Consiliul
Uniunii Europene

Bruxelles, 21 aprilie 2023
(OR. en)

8513/23

CYBER 93
TELECOM 109
EDUC 133
BUDGET 7
CADREFIN 52
EMPL 180
COMPET 342
IND 182
JAI 470
MI 313
POLMIL 88

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	19 aprilie 2023
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2023) 207 final
Subiect:	COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU **Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE („Academia de competențe în materie de securitate cibernetică”)**

În anexă, se pune la dispoziția delegațiilor documentul COM(2023) 207 final.

Anexă: COM(2023) 207 final

COMISIA
EUROPEANĂ

Strasbourg, 18.4.2023
COM(2023) 207 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE („Academia de competențe în materie de securitate cibernetică”)

Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE

(„Academia de competențe în materie de securitate cibernetică”)

1. O nevoie urgentă de a reduce riscurile prin abordarea deficitului și a lacunelor în materie de competențe privind securitatea cibernetică

Securitatea cibernetică nu este doar o componentă a securității cetățenilor, întreprinderilor și statelor membre. De securitatea cibernetică depinde totodată asigurarea stabilității politice a UE, a stabilității democrațiilor sale și a prosperității societății și întreprinderilor noastre. **Peisajul amenințărilor** la adresa securității cibernetice a evoluat considerabil în ultimii ani, existând o tendință îngrijorătoare ca un număr tot mai mare de atacuri cibernetice să vizeze infrastructura critică militară și civilă din UE. Actorii care generează amenințări își sporesc capacitățile, apărând amenințări noi, hibride și emergente, cum ar fi utilizarea roboților software și a tehnicilor bazate pe inteligența artificială[1]. În special, actorii care generează amenințări de tip ransomware cauzează în mod regulat prejudicii considerabile entităților, atât din punct de vedere financiar, cât și din punctul de vedere al reputației[2].

Un număr mare de incidente de securitate cibernetică au vizat, de asemenea, administrația publică și guvernele din statele membre, precum și instituțiile, organele, oficiile și agențiile europene[3]. Sectorul financiar[4] și cel al sănătății[5], ambele considerate stâlpi ai societății și economiei, au fost, de asemenea, vizate în mod constant[6]. Tensiunile geopolitice asociate războiului de agresiune al Rusiei împotriva Ucrainei au sporit amenințarea la adresa securității cibernetice[7] și au potențialul de a ne destabiliza societatea. **Securitatea** UE nu poate fi garantată fără **cel mai valoros atu al UE: populația sa.** UE are nevoie urgent de profesioniști cu aptitudini și competențe adecvate pentru a preveni, detecta, descuraja și apăra

[1] Raportul ENISA privind situația amenințărilor în 2022 – ENISA (europa.eu).

[2] Europol, *Internet Organised Crime Threat Assessment* (IOCTA) (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online), 2021. Acești actori se bazează pe modelul *ransomware-as-a-service* (ransomware ca serviciu). Costul anual pentru întreprinderi a depășit 18,4 miliarde EUR în 2022 [*Cybereason 2022 Report on the true cost or Ransomware* (Raportul Cybereason pe 2022 privind adevăratul cost al ransomware-ului)].

[3] A se vedea, de exemplu, publicația comună a ENISA și CERT-UE, JP-23-01 – Activitățile susținute ale actorilor specifici care generează amenințări, TLP:CLEAR, 15 februarie 2023.

[4] A se vedea, de exemplu, cazul Germaniei, unde 90 % din fraudele privind corespondența raportate în perioada 1 iunie 2021 - 31 mai 2022 au fost de tipul phishing financiar sau atacuri asupra unei societăți din sectorul financiar, implicând peste 20 000 de dispozitive infectate din 125 de țări, *The State of IT Security in Germany in 2022* (Situația securității IT în Germania în 2022), *Bundesamt für Sicherheit in der Informationstechnik* (BSI), 1 ianuarie 2023.

[5] A se vedea, de exemplu, cazul Franței, unde au avut loc atacuri de tip ransomware asupra unităților publice de asistență medicală, cum ar fi Centre Hospitalier Sud Francilien, în cursul cărora 11 GB de date cu caracter personal și date medicale, precum și date referitoare la personal au fost compromise și publicate de actorul care generează amenințări, *Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023*.

[6] Raportul ENISA privind situația amenințărilor în 2022.

[7] A se vedea, de asemenea: CERT-UE – Războiul Rusiei împotriva Ucrainei:un an de operațiuni cibernetice (europa.eu); Operațiunile cibernetice ale Rusiei împotriva Ucrainei:declarația Înaltului Reprezentant în numele Uniunii Europene, 10 mai 2022; Declarația Înaltului Reprezentant, în numele Uniunii Europene, cu privire la activitățile cibernetice răuvoitoare desfășurate de hackeri și de grupurile de hackeri în contextul agresiunii Rusiei împotriva Ucrainei, 19 iulie 2022.

UE, inclusiv infrastructurile sale cele mai importante, împotriva atacurilor cibernetice și pentru a-i asigura **reziliența**.

Deficitul de talente în materie de securitate cibernetică afectează și mai mult **competitivitatea** și **creșterea** Europei, care depind în mare măsură de dezvoltarea și adoptarea tehnologiilor digitale strategice (de exemplu, inteligența artificială, 5G și cloud). Este nevoie de o forță de muncă calificată în domeniul securității cibernetice pentru ca UE să rămână în măsură să furnizeze tehnologii avansate esențiale într-un context global.

Pentru a se pregăti și a face față acestui peisaj al amenințărilor în continuă evoluție și pentru a stimula competitivitatea UE, politica UE în materie de securitate cibernetică a înregistrat progrese semnificative în ultimii ani, conducând la adoptarea unei serii de inițiative, cum ar fi Strategia de securitate cibernetică a UE pentru deceniul digital[8], Directiva revizuită privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS2)[9], legislația sectorială a UE în materie de securitate cibernetică[10], politica UE privind apărarea cibernetică[11], Actul privind reziliența cibernetică[12] și Actul privind solidaritatea cibernetică, propuse de Comisie împreună cu prezenta comunicare. Însă fără persoanele calificate necesare pentru a le pune în aplicare, aceste acte legislative nu își vor atinge obiectivele. Deși cunoștințele de bază în materie de securitate cibernetică ale populației generale sunt abordate ca parte a inițiativelor care sprijină dezvoltarea competențelor generale necesare pentru participarea în societate[13], o forță de muncă competentă este esențială atât în sectorul public, cât și în cel privat, atât la nivel național, cât și la nivelul UE, inclusiv în cadrul organizațiilor de standardizare, **pentru a îndeplini aceste cerințe juridice și de politică în materie de securitate cibernetică.**

Securitatea și competitivitatea UE depind, prin urmare, de existența unei forțe de muncă calificate în domeniul securității cibernetice. Cu toate acestea, UE se confruntă cu un deficit foarte mare de profesioniști calificați în domeniul securității cibernetice, ceea ce expune UE, statele sale membre, întreprinderile și cetățenii săi la riscul de incidente de securitate cibernetică. În 2022, deficitul de profesioniști în domeniul securității cibernetice în Uniunea Europeană a variat între **260 000**[14] **și 500 000**[15], în timp ce nevoile UE în materie de forță de

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

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

[10] Cum ar fi, pentru sectorul financiar, Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (Regulamentul DORA).

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

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

[13] Printre inițiativele relevante care abordează competențele digitale generale ale populației: obiectivul ca 80 % din populație să dețină competențe digitale de bază până în 2030, ca obiectiv al Planului de acțiune privind Pilonul european al drepturilor sociale și al Busolei pentru dimensiunea digitală, al Planului de acțiune pentru educația digitală 2021-2027, al instrumentului cadru al competențelor digitale sau al propunerii de recomandare a Consiliului privind îmbunătățirea ofertei de competențe digitale în educație și formare.

[14] (ISC)² în *Assessing Cyber Skills on the basis of the ECSF* (Evaluarea competențelor cibernetice pe baza ECSF), webinar ENISA, 16 februarie 2023.

muncă în domeniul securității cibernetice au fost estimate la 883 000 de profesioniști[16], ceea ce sugerează o neconcordanță între competențele disponibile și cele necesare pe piața forței de muncă. Forța de muncă din domeniul securității cibernetice este afectată și mai mult din cauza concepției greșite asociate imaginii sale tehnice, în continuare **femeile** nefiind atrase de acest domeniu, procentul lor ridicându-se la 20 % din rândul absolvenților din domeniul securității cibernetice[17] și la 19 % din rândul specialiștilor în tehnologia informației și comunicațiilor (TIC)[18]. Pentru a aborda acest aspect, **programul de politică pentru 2030 privind deceniul digital al Europei**[19] a stabilit obiectivul de creștere a numărului profesioniștilor din domeniul TIC cu 20 de milioane până în 2030 și de a realiza, în același timp, convergența de gen. În plus, punerea în aplicare a politicii UE emergente necesită o forță de muncă suficientă și corespunzător calificată. De exemplu, peste 42 % dintre liderii IT de rang înalt din sectorul serviciilor financiare au subliniat lipsa competențelor și a calificărilor în materie de securitate cibernetică drept o provocare majoră cu care se confruntă întreprinderile lor în ceea ce privește apărarea cibernetică și gestionarea incidentelor[20], într-un moment în care vor trebui să pună în aplicare legislația sectorială în materie de securitate cibernetică, cum ar fi Actul legislativ privind reziliența operațională digitală (DORA).

Reticența angajatorilor de a investi în capitalul uman, căutând forță de muncă deja formată și experimentată, contribuie și mai mult la limitarea pieței forței de muncă[21]. Acest deficit afectează toate tipurile de întreprinderi, inclusiv întreprinderile mici și mijlocii (**IMM-uri**), care reprezintă 99 % din totalul întreprinderilor din UE[22]. Provocarea este, de asemenea, una ridicată pentru **administrațiile publice,** care sunt prejudiciate în mare măsură și cel mai afectate de incidentele de securitate cibernetică[23].

Eliminarea deficitului UE de talente profesionale în domeniul securității cibernetice este, prin urmare, o chestiune urgentă, întrucât sunt în joc securitatea și competitivitatea UE.

2. Lipsa sinergiilor și a acțiunilor coordonate pentru eliminarea deficitului de competențe în materie de securitate cibernetică

Inițiativele la nivel european și național coordonate de entități publice și private pentru a aborda deficitele de pe piața forței de muncă în materie de securitate cibernetică sunt în plină expansiune. Cu toate acestea, ele sunt dispersate și, până în prezent, nu au reușit să atingă o masă critică pentru a determina o schimbare reală.

---

[15] Potrivit Organizației Europene de Securitate Cibernetică (ECSO), astfel cum se menționează în Comunicarea comună către Parlamentul European și Consiliu - Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.

[16] (ISC²) în Evaluarea competențelor cibernetice pe baza ECSF, webinarul ENISA, 16 februarie 2023.

[17] Baza de date privind învățământul superior în domeniul securității cibernetice (CyberHEAD).

[18] Doar 19 % dintre specialiștii în TIC din UE sunt femei Indicele economiei și societății digitale (DESI) 2022 | Conturarea viitorului digital al Europei (europa.eu). Nu este disponibil niciun număr în ceea ce privește forța de muncă din rândul femeilor în domeniul securității cibernetice din Uniune.

[19] Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital, care instituie un mecanism de monitorizare și cooperare în vederea atingerii obiectivelor și țintelor comune pentru transformarea digitală a Europei stabilite în Busola pentru dimensiunea digitală 2030, inclusiv în domeniul competențelor.

[20] Raportul S-RM privind informațiile în materie de securitate cibernetică 2022.

[21] *Cybersecurity Skills Development in the EU* (Dezvoltarea competențelor în materie de securitate cibernetică în UE), ENISA, decembrie 2019.

[22] Definiția IMM-urilor (europa.eu).

[23] Raportul ENISA privind situația amenințărilor în 2022 – ENISA (europa.eu).

În primul rând, în prezent există o înțelegere comună limitată a componenței forței de muncă din UE în domeniul securității cibernetice și a competențelor asociate, întrucât profilurile profesionale similare în domeniul securității cibernetice ar trebui să implice același set de competențe. Nivelul scăzut de adoptare de către actorii relevanți a unui **cadru european comun de referință pentru profesioniștii din domeniul securității cibernetice** se traduce prin lipsa unui instrument de comunicare între angajatori, educatori și factorii de decizie, precum și prin incapacitatea de a efectua măsurători și de a evalua lacunele de pe piața forței de muncă din domeniul securității cibernetice. Aceasta împiedică, de asemenea, elaborarea unor programe de educație și formare și crearea unor parcursuri profesionale care să răspundă nevoilor de politică și de piață ale celor care doresc să exercite această profesie. **Perfecționarea și recalificarea** forței de muncă se bazează în mare măsură pe cursuri de formare și certificate în domeniul securității cibernetice, oferite de obicei de furnizori privați. Cu toate acestea, forța de muncă se confruntă cu dificultăți în a obține o imagine de ansamblu asupra calității cursurilor de formare în materie de securitate cibernetică oferite și a certificatelor aferente eliberate.

Deși educația și formarea și crearea de parcursuri profesionale sunt necesare pentru a spori oferta pe piața forței de muncă, rolul **cererii** în formarea forței sale de muncă și în adaptarea la evoluția acesteia este în prezent subestimat. Industria și angajatorii din sectorul public nu dispun de forumuri și locuri comune pentru a pune în comun ideile cu privire la cea mai bună modalitate de formare a forței de muncă și a aborda modul în care se pot **evalua mai bine** competențele, în special în timpul procesului de recrutare. **Competențele tehnice** cele mai solicitate pot fi legate de securitatea cibernetică[24], cum ar fi dezvoltarea de software sau cloud computing[25], dar **competențele transversale** sunt în continuare ignorate în mod nejustificat. Gândirea critică și analiza, soluționarea problemelor și autogestionarea sunt grupuri de competențe solicitate în mai mare măsură de angajatori[26] și sunt din ce în ce mai importante în perioada premergătoare anului 2025[27].

Există deja numeroase inițiative de investiții publice și private în competențele în materie de securitate cibernetică, UE **finanțând** pe scară largă proiecte în cadrul diferitelor instrumente[28]. Cu toate acestea, deficitul continuu de competențe în UE ridică semne de întrebare în ceea ce privește vizibilitatea și impactul acestora și sugerează că este posibil ca acestea să nu corespundă în mod sistematic nevoilor pieței, care trebuie cartografiate urgent la nivelul UE. În plus, existența mai multor surse de finanțare conduce la suprapuneri, prin urmare, nevalorificându-se posibilitatea de extindere și de creare a unui impact real. În plus, cei care au nevoie de investiții nu pot identifica întotdeauna sursele cele mai adecvate pentru nevoile lor.

Părțile interesate au încercat să soluționeze problema complexă și multidimensională a deficitului de competențe în materie de securitate cibernetică. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a elaborat instrumente legate de profilurile rolurilor

[24] LinkedIn 2023, *Most In-Demand Skills: Learn the Skills Companies Need Most* (Cele mai solicitate competențe: aflați care sunt competențele de care întreprinderile au cea mai mare nevoie).

[25] Infografic ISACA – Situația securității cibernetice 2022.

[26] Cum ar fi instrumentul Cedefop: Skills-OVATE | Cedefop (europa.eu).

[27] *The Future of Jobs Report* (Raportul privind viitorul locurilor de muncă, octombrie 2020, Forumul Economic Mondial).

[28] De exemplu: Alianța competențelor în materie de securitate cibernetică – O nouă viziune pentru Europa – proiect REWIRE (finanțat de programul Erasmus+); proiecte de sprijinire a Centrului de competențe în materie de securitate cibernetică [ECHO, CONCORDIA, CyberSec4Europe, SPARTA (finanțat prin programul Orizont 2020), proiectul Cybersecpro (finanțat prin programul „Europa digitală")].

sau de învățământul superior[29], Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC)[30] abordează competențele în materie de securitate cibernetică în cadrul unui grup de lucru specific, Colegiul European de Securitate și Apărare (CESA) lucrează la dezvoltarea competențelor în materie de securitate cibernetică ale forței de muncă civile și militare în contextul politicii de securitate și apărare comune[31], organizațiile private încearcă să abordeze această problemă[32], iar sectorul certificării securității cibernetice elaborează o foaie de parcurs și cursuri de formare care vizează deficitele în materie de competențe[33]. Statele membre încearcă, de asemenea, să soluționeze această problemă printr-o varietate de inițiative, de la cele cu caracter normativ[34] până la crearea de academii de competențe în materie de securitate cibernetică[35] sau de campusuri cibernetice[36] și centre de excelență pentru combaterea criminalității informatice[37], sau prin parteneriate public-privat[38]. Cu toate acestea, activitatea tuturor acestor părți interesate este adesea lipsită de coordonare și sinergii și nu și-a atins potențialul de a determina o schimbare substanțială pe piața forței de muncă, după cum o demonstrează deficitul tot mai mare de forță de muncă din domeniul securității cibernetice din UE. Intensificarea sinergiilor între comunitățile cibernetice este, de asemenea, necesară, întrucât seturile de competențe necesare pentru a susține securitatea cibernetică, a combate **criminalitatea informatică** sau a construi răspunsuri în materie de **apărare cibernetică** sunt adesea de natură similară.

În cele din urmă, în prezent, UE dispune de mijloace limitate de evaluare a **situației și a evoluției pieței forței de muncă din domeniul securității cibernetice**, precum și a competențelor forței sale de muncă. Statele membre și instituțiile, organele, oficiile și agențiile se bazează fie pe date colectate de entități private, fie pe un set mai larg de date colectate la nivelul UE, în special de Eurostat[39] și de Centrul European pentru Dezvoltarea Formării Profesionale (Cedefop)[40], privind profesioniștii din domeniul TIC. Cu alte cuvinte, UE are o viziune parțială și fragmentată asupra nevoilor sale, ceea ce o împiedică să consolideze o viziune agregată asupra situației pieței forței de muncă din domeniul securității cibernetice.

3. Un răspuns coordonat la nivelul UE: Academia de competențe în materie de securitate cibernetică

[29]În special: Cadrul european de competențe în materie de securitate cibernetică (ECSF); CYBERHEAD – Baza de date privind învățământul superior în domeniul securității cibernetice; Platforma de exerciții de securitate cibernetică (CEP); Concursul european de securitate cibernetică; Luna europeană a securității cibernetice.

[30]Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare.

[31]În special, platforma de educație, formare, evaluare și exerciții în domeniul cibernetic (EFEE).

[32]De exemplu, Grupul de lucru 5 al Organizației Europene de Securitate Cibernetică (ECSO) privind „Educația, formarea, sensibilizarea, poligoanele cibernetice, factorii umani”. Organizația DIGITALEUROPE.

[33]De exemplu, Institutul SANS, (ISC)², ISACA.

[34]De exemplu, în strategiile naționale pentru educație sau securitate cibernetică.

[35]De exemplu, C-Academy din Portugalia.

[36]De exemplu, *Campus Cyber* (campusuri cibernetice) din Franța.

[37]De exemplu, Centrul lituanian de excelență pentru formare, cercetare și educație în domeniul criminalității informatice, Lituania (L3CE).

[38]De exemplu, Inițiativa Microsoft privind calificarea în materie de securitate cibernetică.

[39]Specialiștii TIC și ocuparea forței de muncă – Statistici explicate (europa.eu).

[40]Cum ar fi instrumentul Cedefop: Skills-OVATE | Cedefop (europa.eu).

3.1. Obiectiv

Pentru a răspunde provocării reprezentate de abordarea competențelor în materie de securitate cibernetică și de eliminarea lacunelor de pe piața forței de muncă, Comisia propune înființarea unei **Academii de competențe în materie de securitate cibernetică**, astfel cum a anunțat președinta Comisiei Europene în scrisoarea sa de intenție din 2022 privind starea Uniunii[41, 42] și în contextul Anului european al competențelor.

Academia de competențe în materie de securitate cibernetică (pe scurt, „academia") urmărește să creeze un **ghișeu unic și sinergii** pentru ofertele de educație și formare în materie de securitate cibernetică, precum și pentru oportunități de finanțare și acțiuni specifice de sprijinire a dezvoltării competențelor în materie de securitate cibernetică. Aceasta va intensifica inițiativele părților interesate pentru a atinge o masă critică ce va determina o schimbare pe piața forței de muncă, inclusiv în domeniul apărării. Aceste activități ar urma să se alinieze la obiectivele comune și la indicatorii-cheie de performanță pentru a urmări un impact mai mare.

Academia se va axa pe calificarea **profesioniștilor din domeniul securității cibernetice**. Activitatea academiei va contribui la politicile UE privind securitatea cibernetică, dar și la educație și la învățarea pe tot parcursul vieții. Aceasta completează cele două recomandări ale Consiliului referitoare la educația și competențele digitale propuse de Comisie în același timp cu prezenta comunicare[43].

Academia se va baza pe patru piloni: (1) promovarea **generării de cunoștințe prin educație și formare** prin elaborarea unui cadru comun pentru profilurile rolurilor în materie de securitate cibernetică și competențele asociate, îmbunătățirea ofertei europene de programe de educație și formare pentru a răspunde nevoilor, crearea de parcursuri profesionale și asigurarea vizibilității și a clarității în ceea ce privește formările și certificările în materie de securitate cibernetică pentru a spori oferta de forță de muncă; (2) asigurarea unei mai bune direcționări și vizibilități a **oportunităților de finanțare** disponibile pentru activitățile legate de competențe, pentru a maximiza impactul acestora; (3) invitarea părților interesate **să ia măsuri**; și (4) definirea indicatorilor pentru **monitorizarea evoluției pieței** și pentru a se asigura capacitatea de evaluare a eficacității acțiunilor acestora.

Înființarea academiei va fi sprijinită printr-o finanțare în valoare de 10 milioane EUR din cadrul programului „Europa digitală" (DEP)[44].

3.2. Guvernanța academiei

În cele din urmă, pentru a oferi o infrastructură care să servească drept **ghișeu unic** care să încurajeze cooperarea între mediul academic, furnizorii de formare și industrie, în cadrul

[41] Scrisoarea de intenție din 2022 privind starea Uniunii Europene adresată președintei Roberta Metsola și prim-ministrului Petr Fiala.

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

[43] Propuneri de recomandări ale Consiliului privind factorii favorizanți esențiali pentru succesul educației și formării digitale și privind îmbunătățirea ofertei de competențe digitale în educație și formare.

[44] Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a programului „Europa digitală" și de abrogare a Deciziei (UE) 2015/2240.

căruia oferta și cererea din ecosistemul securității cibernetice al UE s-ar putea reuni și ar putea beneficia de instruire, academia ar putea lua forma unui **consorțiu pentru o infrastructură digitală europeană (EDIC)**[45]. Acest instrument ar permite statelor membre să colaboreze în vederea eliminării deficitului de competențe în materie de securitate cibernetică, precum și să coopereze îndeaproape cu Comisia, ENISA și Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (ECCC), în conformitate cu mandatele și competențele lor, și să reunească toate părțile interesate relevante, dar și investițiile europene, naționale și private, în vederea îndeplinirii unui obiectiv comun. În acest scop, statele membre interesate sunt încurajate să transmită Comisiei până la 30 mai 2023 o notificare prealabilă cu privire la viitoarea lor cerere privind un astfel de EDIC. Această notificare prealabilă voluntară ar permite Comisiei să emită observații timpurii cu privire la proiectul de cerere privind EDIC, permițând astfel dezvoltarea acesteia și accelerarea transmiterii oficiale. Pe parcursul întregului proces și în măsura solicitată de statele membre, Comisia, acționând ca accelerator de proiecte multinaționale, va facilita pregătirea cererii privind EDIC. Apoi, în urma unei evaluări pozitive a cererii de către Comisie și a aprobării de către Comitetul pentru programul privind „Deceniul digital", Comisia ar emite o decizie de instituire a EDIC și, ulterior, ar contribui la coordonarea punerii în aplicare a EDIC[46].

Între timp și concomitent cu instituirea oficială a EDIC, Comisia va crea un ghișeu unic virtual prin îmbunătățirea **Platformei Comisiei pentru competențe și locuri de muncă în sectorul digital**[47]**,** cu ajutorul proiectului de sprijin al Comunității Europene a Securității Cibernetice (ECCO)[48].

ENISA va contribui la punerea în aplicare a academiei în conformitate cu obiectivele agenției[49], în special în ceea ce privește asistența în domeniul educației și formării în materie de securitate cibernetică, și ținând seama de obligațiile sale de raportare în temeiul Directivei NIS2[50]. **ECCC** va acționa în conformitate cu agenda sa strategică pentru a sprijini punerea în aplicare a Academiei de competențe în materie de securitate cibernetică. În special, ECCC va pune în aplicare obiectivul strategic 3 (Securitate cibernetică) al programului „Europa digitală". Acesta va beneficia de sprijinul Comisiei și al statelor membre, prin intermediul **centrelor naționale de coordonare (CNC-uri)**. **Sprijinul Grupului de cooperare** instituit

[45] Consorțiile pentru o infrastructură digitală europeană au fost instituite prin Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital, articolul 13 și următoarele.

[46] ibidem, articolul 12.

[47] Pagina principală |Platforma pentru competențe și locuri de muncă în sectorul digital (europa.eu).

[48] A se vedea Centrul și rețeaua europeană de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică: un nou proiect finanțat de UE pentru sprijinirea comunității cibernetice (europa.eu). În decembrie 2022, Comisia Europeană a semnat un contract în valoare de 3 milioane EUR pentru a sprijini comunitatea cibernetică din UE în contextul Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică. Acest proiect va contribui la îndeplinirea obiectivelor UE privind comunitatea și consolidarea capacităților în ceea ce privește cercetarea, inovarea, adoptarea și baza industrială în materie de securitate cibernetică.

[49] „ENISA sprijină consolidarea capacităților și procesul de pregătire în întreaga Uniune, furnizând asistență instituțiilor, organelor, oficiilor și agențiilor Uniunii, precum și statelor membre și părților interesate din sectorul public și privat [...] pentru a dezvolta aptitudini și competențe în domeniul securității cibernetice." Articolul 4 alineatul (3) din Regulamentul privind securitatea cibernetică.

[50] Articolul 18 din Directiva NIS2.

în temeiul Directivei NIS2[51] va fi solicitat, după caz. În cele din urmă, va fi necesară unirea forțelor cu **industria** și cu **mediul academic** pentru atingerea obiectivului academiei de a elimina deficitul de competențe în materie de securitate cibernetică.

4. Generarea de cunoștințe și formarea: stabilirea unei abordări comune la nivelul UE în ceea ce privește formarea în materie de securitate cibernetică

În cadrul pilonului privind generarea de cunoștințe și formarea al Academiei de competențe în materie de securitate cibernetică, va fi elaborată o abordare structurată, cu obiectivul clar de a crește **numărul** de persoane cu competențe în materie de securitate cibernetică în UE, de a direcționa mai bine cursurile de formare către **nevoile pieței** și de a oferi vizibilitate asupra **parcursurilor profesionale**.

4.1. Un limbaj comun: o abordare comună privind profilurile rolurilor în domeniul securității cibernetice și competențele asociate

ENISA depune deja eforturi în vederea definirii profilurilor rolurilor profesioniștilor din domeniul securității cibernetice în temeiul Cadrului european de competențe în materie de securitate cibernetică (**ECSF**)[52]. Aceasta ar trebui să devină baza pe care academia o va folosi pentru a defini și a evalua competențele relevante, a monitoriza evoluția deficitului de competențe și a oferi indicații cu privire la noile nevoi. Pentru fiecare rol din domeniul securității cibernetice al ECSF, este încorporat un set de cadre europene aplicabile privind competențele electronice[53] ca element al descrierii profilului[54].

Prin urmare, ENISA va revizui ECSF și va **identifica nevoile și deficitele de competențe în continuă evoluție** în ceea ce privește forța de muncă din domeniul securității cibernetice, inclusiv prin instrumente avansate (de exemplu, inteligența artificială, volumele mari de date[55], extragerea datelor). În acest scop, ENISA va lucra sub conducerea EDIC, atunci când va fi înființat, a ECCC, împreună cu CNC-urile, Comisia, proiectul ECCO și actorii de pe piață[56]. În ceea ce privește forța de muncă din domeniul apărării cibernetice, ENISA va ține seama în mod corespunzător de activitatea desfășurată de CESA. În mod similar, în domeniul combaterii criminalității informatice, ENISA va lua în considerare activitățile desfășurate de Agenția UE pentru Formare în Materie de Aplicare a Legii (CEPOL) și Europol în ceea ce

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

[52] Cadrul european de competențe în materie de securitate cibernetică (ECSF) – ENISA (europa.eu) ECSF sprijină identificarea și articularea sarcinilor, a competențelor, a aptitudinilor și a cunoștințelor asociate rolurilor profesioniștilor europeni în domeniul securității cibernetice. Acesta sintetizează toate rolurile din domeniul securității cibernetice în profiluri, care sunt analizate individual în mod detaliat în ceea ce privește responsabilitățile, competențele, sinergiile și interdependențele lor corespunzătoare.

[53] Cadrul european de competențe electronice (e-CF) |Esco (europa.eu) e-CF oferă legături coerente în contextul calificărilor TIC și al altor cadre relevante pentru sector, printre care DigComp.

[54] A se vedea, în acest sens, Manualul utilizatorului – Cadrul european de competențe în materie de securitate cibernetică (ECSF) – septembrie 2022.

[55] A se vedea, de exemplu, Skills-OVATE, elaborat de Cedefop.

[56] Agenția va valorifica în continuare rezultatele altor proiecte finanțate de UE [de exemplu, REWIRE, *Data Space for Skills* (DS4S), CyberSecPro, Concordia] și metodologiile derivate din inițiative similare (de exemplu, „Crearea unei forțe de muncă în domeniul securității cibernetice în cinci țări: Perspective din partea Australiei, Canadei, Noii Zeelande, Regatului Unit și Statelor Unite”, raportul OCDE, lansat la 21 martie 2023) pentru a asigura în viitor o viziune actualizată asupra nevoilor într-un mediu în care cererea evoluează constant.

privește stabilirea unei analize a nevoilor de formare operațională[57] privind atacurile cibernetice.

ECSF va fi completat și revizuit periodic în cadrul academiei pe parcursul unui ciclu bianual. În plus, Comisia și Serviciul European de Acțiune Externă vor contribui la definirea profilurilor specifice și a competențelor asociate pentru sectoare, după caz, cu sprijinul agențiilor și organismelor UE, cum ar fi CESA[58], Europol și CEPOL[59].

De asemenea, se vor stabili legături între ECSF și instrumentele relevante ale politicii UE în domeniul ocupării forței de muncă[60]. În special profilurile profesionale ale ECSF, precum și competențele conexe vor fi integrate în **clasificarea europeană a aptitudinilor, competențelor, calificărilor și ocupațiilor (ESCO)**. Acest lucru va îmbunătăți clasificarea și legăturile dintre ocupații și competențe în domeniul securității cibernetice, facilitând perfecționarea și recalificarea persoanelor și sprijinind corelarea cererii și a ofertei de locuri de muncă bazate pe competențe și mobilitatea transfrontalieră.

4.2.Încurajarea cooperării în vederea conceperii programelor de educație și formare în materie de securitate cibernetică

După înființarea EDIC, academia ar trebui să primească sprijin din partea statelor membre pentru a deveni **locul de referință în Europa pentru conceperea și furnizarea de cursuri de formare în materie de securitate cibernetică** care să abordeze competențele cele mai solicitate și să ofere cursuri de formare la locul de muncă și oportunități de stagii de practică pentru întreprinderile nou-înființate și IMM-uri și pentru administrațiile publice, în întreprinderi inovatoare din sectorul securității cibernetice și centre de competență în materie de securitate cibernetică. EDIC ar trebui să colaboreze cu toate părțile interesate relevante, inclusiv cu industria, pentru a concepe astfel de cursuri de formare și să se bazeze pe proiecte precum **CyberSecPro**[61], finanțat prin programul „Europa digitală”, care reunește 17 instituții de învățământ superior și 13 societăți din sectorul securității din 16 state membre, pentru ca aceasta să devină cea mai bună practică pentru toate programele de formare în materie de securitate cibernetică.

Academia va colabora cu toate părțile interesate relevante pentru a **atrage generația tânără** să urmeze cariere în domeniul securității cibernetice. În conformitate cu propunerea de recomandare a Consiliului privind îmbunătățirea ofertei de competențe digitale în educație și formare, statele membre ar trebui să instituie și să consolideze măsuri de recrutare și formare a profesorilor și formatorilor specializați și de facilitare a dobândirii de competențe în materie de securitate cibernetică, inclusiv prin stagii de ucenicie. Ar trebui să se încurajeze integrarea

[57] CEPOL Evaluarea nevoilor de formare operațională (OTNA).

[58] A se vedea în acest sens Comunicarea comună către Parlamentul European și Consiliu - Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.

[59] În acest sens, se va acorda atenție lucrărilor privind Cadrul de competențe pentru formarea în domeniul criminalității informatice (CCF), aflat în prezent în curs de elaborare.

[60] Cum ar fi Clasificarea europeană a aptitudinilor, competențelor, calificărilor și ocupațiilor (ESCO), Europass, rețeaua de servicii europene pentru ocuparea forței de muncă (EURES).

[61] CyberSecPro Va efectua, de exemplu, o analiză a programelor de securitate cibernetică, a cursurilor și a școlilor de vară oferite în universități și a tabelelor de clasificare ale Sistemului european de acumulare și transfer al creditelor de studii (ECTS) utilizate, va asigura implicarea numărului țintă de peste 530 de stagiari în perioada de 3 ani, va forma personal extern din diferite sectoare și domenii.

securității cibernetice în programele de educație și formare, asigurând în același timp accesibilitatea acestora, dezvoltând oferta de **ucenicii** și stagii, promovând abordări inovatoare, inclusiv, de exemplu, jocuri serioase și platforme de simulare comune, organizând săptămâni de familiarizare cu posturile din domeniul securității cibernetice și explicând profilurile rolurilor fără caracter tehnic. De asemenea, ar trebui sprijinită participarea la aceste oportunități de învățare în materie de securitate cibernetică a grupurilor greu accesibile, cum ar fi tinerii cu handicap, cei care locuiesc în zone îndepărtate sau rurale și cei care aparțin altor grupuri minoritare.

Comisia va continua să ofere sprijin pentru dezvoltarea microcertificărilor și a programelor de educație și formare profesională. În special, **programele comune de licență și de masterat, cursurile sau modulele comune care pot conduce la microcertificări** și **programele intensive mixte**[62] pe toate temele, inclusiv **privind securitatea cibernetică**, vor continua să fie finanțate în cadrul programului Erasmus+. Continuarea implementării **inițiativei privind universitățile europene**[63] și a **centrelor de excelență profesională**[64] va fi, de asemenea, sprijinită pentru a încuraja o mai bună cooperare între învățământul superior și instituțiile relevante de educație și formare profesională din întreaga Europă. Programele de finanțare ale UE, inclusiv Erasmus+ și programul „Europa digitală", precum și fondurile UE pentru dezvoltarea **conturilor personale de învățare pe tot parcursul vieții**[65] vor sprijini acest obiectiv de cooperare mai strânsă.

Pentru a facilita cooperarea la nivel național între mediul academic și furnizorii de cursuri de formare în materie de competențe în domeniul securității cibernetice cu angajatorii din sectorul privat și din sectorul public și pentru a promova sinergiile dintre sectorul public și cel privat, centrele naționale de coordonare sunt invitate să exploreze posibilitatea de creare a unor **campusuri cibernetice** în statele membre. Campusurile cibernetice ar avea ca scop asigurarea unor poli de excelență la nivel național pentru comunitatea de securitate cibernetică, iar academia ar contribui la crearea de rețele și la coordonarea pe mai departe a activităților acestora.

ENISA își va îmbunătăți, de asemenea, oferta de formare în materie de securitate cibernetică, aliniindu-și **catalogul de cursuri**[66] la profilurile ECSF și elaborând module de formare pentru fiecare profil, ceea ce ar putea contribui la îmbunătățirea ofertelor de formare ale statelor membre. De asemenea, ENISA își va extinde **programul de „formare a formatorilor"**[67], vizând nevoile profesionale ale instituțiilor, organelor, oficiilor și agențiilor, ale autorităților publice și ale **operatorilor publici și privați esențiali** din statele membre în domeniul de aplicare al Directivei NIS2.

În plus, alte agenții și organisme ale UE își vor consolida oferta de formare în materie de securitate cibernetică. De exemplu, prin punerea în aplicare a politicii UE în materie de apărare cibernetică, **CESA** va elabora un nou set de cursuri de securitate cibernetică și va alinia unele dintre cursurile sale actuale la ECSF. Aceste cursuri vor conduce la certificarea

[62]Programele intensive mixte combină predarea online cu o perioadă scurtă de mobilitate fizică.

[63]Inițiativa privind universitățile europene |Spațiul european al educației (europa.eu).

[64]Centre de excelență profesională | Erasmus+ (europa.eu).

[65]În conformitate cu Recomandarea Consiliului din 16 iunie 2022 privind conturile personale de învățare.

[66]Cursuri de formare – ENISA (europa.eu).

[67]Programul de formare a formatorilor – ENISA (europa.eu).

rezultatelor învățării[68]. CESA, în colaborare cu Comisia, va analiza posibilitatea integrării certificatelor în portofelul EUeID. CESA va analiza în continuare posibila evaluare a mecanismelor de competențe, pe baza cărora vor fi eliberate certificatele. În mod similar, în domeniul combaterii criminalității informatice, se va avea în vedere crearea de legături strânse cu **Academia de combatere a criminalității informatice a CEPOL**[69] pentru a promova sinergiile și complementaritățile în elaborarea și punerea în aplicare a programelor de formare.

4.3. Crearea de sinergii și asigurarea vizibilității cursurilor de formare și a certificării în materie de securitate cibernetică în toate statele membre

Academia ar trebui să abordeze problema vizibilității și a sinergiilor formării și certificării. Acest lucru ar aduce beneficii comunităților cibernetice din domeniul civil, al apărării, al aplicării legii și diplomatic, întrucât toate sectoarele necesită, în multe cazuri, aceleași calificări, pe baza unor programe de învățământ și a unor rezultate ale învățării similare.

Academia ar oferi un **ghișeu unic** pentru cei interesați de o carieră în domeniul securității cibernetice. Pe termen scurt, acest lucru se va realiza prin consolidarea **Platformei Comisiei pentru competențe și locuri de muncă în sectorul digital**, cu sprijinul proiectului ECCO. O secțiune specifică privind carierele în domeniul securității cibernetice se va corela cu instrumentele existente, de la programele de învățământ superior la oportunitățile de formare, inclusiv cursurile care conduc la microcertificări și programele de educație și formare profesională, până la ofertele de locuri de muncă. Acest lucru se va realiza prin recomandarea activităților și inițiativelor în desfășurare sau prin integrarea acestora în platformă, cum ar fi cele ale ENISA, care, în colaborare cu mediul academic, a realizat o **cartografiere a instituțiilor de învățământ** care furnizează programe de securitate cibernetică. Această activitate va fi consolidată și mai mult cu sprijinul centrelor naționale de coordonare. În plus, ENISA va elabora și va consolida două **registre de cursuri de formare existente din sectoarele public și privat și de certificări în materie de securitate cibernetică**, cu sprijinul centrelor naționale de coordonare, al Comisiei și al proiectului ECCO, în colaborare cu entitățile care furnizează certificări și care se bazează, de asemenea, pe alte inițiative relevante[70]. Acestea vor fi, de asemenea, integrate în ghișeul unic al Platformei pentru competențe și locuri de muncă în sectorul digital. Această activitate va aduce, de asemenea, beneficii centrelor naționale de coordonare, a căror sarcină este în special de a promova și disemina programe educaționale în materie de securitate cibernetică[71].

Este totodată necesar să se ofere asigurări profesioniștilor că cursurile de formare pe care le urmează au calitatea corespunzătoare. În acest sens, ENISA va elabora un **proiect-pilot** care

---

[68] În conformitate cu articolul 20 alineatul (4) din Decizia (PESC) 2020/1515 a Consiliului din 19 octombrie 2020 de instituire a Colegiului European de Securitate și Apărare și de abrogare a Deciziei (PESC) 2016/2382.

[69] Academia de combatere a criminalității informatice a CEPOL a fost înființată în 2019 pentru a oferi o platformă de ultimă generație pentru îmbunătățirea cunoștințelor în materie de criminalitate informatică și a capacităților cibernetice în Europa.

[70] De exemplu, Academia W4C – Women4Cyber sau proiectul mondial de certificare în domeniul criminalității informatice destinat autorităților de aplicare a legii și autorităților judiciare.

[71] „1. Centrele naționale de coordonare au următoarele sarcini: [...] (g) fără a aduce atingere competențelor statelor membre în materie de educație și ținând seama de sarcinile relevante ale ENISA, cooperarea cu autoritățile naționale în ceea ce privește posibilele contribuții la promovarea și diseminarea programelor educaționale în materie de securitate cibernetică”, articolul 7 alineatul (1) litera (g) din Regulamentul privind ECCC. A se vedea, de asemenea, considerentul 28 asociat.

va explora oportunitatea instituirii unui sistem european de atestare pentru competențele în materie de securitate cibernetică.

În plus, identificarea competențelor și a formării și asocierea acestora cu un profil profesional sunt esențiale, dar este, de asemenea, important să se asigure că serviciile de securitate cibernetică dispun de competențele, calificările și experiența necesare. Acest lucru este valabil în special pentru furnizorii de servicii de securitate gestionate în domenii precum răspunsul la incidente, testele de penetrare cibernetică, auditurile și consultanța în materie de securitate. Directiva NIS2 și propunerea de Act privind solidaritatea cibernetică stabilesc sarcini specifice pentru astfel de furnizori de servicii de securitate gestionate. Prin urmare, Comisia propune, de asemenea, o **modificare specifică a Regulamentului privind securitatea cibernetică**[72] pentru a permite sistemele de certificare a serviciilor de securitate gestionate la nivelul UE. Aceste sisteme de certificare ar trebui să vizeze, printre altele, asigurarea faptului că aceste servicii sunt furnizate de personal cu un nivel foarte ridicat de cunoștințe și competențe tehnice în domeniile relevante.

Mecanismele de asigurare a calității și de recunoaștere a microcertificării[73] facilitează transparența, comparabilitatea și portabilitatea rezultatelor învățării. În conformitate cu Recomandarea Consiliului privind o abordare europeană a microcertificatelor[74], statele membre sunt încurajate să includă microcertificarea în materie de securitate cibernetică în cadrele lor naționale de calificare. Acest lucru le-ar permite să coreleze microcertificarea în materie de securitate cibernetică cu Cadrul european al calificărilor[75]. Infrastructura europeană de acreditări digitale pentru învățare este disponibilă pentru a emite calificări și microcertificări în materie de securitate cibernetică semnate digital pentru persoane fizice. Acestea conțin o multitudine de date, inclusiv privind rezultatele învățării în materie de securitate cibernetică, și pot fi stocate în viitorul **portofel digital EUeID**[76].

Acțiuni în cadrul academiei

Statele membre și industria

- Asigurarea sprijinului pentru dezvoltarea și recunoașterea **microcertificărilor** pentru învățare în materie de securitate cibernetică, în conformitate cu Recomandarea Consiliului privind o abordare europeană a microcertificatelor.
- Includerea calificărilor în materie de securitate cibernetică, inclusiv a microcertificărilor, în **cadrele naționale ale calificărilor.**
- Oferirea de **oportunități de formare la locul de muncă** prin ucenicii pentru persoanele

[72] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică).

[73] De exemplu, înregistrarea rezultatelor învățării sau certificatele care atestă aceste rezultate pe care persoanele le obțin în urma unor cursuri de formare la scară mică.

[74] Recomandarea Consiliului privind o abordare europeană a microcertificatelor pentru învățarea pe tot parcursul vieții și capacitatea de inserție profesională.

[75] Recomandarea Consiliului din 22 mai 2017 privind Cadrul european al calificărilor pentru învățarea pe tot parcursul vieții și de abrogare a Recomandării Parlamentului European și a Consiliului din 23 aprilie 2008 privind stabilirea Cadrului european al calificărilor pentru învățarea de-a lungul vieții.

[76] Propunere de Regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană.

care participă la inițiative de dezvoltare a competențelor în materie de securitate cibernetică.

Comisia

- Pe termen scurt, crearea **unui ghișeu unic** pentru programele de securitate cibernetică, cursurile de formare existente și pentru certificările de securitate cibernetică prin intermediul **Platformei pentru competențe și locuri de muncă în sectorul digital** până la sfârșitul anului 2023.
- Propunerea, la 18 aprilie 2023, a unei modificări a **Regulamentului privind securitatea cibernetică** pentru a permite certificarea furnizorilor de servicii de securitate gestionate.

Organismele și agențiile UE

- Instituirea, până la sfârșitul anului 2023, a **ECSF** ca abordare comună privind profilurile rolurilor în domeniul securității cibernetice și competențele asociate.
- Inițierea de către ENISA a elaborării unui proiect-pilot de instituire a unui **sistem european de atestare** pentru competențele în materie de securitate cibernetică în T2 2023.
- Revizuirea de către ENISA a **catalogului său de cursuri** și deschiderea **programului său de „formare a formatorilor"** pentru operatorii publici și privați critici până la sfârșitul anului 2023.
- Finalizarea **alinierii programei de învățământ a CESA la ECSF** până la jumătatea anului 2023.

5. Implicarea părților interesate: angajamentul de a elimina deficitul de competențe în materie de securitate cibernetică.

În cadrul academiei, va fi elaborată o abordare coordonată a implicării părților interesate pentru a aborda deficitul de competențe în materie de securitate cibernetică. Scopul va fi de a maximiza vizibilitatea și impactul diferitelor angajamente ale părților interesate care vizează reducerea deficitului de competențe în materie de securitate cibernetică.

Comisia invită părțile interesate să își asume angajamente concrete privind perfecționarea și recalificarea lucrătorilor prin acțiuni specifice, raportându-se cât mai mult posibil la deficitul de competențe identificat în materie de securitate cibernetică. Astfel de **angajamente în materie de securitate cibernetică ale părților interesate** ar trebui să fie raportate pe **Platforma pentru competențe și locuri de muncă în sectorul digital**, la fel ca alte angajamente digitale deja vizibile pe platformă. Comisia încurajează, de asemenea, părțile interesate care își asumă un angajament în materie de securitate cibernetică pe platformă să se alăture **parteneriatului la scară largă pentru competențe în ecosistemul digital din cadrul Pactului privind competențele**[77]. Se încurajează transmiterea angajamentelor în materie de securitate cibernetică asumate în cadrul parteneriatului la scară largă pentru competențe în ecosistemul digital prin Platforma pentru competențe și locuri de muncă în sectorul digital. De asemenea, se încurajează raportarea angajamentelor asumate prin

[77] Noi parteneriate europene lansate pentru a îndeplini obiectivele ambițioase ale UE pentru deceniul digital | Conturarea viitorului digital al Europei (europa.eu), creat în cadrul Pactului privind competențele pentru a aborda deficitul în materie de tehnologie a informației și comunicațiilor (TIC).

Platforma pentru competențe și locuri de muncă în sectorul digital în cadrul parteneriatului la scară largă pentru competențe în ecosistemul digital.

De asemenea, Comisia invită statele membre să își **continue eforturile de punere în aplicare a Declarației de angajament privind femeile în sectorul digital**[78] pentru a încuraja femeile să joace un rol activ și proeminent în sectorul tehnologiei digitale și să realizeze convergența de gen la nivelul posturilor din domeniul securității cibernetice. De asemenea, Comisia încurajează statele membre să dezvolte sinergii cu programele lor din cadrul **Fondului social european+** (FSE+) pentru a sprijini mai mult obiectivul egalității de gen în ceea ce privește participarea pe piața muncii[79], de exemplu prin instituirea de programe de **mentorat pentru fete și femei.** Acestea pot facilita crearea unor modele de urmat pentru a atrage fetele către profesiile din domeniul securității cibernetice, combătând în același timp stereotipurile legate de gen. De asemenea, încurajează perfecționarea și recalificarea femeilor, precum și dezvoltarea unei comunități care să poată sprijini intrarea sau promovarea femeilor pe piața forței de muncă din domeniul securității cibernetice.

Ca parte a **strategiilor lor naționale în materie de securitate cibernetică, statele membre ar trebui să adopte măsuri specifice pentru a reduce deficitul de competențe în materie de securitate cibernetică**[80], a identifica și a canaliza mai bine eforturile de eliminare a deficitului de competențe și, în cele din urmă, pentru a asigura o punere în aplicare corespunzătoare a obligațiilor care le revin în temeiul Directivei NIS2.

Unele state membre utilizează **sinergiile dintre inițiativele din domeniul civil, al apărării și al aplicării legii.** De exemplu, creșterea forței de muncă ce utilizează serviciul militar național obligatoriu sau utilizarea rezerviștilor din domeniul cibernetic, care sunt cetățeni cu pregătire militară ce ocupă posturi în domeniul securității cibernetice în cadrul forțelor armate[81], permit populației, în special tinerilor adulți, să își sporească competențele în materie de securitate cibernetică și apărare cibernetică. Același lucru este valabil și în domeniul **combaterii criminalității informatice**, întrucât există multe asemănări între eforturile generale în materie de securitate cibernetică și activitățile de asigurare a respectării legii în ceea ce privește răspunsul la incidentele de securitate cibernetică. Comisia încurajează discuțiile dintre statele membre cu privire la astfel de inițiative și le invită să evalueze modul în care o forță de muncă calificată poate servi cel mai bine atât comunităților din domeniul apărării, cât și celor civile din domeniul securității cibernetice.

Comisia va reflecta asupra propunerilor privind modul de eliminare a lacunelor actuale și anticipate identificate în analiza sa privind nevoile instituțiilor, organelor, oficiilor și agențiilor. În special, aceasta va încuraja personalul să beneficieze de viitoarea **bursă UE-Statele Unite (SUA) în materie de securitate cibernetică** instituită în cadrul dialogului UE-SUA.

Acțiuni în cadrul academiei

[78] Țările UE se angajează să stimuleze participarea femeilor în domeniul digital | Conturarea viitorului digital al Europei (europa.eu).

[79] Regulamentul (UE) 2021/1057 al Parlamentului European și al Consiliului din 24 iunie 2021 de instituire a Fondului social european Plus (FSE+) și de abrogare a Regulamentului (UE) nr. 1296/2013, articolul 4 alineatul (1) litera (c).

[80] Directiva NIS2, articolul 7 alineatul (2) litera (f).

[81] Raport – Încorporarea cibernetică: experiența și bunele practici din țările selectate, Martin Hurt și Tiia Sõmer, Centrul Internațional pentru Apărare și Securitate, februarie 2021.

Industria

- Propunerea de **angajamente specifice în materie de securitate cibernetică** pe Platforma pentru competențe și locuri de muncă în sectorul digital începând cu 18 aprilie 2023.

Statele membre

- Includerea în **strategiile naționale de securitate cibernetică** a unor măsuri specifice pentru a aborda deficitul de competențe în materie de securitate cibernetică.

Statele membre și industria

- Punerea în aplicare a Declarației de angajament privind femeile în sectorul digital și realizarea **convergenței de gen la nivelul posturilor din domeniul securității cibernetice** până în 2030.

6. Finanțare: crearea de sinergii pentru a maximiza impactul cheltuielilor pentru dezvoltarea competențelor în materie de securitate cibernetică

În cadrul academiei, impactul investițiilor în competențele în materie de securitate cibernetică va fi maximizat prin asigurarea unui ghișeu unic, facilitând o mai bună direcționare a fondurilor către nevoile pieței și integrând utilizarea finanțării, facilitând sinergiile dintre diferitele instrumente, evitând, în același timp, duplicarea eforturilor[82].

6.1. Corelarea fondurilor cu nevoile

În cadrul academiei, ECCC, cu sprijinul Comisiei, al proiectului ECCO și al centrelor naționale de coordonare, va colecta **informații cu privire la modul în care sunt utilizate fondurile UE pentru a finanța competențele în materie de securitate cibernetică** și va evalua modul în care fondurile UE sprijină reducerea deficitului de competențe în materie de securitate cibernetică. Luând în considerare aceste informații agregate, ECCC va încerca să asigure o mai bună direcționare a fondurilor UE către nevoile identificate. Va finanța acțiuni care ar aborda cele mai presante deficite în ceea ce privește forța de muncă din domeniul securității cibernetice, inclusiv cele legate de punerea în aplicare a nevoilor de politică în materie de securitate cibernetică.

6.2. Asigurarea vizibilității fondurilor disponibile și a inițiativelor de tipul parteneriatelor pentru competențele în materie de securitate cibernetică

Pe termen scurt, **Platforma pentru competențe și locuri de muncă în sectorul digital** va deveni ghișeul unic pentru părțile interesate, unde vor fi disponibile toate informațiile privind oportunitățile de finanțare pentru competențele în materie de securitate cibernetică.

[82] Oportunități de finanțare (europa.eu) Serviciile de sprijinire a Pactului privind competențele oferă un ghișeu unic pentru informațiile privind finanțarea competențelor, inclusiv pentru ecosistemul digital. Serviciile de sprijinire a pactului oferă informații generice cu privire la instrumentele de finanțare care nu vizează în mod specific competențele în materie de securitate cibernetică; cu toate acestea, activitatea lor ar trebui să fie luată în considerare de academie pentru a se evita duplicarea eforturilor.

UE investește în oameni și în competențele acestora și utilizează parteneriate în special cu industria pentru a mobiliza acțiuni de perfecționare și recalificare prin intermediul mai multor instrumente identificate în cadrul **Agendei pentru competențe în Europa**[83], în special **Pactul privind competențele**[84] și **Planul de acțiune pentru educația digitală**[85]. **Programul „Europa digitală”** finanțează oportunități privind competențele în materie de securitate cibernetică, în special prin inițiative de proiecte multinaționale, în complementaritate clară cu sprijinul oferit de Orizont Europa pentru cercetare și soluții tehnologice inovatoare în materie de securitate cibernetică. **Fondul european de apărare**[86] finanțează cercetarea și dezvoltarea tehnologică pentru desfășurarea de operațiuni cibernetice eficiente, inclusiv cursuri de formare și exerciții[87]. **Erasmus+** va continua să sprijine astfel de inițiative, inclusiv prin programe intensive mixte și proiecte de cooperare.

Statele membre sunt încurajate să mobilizeze fondurile UE pe care le gestionează direct pentru a sprijini competențele și locurile de muncă în domeniul securității cibernetice. Fondurile politicii de coeziune, cum ar fi **Fondul european de dezvoltare regională (FEDR)** și **FSE+**, au un potențial important de sinergii în acest sens[88]. Domeniul de aplicare al acțiunilor din cadrul **Mecanismului de redresare și reziliență** (MRR)[89] și al **InvestEU**[90] include și alte complementarități esențiale în realizarea obiectivelor academiei.

Acțiuni în cadrul academiei

Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și ENISA

- Cartografierea finanțării existente din partea UE pentru competențele în materie de securitate cibernetică în funcție de nevoile pieței, evaluarea **eficacității** și identificarea **priorităților** de finanțare până la sfârșitul anului 2024

Comisia

- Crearea unui **ghișeu unic** pentru oportunitățile de finanțare a competențelor în materie de

[83] Agenda pentru competențe în Europa – Ocuparea forței de muncă, afaceri sociale și incluziune – Comisia Europeană (europa.eu).

[84] Instrumente de finanțare UE pentru perfecționare și recalificare – Ocuparea forței de muncă, afaceri sociale și incluziune – Comisia Europeană (europa.eu).

[85] Planul de acțiune pentru educația digitală 2021-2027.

[86] Regulamentul (UE) 2021/697 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a Fondului european de apărare și de abrogare a Regulamentului (UE) 2018/1092.

[87] Statele membre și-au luat angajamentul să organizeze cursuri de formare și exerciții comune, de exemplu, prin instituirea și participarea la cursuri de formare și proiecte de exerciții cibernetice în cadrul Cooperării structurate permanente (PESCO), cum ar fi Academia și centrul de inovare ale UE în domeniul cibernetic (EU CAIH) și Federațiile de medii cibernetice de simulare în scopuri de antrenament (*cyber ranges*).

[88] Regulamentul (UE) 2021/1058 articolul 3 alineatul (1) și Regulamentul (UE) 2021/1057 articolul 4 alineatul (1) litera (g).

[89] De exemplu, planul estonian de redresare și reziliență prevede investiții (10 milioane EUR) în competențele digitale, va include revizuirea cursurilor de formare disponibile pentru experții TIC, va finanța perfecționarea și conversia profesională a specialiștilor TIC în domeniul securității cibernetice și va contribui la dezvoltarea unui program-pilot de redefinire a cadrului de calificare pentru specialiștii TIC.

[90] Părțile interesate (de exemplu, furnizorii de formare și întreprinderile care doresc să își conceapă sau să își îmbunătățească activitățile de formare în materie de securitate cibernetică) se pot adresa Platformei de consiliere InvestEU, care oferă sprijin și asistență tehnică, inclusiv consolidarea capacităților, dezvoltatorilor de proiecte și entităților, și pot consulta Portalul InvestEU.

securitate cibernetică pe Platforma pentru competențe și locuri de muncă în sectorul digital până la sfârșitul anului 2023.

7. Evaluarea progreselor realizate: responsabilitate integrată

În cadrul academiei, va fi elaborată o **metodologie** care va permite **măsurarea progreselor în vederea eliminării deficitului de competențe în materie de securitate cibernetică.**

7.1. Definirea indicatorilor de securitate cibernetică pentru a monitoriza evoluția pieței forței de muncă din domeniul securității cibernetice

Indicele economiei și societății digitale (DESI) sintetizează indicatorii privind performanțele digitale ale Europei și monitorizează progresele realizate în această privință de statele membre ale UE. În cadrul Academiei de competențe în materie de securitate cibernetică, ENISA, în cooperare cu Comisia și cu Grupul de cooperare NIS[91], va elabora **indicatori**, inclusiv în materie de gen, pentru a urmări progresele înregistrate în statele membre ale UE în ceea ce privește creșterea numărului de profesioniști în domeniul securității cibernetice, consultând, de asemenea, actorii relevanți de pe piață și centrele naționale de coordonare. ENISA se va baza pe metodologia DESI[92] și se va asigura că indicatorii sunt în conformitate cu obiectivele digitale ale Europei privind profesioniștii din domeniul TIC și privind realizarea convergenței de gen în domeniul TIC. Ulterior, Comisia va depune eforturi pentru integrarea acestor indicatori în DESI**,** permițând astfel monitorizarea anuală a situației competențelor în materie de securitate cibernetică și a pieței forței de muncă în acest domeniu.

7.2. Colectarea și raportarea datelor

ENISA va colecta datele privind indicatorii cu sprijinul proiectului ECCO și al centrelor naționale de coordonare. Pe baza datelor colectate, ENISA va elabora un **raport anual** care va contribui la raportul privind deceniul digital[93], care, împreună cu DESI, va contribui în continuare la analiza și recomandările specifice fiecărei țări din cadrul **semestrului european**[94]. În plus, indicatorii privind competențele în materie de securitate cibernetică vor contribui la **raportul bienal** al ENISA privind situația securității cibernetice în UE**,** prevăzut în Directiva NIS2**,** care vizează capacitățile, sensibilizarea și igiena în materie de securitate cibernetică în întreaga UE.

7.3. Pregătirea indicatorilor-cheie de performanță (KPI) pentru securitatea cibernetică

În vederea eliminării deficitului de talente în materie de securitate cibernetică la nivel european, ENISA, în strânsă cooperare cu Comisia și cu centrele naționale de coordonare, va propune Comisiei o serie de indicatori-cheie de performanță, bazându-se pe metodologia

[91] Utilizarea și completarea metodologiei care urmează să fie elaborată de ENISA în scopul raportului bienal al agenției privind situația securității cibernetice în Uniune în temeiul articolului 18 alineatul (3) din Directiva NIS2.

[92] A se vedea Indicele economiei și societății digitale (DESI) 2022, Notă metodologică, disponibil la Indicele economiei și societății digitale (DESI) | Conturarea viitorului digital al Europei (europa.eu).

[93] Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital.

[94] Ibidem, considerentul 25.

programului de politică pentru 2030 privind deceniul digital, precum și pe experiența industriei. ENISA va ține seama în mod corespunzător de indicatorii-cheie de performanță utilizați de statele membre pentru a-și evalua strategiile naționale în materie de securitate cibernetică[95].

Acțiuni în cadrul academiei

ENISA

- Pregătirea unor **indicatori și indicatori-cheie de performanță** privind competențele în materie de securitate cibernetică până la sfârșitul anului 2023.
- **Colectarea de date** cu privire la indicatori și raportarea cu privire la aceștia, o primă colectare urmând să fie realizată până în 2025.

Comisia

- Depunerea de eforturi în vederea integrării **indicatorilor privind securitatea cibernetică în DESI** și în **raportul privind deceniul digital**.

8. Concluzie

Prezenta comunicare pune bazele unei restructurări a abordării UE în ceea ce privește stimularea competențelor în materie de securitate cibernetică pentru profesioniștii din UE. Scopul său este de a reduce deficitul de competențe în materie de securitate cibernetică și de a echipa UE cu forța de muncă necesară pentru a-i permite să răspundă unui peisaj al amenințărilor în continuă evoluție, să pună în aplicare politici ale UE care vizează protejarea UE împotriva atacurilor cibernetice, dar și să stimuleze oportunitățile de afaceri și competitivitatea. O forță de muncă calificată în domeniul securității cibernetice poate aduce beneficii comunităților din domeniul **civil, al apărării, diplomatic și al aplicării legii**, facilitând sinergiile dintre acestea.

Comisia invită statele membre și toate părțile interesate să contribuie la îndeplinirea obiectivelor ambițioase ale Academiei de competențe în materie de securitate cibernetică.

[95]Directiva NIS2, articolul 7 alineatul (4).