a combaterii amenințărilor generate de spațiul cibernetic. SUBLINIAZĂ necesitatea ca ENISA să colaboreze cu SEAE și cu Comisia, în cazurile în care ENISA are un rol în sprijinirea punerii în aplicare a politicii UE în domeniul apărării cibernetice, în strânsă cooperare cu AEA, ECCC și comunitatea de apărare cibernetică. SUBLINIAZĂ rolul ENISA ca agenție civilă. SUBLINIAZĂ importanța aprofundării și raționalizării cooperării civilo-militare în domeniul cibernetic în cadrul UE, inclusiv a unor repartizări clare ale rolurilor și responsabilităților între cele două comunități și între UE și NATO, cu respectarea deplină a principiilor incluziunii, reciprocității, deschiderii reciproce și transparenței, precum și a autonomiei decizionale a ambelor organizații. ÎNCURAJEAZĂ ENISA să continue acordurile de lucru cu Agenția NATO pentru comunicații și informații.

23. ÎNCURAJEAZĂ UE să continue să promoveze valorile și eforturile noastre comune în cadrul forumurilor mondiale pentru a garanta un spațiu cibernetic liber, mondial, deschis și securizat. SUBLINIAZĂ că natura transfrontalieră a amenințărilor și incidentelor cibernetice necesită o colaborare puternică și eficace, nu numai la nivelul UE, ci și **cu organizațiile și partenerii internaționali**. IA ACT de faptul că implicarea internațională a ENISA ar trebui să se concentreze asupra partenerilor strategici și a țărilor candidate la aderarea la UE, în conformitate cu politica externă și de securitate comună a UE. SUBLINIAZĂ că, în implicarea sa internațională, ENISA ar trebui să acționeze în conformitate cu mandatul său și cu dispozițiile respective ale Regulamentului privind securitatea cibernetică. RECUNOAȘTE necesitatea de a clarifica, în conformitate cu procedurile relevante, implicarea internațională a ENISA, asigurându-se, în special, informarea în mod corespunzător și în timp util a consiliului său de administrație cu privire la activitățile conexe. ÎNCURAJEAZĂ implicarea ENISA în cadrele internaționale relevante de cooperare în materie de securitate cibernetică, inclusiv în organizații precum NATO și OSCE.

24. REITEREAZĂ faptul că UE și statele sale membre au evidențiat frecvent lacune în ceea ce privește **competențele în materie de securitate cibernetică**. REAMINTEȘTE că Comisia și ENISA au introdus un cadru amplu și cuprinzător cu scopul oferirii de orientări tuturor părților implicate, cum ar fi Cadrul european de competențe în materie de securitate cibernetică, Comunicarea privind Academia de competențe în materie de securitate cibernetică și Conferința europeană privind competențele în domeniul cibernetic, organizată anual, și ÎNCURAJEAZĂ Comisia și ENISA să valorifice aceste inițiative, acordând o atenție deosebită discuțiilor în curs privind consorțiul pentru o infrastructură digitală europeană (EDIC). În acest scop, INVITĂ Comisia să colaboreze cu statele membre interesate de înființarea EDIC. RECUNOAȘTE că atât ENISA, cât și ECCC sunt mandatate să promoveze competențele în întreaga Uniune. INVITĂ ENISA să acorde prioritate sprijinirii eforturilor statelor membre în materie de competențe și educație, consolidând sensibilizarea publicului larg, și să colaboreze cu ECCC, după caz.

25. RECUNOAȘTE că ENISA a dezvoltat **cooperarea cu sectorul privat** în ultimii ani. REAMINTEȘTE că, întrucât sectorul privat monitorizează în permanență situația amenințărilor cibernetice, informațiile colectate de industrie ar putea contribui la îmbunătățirea conștientizării comune a situației. Prin urmare, ÎNCURAJEAZĂ ENISA, în strânsă cooperare cu statele membre și la nivelul entităților din UE, să consolideze cooperarea cu sectorul privat.

26. INVITĂ Comisia și ENISA să ia în considerare modalități de consolidare a colaborării dintre ENISA și organismele europene **de standardizare**. SUBLINIAZĂ necesitatea ca ENISA să își sporească expertiza pentru standardizarea europeană în materie de securitate cibernetică prin monitorizarea activităților de standardizare și prin participarea la acestea, printre altele.

27. ÎNDEAMNĂ Comisia și ENISA să examineze modalitățile de optimizare suplimentară a funcționării cadrului UE în materie de securitate cibernetică, ținând seama de recomandările și propunerile formulate în prezentele concluzii. Cooperarea continuă, prioritizarea sarcinilor și a resurselor, precum și simplificarea situației complexe a securității cibernetice vor constitui elemente-cheie pentru a face față provocărilor actuale și viitoare.