COMMISSIONE
EUROPEA

Strasburgo, 18.4.2023
COM(2023) 207 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza")

Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza")

1. Un'urgente necessità di ridurre i rischi affrontando la carenza e i divari di competenze in materia di cibersicurezza

La cibersicurezza non è solo parte della sicurezza dei cittadini, delle imprese e degli Stati membri, ma è anche una necessità per garantire la stabilità politica dell'UE, la stabilità delle sue democrazie e la prosperità della nostra società e delle nostre imprese. Il **panorama delle minacce** alla cibersicurezza si è evoluto notevolmente negli ultimi anni, evidenziando la preoccupante tendenza di un numero crescente di attacchi informatici che prendono di mira le infrastrutture critiche militari e civili nell'Unione. Gli autori delle minacce accrescono le loro capacità e si stanno profilando minacce nuove, ibride ed emergenti, come l'uso di bot e di tecniche basate sull'intelligenza artificiale[1]. In particolare, gli autori delle minacce ransomware arrecano abitualmente a diversi soggetti danni considerevoli, sia dal punto di vista finanziario che da quello della reputazione[2].

Un gran numero di incidenti di cibersicurezza ha interessato anche la pubblica amministrazione e i governi degli Stati membri, nonché le istituzioni, gli organi e gli organismi europei[3]. Anche i settori della finanza[4] e della sanità[5], entrambi colonne portanti della società e dell'economia, sono stati costantemente presi di mira[6]. Le tensioni geopolitiche legate alla guerra di aggressione della Russia contro l'Ucraina hanno aumentato la minaccia alla cibersicurezza[7] e hanno il potenziale di destabilizzare la nostra società. La **sicurezza** dell'UE non può essere garantita senza **il bene più prezioso dell'UE: la sua popolazione.** L'UE ha urgentemente bisogno di professionisti con le capacità e le competenze per prevenire, individuare e scoraggiare gli attacchi informatici nei confronti dell'UE, nonché per difenderla da tali attacchi e garantirne la **resilienza**.

Il divario di talenti nel settore della cibersicurezza ostacola ulteriormente la **competitività** e la **crescita** dell'Europa, che dipendono fortemente dallo sviluppo e dall'adozione di

---

[1] Relazione dell'ENISA sul panorama delle minacce 2022 — ENISA (europa.eu) (solo in EN).

[2] Europol, Valutazione della minaccia della criminalità organizzata su internet (IOCTA) 2021. Tali attori si basano sul modello del Ransomware-as-a-service. Il costo annuale per le imprese ha superato i 18,4 miliardi di EUR nel 2022 (Relazione Cybereason 2022 sul vero costo del ransomware).

[3] Cfr. ad esempio la pubblicazione congiunta di ENISA e CERT-EU, JP-23-01 - Attività sostenuta di specifici autori delle minacce, TLP:CLEAR, 15 febbraio 2023 (solo in EN).

[4] Ad esempio, in Germania il 90 % delle frodi postali segnalate dal 1º giugno 2021 al 31 maggio 2022 era costituito da phishing finanziario o dall'attacco a un'impresa del settore finanziario, e ha coinvolto più di 20 000 dispositivi infetti di 125 paesi. *The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI)*, 1° gennaio 2023.

[5] Ad esempio, in Francia sono stati registrati attacchi ransomware a strutture sanitarie pubbliche come il Centre Hospitalier Sud Francilien, durante i quali 11 GB di dati personali e medici, nonché dati relativi al personale, sono stati compromessi e pubblicati dall'autore della minaccia. *Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI)*, gennaio 2023.

[6] Relazione dell'ENISA sul panorama delle minacce 2022.

[7] Cfr. anche: CERT-UE - La guerra della Russia contro l'Ucraina: un anno di operazioni informatiche (europa.eu) (solo in EN); Operazioni informatiche russe contro l'Ucraina: dichiarazione dell'alto rappresentante a nome dell'Unione europea, 10 maggio 2022; Dichiarazione dell'alto rappresentante a nome dell'Unione europea sulle attività informatiche malevole condotte da hacker e gruppi di hacker nel contesto dell'aggressione della Russia nei confronti dell'Ucraina, 19 luglio 2022.

tecnologie digitali strategiche (ad esempio, intelligenza artificiale, 5G e cloud). Una forza lavoro qualificata nel settore della cibersicurezza è necessaria affinché l'UE possa continuare a fornire tecnologie avanzate chiave in un contesto globale.

Per prepararsi ad affrontare questo panorama di minacce in evoluzione e per promuovere la competitività dell'UE, la politica dell'UE in materia di cibersicurezza ha compiuto notevoli progressi negli ultimi anni, sfociando nell'adozione di una serie di iniziative come la strategia dell'UE in materia di cibersicurezza per il decennio digitale[8], la revisione della direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS 2)[9], la normativa settoriale dell'UE in materia di cibersicurezza[10], la politica di ciberdifesa dell'UE[11], la legge sulla ciberresilienza[12] e la normativa sulla cibersolidarietà, proposta dalla Commissione insieme alla presente comunicazione. Ma senza le persone qualificate necessarie per attuarli, questi atti legislativi non raggiungeranno i loro obiettivi. Mentre la conoscenza di base della cibersicurezza da parte della popolazione generale viene affrontata nell'ambito delle iniziative a sostegno dello sviluppo delle competenze generali necessarie per partecipare alla società[13], una forza lavoro competente è essenziale sia nel settore pubblico sia in quello privato, a livello nazionale e dell'UE, anche in seno alle organizzazioni di normazione, **per attuare i requisiti giuridici e politici in materia di cibersicurezza**.

La sicurezza e la competitività dell'UE dipendono quindi dalla presenza di una forza lavoro composta da professionisti qualificati nel campo della cibersicurezza. L'Unione europea si trova tuttavia di fronte a una carenza sostanziale di professionisti della cibersicurezza qualificati, che mette l'Unione, i suoi Stati membri, le sue imprese e i suoi cittadini a rischio di incidenti di cibersicurezza. Nel 2022 la carenza di professionisti della cibersicurezza nell'Unione europea si aggirava **tra le 260 000**[14] **e le 500 000**[15] unità, mentre, secondo le stime, il fabbisogno di forza lavoro dell'UE nel settore della cibersicurezza era pari a 883 000 professionisti[16], il che suggerisce un disallineamento tra le competenze disponibili e quelle richieste dal mercato del lavoro. La forza lavoro nel settore della cibersicurezza risente inoltre della percezione errata associata alla sua immagine tecnica e continua a non attrarre le **donne**, che rappresentano il 20 % delle persone laureate in cibersicurezza[17] e il 19 % di quelle

[8] Comunicazione congiunta al Parlamento europeo e al Consiglio – La strategia dell'UE in materia di cibersicurezza per il decennio digitale (JOIN(2020) 18 final).

[9] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[10] Come ad esempio, per il settore finanziario, il regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (regolamento DORA).

[11] Comunicazione congiunta al Parlamento europeo e al Consiglio - La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

[12] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM(2022) 454 final).

[13] Tra le iniziative pertinenti che riguardano le competenze digitali generali della popolazione figurano il piano d'azione sul pilastro europeo dei diritti sociali e la bussola per il digitale, il piano d'azione per l'istruzione digitale 2021-2027, lo strumento del quadro delle competenze digitali o la proposta di raccomandazione del Consiglio sul miglioramento dell'offerta di competenze digitali nell'istruzione e nella formazione, che hanno l'obiettivo di far sì che l'80 % della popolazione acquisisca le competenze digitali di base entro il 2030.

[14] (ISC)², Valutazione delle competenze informatiche sulla base dell'ECSF, webinar ENISA, 16 febbraio 2023 (solo in EN).

[15] Secondo l'Organizzazione europea per la cibersicurezza (ECSO), come dichiarato nella comunicazione congiunta al Parlamento europeo e al Consiglio "La politica di ciberdifesa dell'UE" (JOIN(2022) 49 final).

[16] (ISC)², Valutazione delle competenze informatiche sulla base dell'ECSF, webinar ENISA, 16 febbraio 2023 (solo in EN).

[17] Banca dati dell'istruzione superiore sulla cibersicurezza (CyberHEAD) (solo in EN).

specialiste in tecnologie dell'informazione e della comunicazione (TIC)[18]. Per affrontare questo problema, il **programma strategico per il decennio digitale 2030** dell'Europa[19] ha fissato l'obiettivo di aumentare il numero di professionisti delle TIC di 20 milioni di unità entro il 2030, raggiungendo anche la convergenza di genere. Inoltre l'attuazione della politica emergente dell'UE richiede una forza lavoro adeguatamente qualificata e sufficiente. Ad esempio oltre il 42 % dei dirigenti informatici nel settore dei servizi finanziari ha evidenziato come la mancanza di competenze e conoscenze in materia di cibersicurezza sia una delle sfide principali per la loro impresa nell'ambito della difesa della cibersicurezza e della gestione degli incidenti[20], nel momento in cui dovranno attuare la normativa settoriale in materia di cibersicurezza come il regolamento sulla resilienza operativa digitale (DORA).

L'esitazione dei datori di lavoro a investire nel capitale umano, cercando forza lavoro già formata ed esperta, contribuisce ulteriormente a limitare il mercato del lavoro[21]. Questa carenza riguarda tutti i tipi di imprese, comprese le piccole e medie imprese (**PMI**), che rappresentano il 99 % di tutte le imprese dell'UE[22]. La sfida è notevole anche per le **amministrazioni pubbliche**, che sono le più colpite e penalizzate degli incidenti di cibersicurezza[23].

Colmare il divario di talenti professionali nel settore della cibersicurezza dell'UE è quindi una questione urgente, poiché sono in gioco la sicurezza e la competitività dell'Unione.

2. Mancanza di sinergie e di azioni coordinate per colmare il divario di competenze in materia di cibersicurezza

Per affrontare le carenze del mercato del lavoro nel settore della cibersicurezza, gli enti pubblici e privati hanno avviato una serie di iniziative a livello europeo e nazionale. Essendo realizzate in modo frammentario, tali iniziative non sono ancora riuscite a raggiungere una massa critica in grado di innescare un vero e proprio cambiamento.

Innanzitutto la comprensione comune della composizione della forza lavoro nel settore della cibersicurezza dell'UE e delle competenze associate è attualmente limitata, ma profili professionali simili nel campo della cibersicurezza dovrebbero comportare lo stesso insieme di competenze. La scarsa adozione da parte dei soggetti interessati di un **quadro di riferimento** comune **europeo per i professionisti della cibersicurezza** si traduce nella mancanza di uno strumento di comunicazione tra datori di lavoro, educatori e responsabili politici, e nell'incapacità di condurre misurazioni e di valutare le lacune del mercato del lavoro nel settore della cibersicurezza. Ciò impedisce inoltre l'elaborazione di programmi di istruzione e formazione e la creazione di percorsi di carriera che rispondano alle esigenze strategiche e di mercato per coloro che desiderano accedere alla professione. Il **miglioramento delle competenze e la riqualificazione** della forza lavoro si basano in larga misura su corsi di formazione e attestati in materia di cibersicurezza, solitamente offerti da

[18] Solo il 19 % degli specialisti nelle TIC dell'UE è costituito da donne. Indice di digitalizzazione dell'economia e della società (DESI) 2022 | Plasmare il futuro digitale dell'Europa (europa.eu). Non sono disponibili dati relativi alla forza lavoro femminile dell'Unione nel settore della cibersicurezza.

[19] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030, che stabilisce un meccanismo di monitoraggio e cooperazione per raggiungere gli obiettivi e i traguardi comuni per la trasformazione digitale dell'Europa definiti nella bussola per il digitale 2030, compreso il settore delle competenze.

[20] S-RM, *Cyber Security Insights Report 2022*.

[21] Lo sviluppo delle competenze in materia di cibersicurezza nell'UE, ENISA, dicembre 2019 (solo in EN).

[22] Definizione di PMI (europa.eu) (solo in EN).

[23] Relazione dell'ENISA sul panorama delle minacce 2022 — ENISA (europa.eu) (solo in EN).

erogatori privati. La forza lavoro ha tuttavia difficoltà a ottenere una visione d'insieme della qualità dell'offerta di corsi di formazione in materia di cibersicurezza e dei relativi attestati rilasciati.

Mentre l'istruzione, la formazione e la definizione di percorsi di carriera sono necessari per stimolare il lato dell'offerta del mercato del lavoro, attualmente il ruolo del lato della **domanda** nella formazione della forza lavoro e nell'adattamento all'evoluzione del mercato del lavoro è sottovalutato. I datori di lavoro dell'industria e del settore pubblico non dispongono di consessi e sedi comuni dove poter condividere le idee su come formare al meglio la forza lavoro e su come **valutare le competenze in modo più adeguato**, soprattutto durante il processo di assunzione. Le **competenze tecnico-specialistiche** (*hard skills*) più richieste possono essere legate alla cibersicurezza[24], come lo sviluppo di software o il cloud computing[25], ma le **competenze trasversali** sono ancora ingiustificatamente ignorate. Il pensiero critico e l'analisi, la risoluzione dei problemi e l'autogestione sono le competenze più richieste dai datori di lavoro[26], e la loro importanza è in aumento in vista del 2025[27].

Esistono già numerose iniziative di investimento pubblico e privato nelle competenze in materia di cibersicurezza e l'UE **finanzia** ampiamente progetti nell'ambito di diversi strumenti[28]. Tuttavia la continua carenza di competenze nell'UE solleva dubbi sulla visibilità e sull'impatto di tali iniziative e suggerisce che potrebbero non corrispondere sistematicamente alle esigenze del mercato, che devono essere mappate con urgenza a livello dell'UE. Inoltre diverse fonti di finanziamento portano alla duplicazione, facendo così perdere l'opportunità di ampliare i progetti e di produrre effetti concreti. Inoltre, chi ha bisogno di investimenti non sempre riesce a individuare le fonti più adatte alle proprie esigenze.

I **portatori di interessi** hanno cercato di affrontare il problema complesso e sfaccettato della carenza di competenze in materia di cibersicurezza. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) sta sviluppando strumenti relativi ai profili di ruolo o all'istruzione superiore[29], il Centro europeo di competenza per la cibersicurezza (ECCC)[30] sta affrontando il tema delle competenze in materia di cibersicurezza in un gruppo di lavoro dedicato, l'Accademia europea per la sicurezza e la difesa (AESD) sta lavorando sulle competenze in materia di cibersicurezza della forza lavoro civile e militare nel contesto della politica di sicurezza e di difesa comune[31], le organizzazioni private stanno cercando di affrontare il problema[32], il settore che si occupa del rilascio delle certificazioni in materia di cibersicurezza sta mettendo a punto una tabella di marcia e corsi di formazione volti a

---

[24] *LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most*.

[25] ISACA, infografica sullo stato della sicurezza informatica 2022.

[26] Come lo strumento CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[27] *The Future of Jobs Report*, ottobre 2020, Forum economico mondiale.

[28] Ad esempio: Cybersecurity Skills Alliance – New Vision for Europe – Progetto REWIRE (finanziato dal programma Erasmus+); progetti a sostegno del Centro di competenza per la cibersicurezza (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (finanziato da Orizzonte 2020), progetto Cybersecpro (finanziato dal programma Europa digitale).

[29] In particolare: il quadro europeo delle competenze in materia di cibersicurezza (ECSF); la banca dati dell'istruzione superiore sulla cibersicurezza (CYBERHEAD); la piattaforma di esercitazione informatica (CEP); la sfida europea per la cibersicurezza; il mese europeo della cibersicurezza.

[30] Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

[31] In particolare la piattaforma informatica in materia di istruzione, formazione, valutazione ed esercitazioni (ETEE).

[32] Ad esempio, il gruppo di lavoro 5 dell'Organizzazione europea per la cibersicurezza (ECSO) "Istruzione, formazione, consapevolezza, poligoni virtuali, fattori umani"; l'organizzazione DIGITALEUROPE.

colmare il divario di competenze[33]. Gli Stati membri stanno inoltre cercando di affrontare il problema attraverso una serie di iniziative, che vanno dalla regolamentazione[34] alla creazione di accademie per le competenze in materia di cibersicurezza[35], Cyber Campus[36] o centri di eccellenza per contrastare la criminalità informatica[37], o attraverso partenariati pubblico-privati[38]. Tuttavia il lavoro svolto da tutti questi portatori di interessi manca spesso di coordinamento e sinergie, e non è stato in grado di sfruttare appieno il proprio potenziale e incidere in modo sostanziale sul mercato del lavoro, come dimostra la crescente carenza di forza lavoro nel settore della cibersicurezza nell'UE. Occorre inoltre potenziare le sinergie tra le cibercomunità, poiché le competenze necessarie per sostenere la cibersicurezza, combattere la **criminalità informatica** o mettere a punto misure **di ciberdifesa** sono spesso di natura analoga.

Si noti infine che attualmente l'UE dispone di mezzi limitati per valutare lo **stato e l'evoluzione del mercato del lavoro nel settore della cibersicurezza** e delle competenze della sua forza lavoro. Gli Stati membri, nonché le istituzioni, gli organi e gli organismi europei si basano su dati raccolti da enti privati o su una serie più ampia di dati raccolti dall'UE, in particolare da Eurostat[39] e dal Centro europeo per lo sviluppo della formazione professionale (CEDEFOP)[40], sui professionisti delle TIC. In altre parole l'UE ha una visione parziale e frammentaria delle sue esigenze, che le impedisce di consolidare una visione aggregata dello stato del mercato del lavoro nel settore della cibersicurezza.

3. Una risposta coordinata a livello dell'UE: l'Accademia per le competenze in materia di cibersicurezza

3.1. Obiettivo

Per rispondere alla sfida riguardante le competenze in materia di cibersicurezza e colmare il divario nel mercato del lavoro, la Commissione propone l'istituzione di un'**Accademia per le competenze in materia di cibersicurezza**, come annunciato dalla presidente della Commissione europea nella sua lettera d'intenti che correda il discorso sullo Stato dell'Unione 2022[41, , 42] e nel contesto dell'Anno europeo delle competenze.

L'Accademia per le competenze in materia di cibersicurezza (in breve "l'Accademia") mira a creare un **unico punto di accesso e sinergie** per le offerte di istruzione e formazione nel campo della cibersicurezza, nonché per le opportunità di finanziamento e le azioni specifiche volte a sostenere lo sviluppo delle competenze nel settore della cibersicurezza. Aumenterà le iniziative dei portatori di interessi per raggiungere una massa critica in grado di fare la differenza sul mercato del lavoro, anche per la difesa. Queste attività si allineerebbero su obiettivi e indicatori chiave di prestazione comuni per cercare di ottenere un impatto maggiore.

---

[33] Ad esempio, l'Istituto SANS, (ISC)², ISACA.

[34] Ad esempio, nelle strategie nazionali per l'istruzione o la cibersicurezza.

[35] Ad esempio, la C-Academy in Portogallo.

[36] Ad esempio, i Cyber Campus in Francia.

[37] Ad esempio, il centro lituano di eccellenza contro la criminalità informatica per la formazione, la ricerca e l'istruzione in Lituania (L3CE).

[38] Ad esempio, l'iniziativa promossa da Microsoft per lo sviluppo delle competenze in materia di cibersicurezza.

[39] Specialisti nelle TIC nel mondo del lavoro - Spiegazione delle statistiche (europa.eu) (solo in EN).

[40] Come lo strumento CEDEFOP: Skills-OVATE | CEDEFOP (europa.eu).

[41] Stato dell'Unione 2022 - Lettera d'intenti alla presidente Roberta Metsola e al primo ministro Petr Fiala.

[42] Comunicazione congiunta al Parlamento europeo e al Consiglio - La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

Al centro dell'attività dell'Accademia vi sarà lo sviluppo delle competenze dei **professionisti della cibersicurezza**. L'attività dell'Accademia si inserirà nel contesto delle politiche dell'UE sulla cibersicurezza, ma anche di quelle inerenti l'istruzione e l'apprendimento permanente, e integra le due raccomandazioni del Consiglio relative all'istruzione e alle competenze digitali proposte dalla Commissione parallelamente alla presente comunicazione[43].

L'Accademia si baserà su quattro pilastri: 1) promuovere la **generazione di conoscenze mediante l'istruzione e la formazione**, elaborando un quadro comune per i profili di ruolo in materia di cibersicurezza e le competenze associate, rafforzando l'offerta europea di istruzione e formazione per soddisfare le esigenze del settore, definendo percorsi di carriera e fornendo visibilità e chiarezza in merito alle formazioni e alle certificazioni in materia di cibersicurezza al fine di rafforzare il lato dell'offerta sul mercato del lavoro; 2) garantire un migliore indirizzamento e visibilità delle **opportunità di finanziamento** disponibili per le attività legate alle competenze, al fine di massimizzarne l'impatto; 3) invitare i portatori di interessi **ad agire**; e 4) definire indicatori per **monitorare l'evoluzione del mercato** ed essere in grado di valutare l'efficacia delle proprie azioni.

La realizzazione dell'Accademia sarà sostenuta da un finanziamento di 10 milioni di EUR a titolo del programma Europa digitale[44].

3.2. Governance dell'Accademia

Per garantire un'infrastruttura che funga da **punto di accesso unico** per la promozione della cooperazione tra il mondo accademico, gli erogatori di formazione e l'industria, in cui il lato dell'offerta e quello della domanda dell'ecosistema di cibersicurezza dell'UE possano incontrarsi ed essere formati, l'Accademia potrebbe assumere la forma di un **consorzio per l'infrastruttura digitale europea (EDIC)**[45]. Questo strumento consentirebbe agli Stati membri di lavorare congiuntamente per colmare il divario di competenze in materia di cibersicurezza, nonché di collaborare strettamente con la Commissione, l'ENISA e il Centro europeo di competenza per la cibersicurezza (ECCC), in linea con i rispettivi mandati e le rispettive competenze, e di coinvolgere tutti i portatori di interessi pertinenti, ma anche di indirizzare gli investimenti europei, nazionali e privati verso un obiettivo comune. A tal fine gli Stati membri interessati sono incoraggiati a presentare alla Commissione, entro il 30 maggio 2023, una pre-notifica della loro futura domanda per la costituzione di tale EDIC. Tale pre-notifica volontaria consentirebbe alla Commissione di formulare osservazioni tempestive sul progetto di domanda per la costituzione di un EDIC, consentendone così l'ulteriore elaborazione e la presentazione formale in modo più rapido. Durante l'intero processo e nella misura richiesta dagli Stati membri, la Commissione, fungendo da acceleratore di progetti multinazionali, faciliterà la preparazione della domanda per la costituzione di un EDIC. In seguito, dopo una valutazione positiva della domanda da parte della Commissione e l'approvazione da parte del comitato del programma per il decennio digitale, la Commissione adotterà una decisione che costituisce l'EDIC e successivamente contribuirà al coordinamento della sua attuazione[46].

---

[43] Proposte di raccomandazioni del Consiglio sui fattori abilitanti fondamentali per il successo dell'istruzione e della formazione digitale e sul miglioramento dell'offerta di competenze digitali nell'istruzione e nella formazione.

[44] Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

[45] Gli EDIC sono stati istituiti nel quadro della decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030, articolo 13 e segg.

[46] Ibidem, articolo 12.

Nel frattempo, mentre l'EDIC sarà costituito formalmente, la Commissione creerà un punto di accesso unico virtuale potenziando la **piattaforma per le competenze e le occupazioni digitali** della Commissione[47] con il sostegno del progetto volto a promuovere la comunità europea della cibersicurezza (*European Cybersecurity Community*, ECCO)[48].

L'**ENISA** contribuirà alla realizzazione dell'Accademia in linea con gli obiettivi dell'Agenzia[49], in particolare per quanto riguarda l'assistenza all'istruzione e alla formazione in materia di cibersicurezza, e tenendo conto dei suoi obblighi di comunicazione a norma della direttiva NIS 2[50]. L'**ECCC** opererà in linea con la sua agenda strategica a sostegno della realizzazione dell'Accademia per le competenze in materia di cibersicurezza. In particolare l'ECCC attuerà l'obiettivo strategico 3 (Cibersicurezza) del programma Europa digitale. Il Centro beneficerà del sostegno della Commissione e degli Stati membri mediante i **centri nazionali di coordinamento (CNC)**. La partecipazione del **gruppo di cooperazione** istituito ai sensi della direttiva NIS 2[51] sarà richiesta laddove opportuno. Infine sarà necessaria la collaborazione con l'**industria** e il **mondo accademico** per conseguire l'obiettivo dell'Accademia di colmare il divario di competenze in materia di cibersicurezza.

4. Generazione di conoscenze e formazione: stabilire un approccio comune dell'UE alla formazione in materia di cibersicurezza

Nell'ambito del pilastro sulla generazione di conoscenze e sulla formazione dell'Accademia per le competenze in materia di cibersicurezza, verrà elaborato un approccio strutturato con il chiaro obiettivo di accrescere il **numero** di persone con competenze in materia di cibersicurezza nell'UE, di orientare meglio i percorsi formativi alle **esigenze del mercato** e di garantire la visibilità dei **percorsi di carriera**.

4.1. Parlare la stessa lingua: un approccio comune sui profili di ruolo in materia di cibersicurezza e sulle competenze associate

L'ENISA si è già attivata per definire i profili di ruolo dei professionisti della cibersicurezza nell'ambito del quadro europeo delle competenze in materia di cibersicurezza **(ECSF**)[52], sul quale l'Accademia dovrebbe basarsi per definire e valutare le competenze pertinenti, monitorare l'evoluzione dei divari di competenze e fornire indicazioni sulle nuove esigenze. Per ogni ruolo nel settore della cibersicurezza dell'ECSF, un insieme di competenze

[47] Home | Piattaforma per le competenze e le occupazioni digitali (europa.eu).

[48] Cfr. il Centro e la rete europei di competenza per la cibersicurezza: un nuovo progetto finanziato dall'UE per sostenere la cibercomunità (solo in EN). Nel dicembre 2022 la Commissione europea ha firmato un contratto di 3 milioni di EUR per sostenere la cibercomunità dell'UE nel quadro del Centro europeo di competenza per la cibersicurezza. Questo progetto contribuirà agli obiettivi dell'UE in materia di sviluppo della comunità e delle capacità per quanto riguarda la ricerca e l'innovazione nel settore della cibersicurezza, nonché la sua diffusione e la relativa base industriale.

[49] "L'ENISA sostiene lo sviluppo delle capacità e la preparazione nell'Unione, assistendo le istituzioni, gli organi e gli organismi dell'Unione, nonché gli Stati membri e i portatori di interessi del settore pubblico e privato [...] nello sviluppo di abilità e competenze nel campo della cibersicurezza". Articolo 4, paragrafo 3, del regolamento sulla cibersicurezza.

[50] Articolo 18 della direttiva NIS 2.

[51] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

[52] Quadro europeo delle competenze in materia di cibersicurezza (ECSF) - ENISA (europa.eu). L'ECSF sostiene l'individuazione e l'articolazione di competenze, abilità, conoscenze e compiti associati ai ruoli dei professionisti europei della cibersicurezza. Riassume tutti i ruoli legati alla cibersicurezza in profili che sono analizzati singolarmente, esaminando nel dettaglio le responsabilità, competenze, sinergie e interdipendenze corrispondenti.

applicabili del quadro europeo delle competenze informatiche[53] è stato incorporato nella descrizione del profilo[54].

L'ENISA rivedrà quindi l'ECSF e **individuerà le esigenze e i divari di competenze in evoluzione** nella forza lavoro del settore della cibersicurezza, anche tramite strumenti avanzati (ad esempio, intelligenza artificiale, big data[55], estrazione di dati). A tal fine l'ENISA lavorerà sotto la guida dell'EDIC, una volta costituito, e dell'ECCC, insieme ai CNC, alla Commissione, al progetto ECCO e agli attori del mercato[56]. Per quanto riguarda la forza lavoro nel settore della ciberdifesa, l'ENISA terrà in debito conto il lavoro svolto dall'AESD. Analogamente, nell'ambito della lotta alla criminalità informatica, l'ENISA terrà conto delle attività svolte dall'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL) e da Europol nell'elaborazione di un'analisi delle esigenze formative operative[57] in materia di attacchi informatici.

L'ECSF sarà regolarmente integrato e rivisto nell'ambito dell'Accademia ogni due anni. Inoltre la Commissione e il servizio europeo per l'azione esterna contribuiranno a definire, secondo le necessità, profili specifici e competenze associate per settori, con il sostegno di agenzie e organismi dell'UE quali l'AESD[58], Europol e CEPOL[59].

Saranno inoltre creati dei collegamenti tra l'ECSF e i pertinenti strumenti della politica dell'UE in materia di occupazione[60]. In particolare i profili professionali dell'ECSF e le relative competenze saranno integrati nella **classificazione ESCO**. Ciò permetterà di migliorare la classificazione delle professioni e delle competenze nel campo della cibersicurezza e favorire il collegamento tra di esse, rendendo più facile per i singoli il miglioramento delle competenze e la riqualificazione professionale e promuovendo l'incontro tra domanda e offerta di lavoro sulla base delle competenze e la mobilità transfrontaliera.

4.2. Favorire la cooperazione per ideare programmi di istruzione e formazione in materia di cibersicurezza

Una volta costituito l'EDIC, l'Accademia dovrebbe ricevere il sostegno degli Stati membri per diventare il **luogo di riferimento in Europa per la concezione e l'erogazione di corsi di formazione in materia di cibersicurezza** che consentano di acquisire le competenze più richieste e forniscano opportunità di formazione sul posto di lavoro e di tirocinio per le start-up, le PMI e le amministrazioni pubbliche in imprese innovative nel campo della

---

[53] Quadro europeo delle competenze informatiche (e-CF) | Esco (europa.eu) L'e-CF fornisce collegamenti coerenti nel contesto delle qualifiche TIC e di altri quadri pertinenti per il settore, tra i quali il quadro DigComp.

[54] Cfr. a questo proposito il Manuale d'uso - Quadro europeo delle competenze in materia di cibersicurezza (ECSF) - settembre 2022 (solo in EN).

[55] Cfr., ad esempio, Skills-OVATE, elaborato dal Cedefop.

[56] L'Agenzia farà ulteriormente leva sui risultati di altri progetti finanziati dall'UE (ad esempio REWIRE, Spazio di dati per le competenze (DS4S), CyberSecPro, Concordia) e sulle metodologie derivanti da iniziative analoghe (ad esempio "*Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States*", relazione OCSE, pubblicata il 21 marzo 2023) per garantire in futuro una visione aggiornata delle esigenze in un contesto in cui la domanda è in continua evoluzione.

[57] CEPOL Analisi delle esigenze formative operative (*Operational Training Needs Assessment*, OTNA).

[58] Cfr. a questo proposito la comunicazione congiunta al Parlamento europeo e al Consiglio - La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

[59] A questo riguardo si presterà attenzione al lavoro sul quadro delle competenze per la formazione in materia di criminalità informatica (TCF), attualmente in fase di sviluppo.

[60] Come la classificazione europea di abilità, competenze, qualifiche e occupazioni (ESCO), Europass e la rete di cooperazione europea dei servizi per l'impiego(EURES).

cibersicurezza e in centri specializzati nella cibersicurezza. L'EDIC dovrebbe collaborare con tutti i portatori di interessi pertinenti, compresa l'industria, per concepire tali corsi di formazione, e basarsi su progetti come il progetto **CyberSecPro**[61], finanziato dal programma Europa digitale, che riunisce 17 istituti di istruzione superiore e 13 imprese operanti nel settore della sicurezza di 16 Stati membri, e che mira a convertirsi nella migliore prassi di riferimento per tutti i programmi di formazione in materia di cibersicurezza.

L'Accademia collaborerà con tutti i portatori di interessi pertinenti per **attrarre le giovani generazioni** affinché intraprendano una carriera nella cibersicurezza. In linea con la proposta di raccomandazione del Consiglio sul miglioramento dell'offerta di competenze digitali nell'istruzione e nella formazione, gli Stati membri dovrebbero stabilire e rafforzare misure finalizzate ad assumere e formare insegnanti e formatori specializzati, e agevolare l'acquisizione di competenze in materia di cibersicurezza, anche mediante tirocini. Si dovrebbe incoraggiare l'integrazione della cibersicurezza nei programmi di istruzione e formazione, garantendone l'accessibilità, ampliando l'offerta di periodi di **apprendistato** e tirocinio, promuovendo approcci innovativi che includano, ad esempio, serious games e piattaforme di simulazione condivise, organizzando settimane di immersione in posizioni di cibersicurezza e illustrando le caratteristiche dei profili di ruolo non tecnici. È inoltre opportuno sostenere la partecipazione a queste opportunità di apprendimento in materia di cibersicurezza di gruppi difficili da raggiungere, come i giovani con disabilità, che vivono in aree remote o rurali, o appartenenti ad altri gruppi minoritari.

La Commissione continuerà a sostenere lo sviluppo di microcredenziali, nonché di programmi di istruzione e formazione professionale. In particolare continueranno a essere finanziati nell'ambito di Erasmus+ **programmi di laurea di primo livello e magistrale congiunti, corsi o moduli congiunti volti al conseguimento di microcredenziali** e **programmi intensivi misti**[62] su tutti i temi, compreso quello della **cibersicurezza**. Sarà inoltre sostenuta l'ulteriore diffusione dell'**iniziativa delle università europee**[63] e dei **centri di eccellenza professionale**[64] per incoraggiare una maggiore cooperazione tra gli istituti di istruzione superiore e gli istituti di istruzione e formazione professionale pertinenti in tutta Europa. I programmi di finanziamento dell'UE, tra cui Erasmus+ e il programma Europa digitale, sosterranno l'obiettivo summenzionato di rafforzamento della cooperazione, insieme ai fondi UE destinati allo sviluppo di **conti individuali di apprendimento**[65].

Per facilitare la cooperazione a livello nazionale tra il mondo accademico, gli erogatori di corsi di formazione sulle competenze in materia di cibersicurezza e i datori di lavoro del settore pubblico e privato, e per promuovere sinergie tra il settore pubblico e quello privato, i CNC sono invitati a valutare la creazione di **Cyber Campus** negli Stati membri. I Cyber Campus mirerebbero a fornire poli di eccellenza a livello nazionale per la comunità della cibersicurezza, e l'Accademia favorirebbe la loro collaborazione in rete e l'ulteriore coordinamento delle relative attività.

---

[61] Il progetto CyberSecPro effettuerà, ad esempio, un'analisi dei programmi, dei corsi e delle scuole estive in materia di cibersicurezza offerti nelle università e delle tabelle di classificazione del sistema europeo di accumulazione e trasferimento dei crediti (ECTS) utilizzate, garantirà la partecipazione di oltre 530 tirocinanti nell'arco di tre anni e formerà persone esterne provenienti da diversi settori e industrie.

[62] I programmi intensivi misti combinano l'insegnamento online con un breve periodo di mobilità fisica.

[63] Iniziativa delle università europee | Spazio europeo dell'istruzione (europa.eu).

[64] Centri di eccellenza professionale | Erasmus+ (europa.eu).

[65] In linea con la raccomandazione del Consiglio del 16 giugno 2022 sui conti individuali di apprendimento.

Anche l'ENISA migliorerà la sua offerta formativa in materia di cibersicurezza, allineando **il catalogo dei corsi**[66] ai profili dell'ECSF ed elaborando moduli formativi per profilo, che potrebbero arricchire l'offerta formativa degli Stati membri. L'ENISA amplierà inoltre il suo **programma di "formazione dei formatori"**[67], focalizzandosi sulle esigenze professionali delle istituzioni, degli organi e degli organismi europei, delle autorità pubbliche degli Stati membri e degli **operatori critici pubblici e privati** che rientrano nell'ambito di applicazione della direttiva NIS 2.

Inoltre altri organi e organismi dell'UE amplieranno la loro offerta formativa in materia di cibersicurezza. Ad esempio, attuando la politica dell'UE sulla ciberdifesa, l'**AESD** metterà a punto una nuova serie di corsi sulla cibersicurezza e allineerà alcuni dei suoi corsi attuali con l'ECSF. Tali corsi termineranno con la certificazione dei risultati di apprendimento[68]. L'AESD, in collaborazione con la Commissione, valuterà la possibilità di integrare i certificati nel portafoglio EUeID ed esaminerà ulteriormente i possibili meccanismi di valutazione delle competenze, in base ai quali saranno rilasciati i certificati. Analogamente, nell'ambito della lotta alla criminalità informatica, si cercherà di stabilire rapporti di stretta collaborazione con l'**Accademia CEPOL per la criminalità informatica**[69], al fine di favorire sinergie e complementarità nella concezione e realizzazione dei programmi di formazione.

4.3.Creare sinergie e garantire visibilità ai percorsi formativi e alle certificazioni in materia di cibersicurezza negli Stati membri

L'Accademia dovrebbe affrontare la questione della visibilità e delle sinergie tra formazione e certificazione a vantaggio delle cibercomunità civile, della difesa, di contrasto e diplomatica, poiché tutti i settori richiedono in molti casi le stesse competenze, basate su programmi e risultati di apprendimento analoghi.

L'Accademia offrirebbe un **punto di accesso unico** per coloro che sono interessati a una carriera nel settore della cibersicurezza. Nel breve termine ciò si concretizzerà tramite il potenziamento della **piattaforma per le competenze e le occupazioni digitali** della Commissione, con il sostegno del progetto ECCO. Una sezione specifica per le carriere nella cibersicurezza fornirà collegamenti con gli strumenti esistenti, dai programmi di istruzione superiore alle opportunità di formazione, compresi i corsi volti al conseguimento di microcredenziali e i programmi di istruzione e formazione professionale, fino alle offerte di lavoro. A tal fine nella piattaforma saranno integrate le attività e le iniziative in corso o saranno forniti riferimenti a tali attività e iniziative, come quelle dell'ENISA che, in collaborazione con il mondo accademico, ha proceduto alla **mappatura degli istituti di istruzione** che offrono programmi sulla cibersicurezza. Questo aspetto sarà rafforzato con il sostegno dei CNC. Inoltre l'ENISA provvederà a sviluppare e consolidare due **archivi contenenti corsi di formazione esistenti offerti dal settore pubblico e privato e certificazioni in materia di cibersicurezza** con il sostegno dei CNC, della Commissione e del progetto ECCO e in collaborazione con gli enti che rilasciano certificazioni, basandosi

[66] Corsi di formazione - ENISA (europa.eu).

[67] Programma di formazione dei formatori - ENISA (europa.eu).

[68] In linea con l'articolo 20, paragrafo 4, della decisione (PESC) 2020/1515 del Consiglio, del 19 ottobre 2020, che istituisce l'Accademia europea per la sicurezza e la difesa e abroga la decisione (PESC) 2016/2382.

[69] L'Accademia CEPOL per la criminalità informatica è stata istituita nel 2019 per fornire una piattaforma all'avanguardia tesa a migliorare la conoscenza della criminalità informatica e le capacità informatiche in Europa.

anche su altre iniziative pertinenti[70]. Gli archivi saranno anche integrati nel punto di accesso unico della piattaforma per le competenze e le occupazioni digitali. Tale iniziativa andrà anche a beneficio dei CNC, il cui compito è in particolare quello di promuovere e diffondere i programmi didattici in materia di cibersicurezza[71].

Occorre inoltre fornire ai professionisti la garanzia che i percorsi formativi che intraprendono siano della qualità richiesta. A tal proposito l'ENISA metterà a punto un **progetto pilota** che valuterà l'istituzione di un sistema europeo di attestazione delle competenze in materia di cibersicurezza.

È inoltre essenziale individuare le competenze e i percorsi formativi e associarli a un profilo professionale, ma è altresì importante garantire che i servizi di cibersicurezza siano forniti con la competenza, la perizia e l'esperienza richieste. Ciò vale in particolare per i fornitori di servizi di sicurezza gestiti, in ambiti come la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza. La direttiva NIS 2 e la proposta di normativa sulla cibersolidarietà stabiliscono compiti specifici per tali fornitori di servizi di sicurezza gestiti. La Commissione propone pertanto anche una **modifica mirata del regolamento sulla cibersicurezza**[72] per consentire sistemi di certificazione dei servizi di sicurezza gestiti a livello dell'UE, che dovrebbero mirare, tra l'altro, a garantire che i servizi in questione siano forniti da personale con un livello molto elevato di conoscenze e competenze tecniche nei settori pertinenti.

I **meccanismi di garanzia della qualità e di riconoscimento delle microcredenziali**[73] favoriscono la trasparenza, la comparabilità e la portabilità dei risultati dell'apprendimento. In linea con la raccomandazione del Consiglio su un approccio europeo alle microcredenziali[74], gli Stati membri sono incoraggiati a includere le microcredenziali nel campo della cibersicurezza nei rispettivi quadri nazionali delle qualifiche. Ciò consentirebbe loro di mettere in relazione tali microcredenziali con il quadro europeo delle qualifiche[75]. L'infrastruttura delle credenziali digitali europee per l'apprendimento è disponibile per rilasciare ai singoli soggetti qualifiche e microcredenziali relative alla cibersicurezza firmate digitalmente. Tali qualifiche e microcredenziali contengono dati esaustivi, tra cui i risultati dell'apprendimento sulla cibersicurezza, e possono essere conservate nel futuro **portafoglio digitale EUeID**[76].

---

[70] Ad esempio, l'Accademia W4C - Women4Cyber o il progetto di certificazione per la lotta alla criminalità informatica globale rivolto alle autorità di contrasto e alle autorità giudiziarie.

[71] "1. I centri nazionali di coordinamento hanno i compiti seguenti: [...] g) fatte salve le competenze degli Stati membri in materia di istruzione e tenendo conto dei pertinenti compiti dell'ENISA, avviare un dialogo con le autorità nazionali in merito a un possibile contributo alla promozione e alla diffusione di programmi didattici in materia di cibersicurezza", articolo 7, paragrafo 1, lettera g), del regolamento sull'ECCC. Cfr. anche il considerando 28 associato.

[72] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza").

[73] Ad esempio la registrazione o la certificazione dei risultati di apprendimento ottenuti in seguito a formazioni di breve durata.

[74] Raccomandazione del Consiglio, del 16 giugno 2022, relativa a un approccio europeo alle microcredenziali per l'apprendimento permanente e l'occupabilità.

[75] Raccomandazione del Consiglio, del 22 maggio 2017, sul quadro europeo delle qualifiche per l'apprendimento permanente, che abroga la raccomandazione del Parlamento europeo e del Consiglio, del 23 aprile 2008, sulla costituzione del quadro europeo delle qualifiche per l'apprendimento permanente.

[76] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea.

Azioni nell'ambito dell'Accademia

Stati membri e industria

- Garantire il sostegno allo sviluppo e al riconoscimento di **microcredenziali** di apprendimento in materia di cibersicurezza, in linea con la raccomandazione del Consiglio su un approccio europeo alle microcredenziali.
- Includere le qualifiche relative alla cibersicurezza, comprese le microcredenziali, nei **quadri nazionali delle qualifiche**.
- Offrire, tramite apprendistati, **opportunità di apprendimento sul posto di lavoro** alle persone che partecipano a iniziative di sviluppo delle competenze in materia di cibersicurezza.

Commissione

- A breve termine, entro la fine del 2023 creare **un punto di accesso unico** per i programmi sulla cibersicurezza, i percorsi formativi esistenti e le certificazioni sulla cibersicurezza mediante la **piattaforma per le competenze e le occupazioni digitali**.
- Il 18 aprile 2023 proporre una modifica del **regolamento sulla cibersicurezza** per consentire la certificazione dei fornitori di servizi di sicurezza gestiti.

Organi e organismi dell'UE

- Entro la fine del 2023 far sì che l'**ECSF** sia riconosciuto come un approccio comune ai profili di ruolo in materia di cibersicurezza e alle competenze associate.
- Nel secondo trimestre del 2023 l'ENISA avvierà l'elaborazione di un progetto pilota per la creazione di un **sistema europeo di attestazione** delle competenze in materia di cibersicurezza.
- Entro la fine del 2023 l'ENISA rivedrà il suo **catalogo di corsi** ed estenderà il **programma di "formazione dei formatori"** agli **operatori** critici pubblici e privati.
- Portare a termine l'**allineamento dei programmi di studio dell'AESD all'ECSF** entro la metà del 2023.

5. Partecipazione dei portatori di interessi: impegnarsi a colmare il divario di competenze in materia di cibersicurezza

Nell'ambito dell'Accademia verrà definito un approccio coordinato alla partecipazione dei portatori di interessi al fine di colmare il divario di competenze in materia di cibersicurezza. L'obiettivo sarà quello di massimizzare la visibilità e l'impatto dei vari impegni assunti dai portatori di interessi finalizzati a ridurre il divario di competenze in materia di cibersicurezza.

La Commissione invita i portatori di interessi ad assumere impegni concreti per il miglioramento delle competenze e la riqualificazione dei lavoratori attraverso azioni specifiche, basandosi il più possibile sul divario di competenze in materia di cibersicurezza individuato. Tali **impegni in materia di cibersicurezza assunti dai portatori di interessi** dovrebbero essere riportati sulla **piattaforma per le competenze e le occupazioni digitali**, analogamente ad altri impegni digitali già visibili sulla medesima. La Commissione incoraggia inoltre i portatori di interessi che assumono un impegno in materia di cibersicurezza sulla piattaforma ad aderire al **partenariato digitale su vasta scala**

nell'ambito del patto per le competenze[77]. Si invita a presentare sulla piattaforma per le competenze e le occupazioni digitali gli impegni in materia di cibersicurezza assunti nell'ambito del partenariato digitale su vasta scala. Analogamente si incoraggia a riportare nel quadro del partenariato digitale su vasta scala del patto per le competenze gli impegni assunti nell'ambito della piattaforma per le competenze e le occupazioni digitali.

La Commissione invita altresì gli Stati membri a **proseguire le iniziative intraprese per l'attuazione della dichiarazione di impegno sulle donne nel digitale**[78] per incoraggiare le donne a svolgere un ruolo attivo e di primo piano nel settore della tecnologia digitale e per raggiungere la convergenza di genere nei posti di lavoro nel settore della cibersicurezza. La Commissione incoraggia inoltre gli Stati membri a sviluppare sinergie con i programmi elaborati nel quadro del **Fondo sociale europeo+** (FSE+), al fine di sostenere ulteriormente l'obiettivo della parità di genere nella partecipazione al mercato del lavoro[79], ad esempio istituendo **programmi di tutoraggio per le ragazze e le donne**. Tali programmi possono facilitare la creazione di modelli di riferimento per incoraggiare le ragazze a intraprendere professioni nel settore della cibersicurezza, contrastando al tempo stesso gli stereotipi legati al genere. La Commissione promuove inoltre il miglioramento delle competenze e la riqualificazione delle donne, nonché lo sviluppo di una comunità che possa sostenere le donne durante l'inserimento nel mercato del lavoro della cibersicurezza o favorirne la promozione.

Gli Stati membri dovrebbero adottare, nell'ambito delle **rispettive strategie nazionali nel settore della cibersicurezza, misure specifiche finalizzate a mitigare la carenza di competenze in materia di cibersicurezza**[80], individuando e incanalando meglio gli sforzi per colmare il divario di competenze e, in ultima analisi, garantendo un'adeguata attuazione degli obblighi previsti dalla direttiva NIS 2.

Alcuni Stati membri sfruttano le **sinergie tra le iniziative civili, di difesa e di contrasto**, creando ad esempio forza lavoro tramite il ricorso al servizio militare obbligatorio nazionale o impiegando riservisti esperti di cibersicurezza, ossia cittadini aventi una formazione militare che occupano posizioni nel settore della cibersicurezza all'interno delle forze armate[81], al fine di consentire alla popolazione, e in particolare ai giovani adulti, di migliorare le proprie competenze in materia di cibersicurezza e ciberdifesa. Lo stesso vale nell'ambito della **lotta alla criminalità informatica**, poiché esistono molte analogie tra le iniziative intraprese in generale nel campo della cibersicurezza e le attività svolte dalle autorità di contrasto in risposta agli incidenti di cibersicurezza. La Commissione incoraggia gli Stati membri a discutere tra loro su tali iniziative e li invita a valutare in che modo una forza lavoro qualificata possa servire al meglio le comunità di cibersicurezza sia di difesa che civili.

---

[77] Nuovi partenariati europei avviati per realizzare le ambizioni dell'UE per il decennio digitale | Plasmare il futuro digitale dell'Europa (europa.eu). I partenariati sono stati costituiti nell'ambito del patto per le competenze al fine di affrontare la carenza di tecnologie dell'informazione e della comunicazione (TIC).

[78] I paesi dell'UE si impegnano a stimolare la partecipazione delle donne al digitale |Plasmare il futuro digitale dell'Europa (europa.eu).

[79] Regolamento (UE) 2021/1057 del Parlamento europeo e del Consiglio, del 24 giugno 2021, che istituisce il Fondo sociale europeo Plus (FSE+) e che abroga il regolamento (UE) n. 1296/2013, articolo 4, paragrafo 1, lettera c).

[80] Direttiva NIS 2, articolo 7, paragrafo 2, lettera f).

[81] Relazione - *Cyber Conscription*: *Experience and Best Practice from Selected Countries*, Martin Hurt e Tiia Sõmer, Centro internazionale per la difesa e la sicurezza, febbraio 2021.

La Commissione rifletterà sulle proposte relative alle modalità per colmare i divari attuali e previsti, individuati nel corso del riesame delle esigenze di istituzioni, organi e organismi dell'Unione. In particolare incoraggerà il personale a usufruire della futura **borsa di studio in materia di cibersicurezza promossa dall'UE e dagli Stati Uniti** e istituita nell'ambito del dialogo UE-USA.

Azioni nell'ambito dell'Accademia

Industria

- Proporre **impegni** specifici **in materia di cibersicurezza** sulla piattaforma per le competenze e le occupazioni digitali a partire dal 18 aprile 2023.

Stati membri

- Includere nelle **strategie nazionali di cibersicurezza** misure specifiche volte a colmare il divario di competenze in materia di cibersicurezza.

Stati membri e industria

- Entro il 2030 attuare la dichiarazione di impegno sulle donne nel digitale e garantire la **convergenza di genere nei posti di lavoro del settore della cibersicurezza**.

6. Finanziamento: creare sinergie per massimizzare l'impatto della spesa destinata allo sviluppo delle competenze in materia di cibersicurezza

Nell'ambito dell'Accademia l'impatto degli investimenti nelle competenze in materia di cibersicurezza sarà massimizzato attraverso la creazione di un punto di accesso comune, un migliore indirizzamento dei fondi in funzione delle esigenze del mercato e un migliore uso dei finanziamenti, promuovendo sinergie tra i diversi strumenti ed evitando nel contempo la duplicazione degli sforzi[82].

6.1. Corrispondenza tra i fondi e le esigenze

Nell'ambito dell'Accademia l'ECCC, con il sostegno della Commissione, del progetto ECCO e dei CNC, raccoglierà **informazioni sull'utilizzo dei fondi dell'UE per finanziare le competenze in materia di cibersicurezza** e valuterà il sostegno fornito da tali fondi per ridurre il divario di competenze in materia di cibersicurezza. Prendendo in considerazione queste informazioni aggregate l'ECCC cercherà di garantire un migliore indirizzamento dei fondi dell'UE in funzione delle esigenze individuate. Finanzierà inoltre azioni volte ad affrontare le lacune più urgenti nella forza lavoro del settore della cibersicurezza, comprese quelle relative alle esigenze connesse all'attuazione della politica in materia di cibersicurezza.

6.2. Garantire visibilità ai fondi disponibili e alle iniziative di partenariato per le competenze in materia di cibersicurezza

A breve termine la **piattaforma per le competenze e le occupazioni digitali** diventerà, per i portatori di interessi, il punto di accesso unico a tutte le informazioni sulle opportunità di finanziamento destinate allo sviluppo delle competenze in materia di cibersicurezza.

[82] Opportunità di finanziamento (europa.eu). I servizi di supporto del patto per le competenze forniscono un punto di accesso unico alle informazioni sui finanziamenti destinati allo sviluppo delle competenze, anche per quanto riguarda l'ecosistema digitale. I servizi di supporto del patto forniscono informazioni generiche sugli strumenti di finanziamento che non si focalizzano specificamente sulle competenze in materia di cibersicurezza, ma il loro lavoro dovrebbe essere preso in considerazione dall'Accademia per evitare duplicazioni.

L'UE sta investendo nelle persone e nello sviluppo delle loro competenze e, tramite i partenariati, in particolare quelli con l'industria, sta promuovendo interventi a favore del miglioramento delle competenze e della riqualificazione professionale attraverso diversi strumenti individuati nell'ambito dell'**agenda europea per le competenze**[83], in particolare il **patto per le competenze**[84] e il **piano d'azione per l'istruzione digitale**[85]. Il **programma Europa digitale** finanzia opportunità per acquisire competenze in materia di cibersicurezza, in particolare tramite iniziative connesse a progetti multinazionali, in chiara complementarità con il sostegno offerto da Orizzonte Europa per la ricerca e le soluzioni tecnologiche innovative in materia di cibersicurezza. Il **Fondo europeo per la difesa**[86] finanzia la ricerca e lo sviluppo tecnologico per condurre operazioni informatiche efficienti, compresi percorsi di formazione ed esercitazioni[87]. **Erasmus+** continuerà a sostenere tali iniziative, anche attraverso programmi intensivi misti e progetti di cooperazione.

Gli Stati membri sono incoraggiati a mobilitare i fondi dell'UE da essi direttamente gestiti per sostenere lo sviluppo delle competenze e la creazione di posti di lavoro nel settore della cibersicurezza. I fondi della politica di coesione, come il **Fondo europeo di sviluppo regionale (FESR)** e il **FSE+**, presentano un importante potenziale in termini di sinergie in tale ambito[88]. Le azioni previste dal **dispositivo per la ripresa e la resilienza** (RRF)[89] e da **InvestEU**[90] includono ulteriori complementarità fondamentali per il conseguimento degli obiettivi stabiliti dall'Accademia.

Azioni nell'ambito dell'Accademia

Centro europeo di competenza per la cibersicurezza e ENISA

- **Mappare** i finanziamenti dell'UE esistenti per le competenze in materia di cibersicurezza confrontandoli alle esigenze del mercato, valutarne l'**efficacia** e individuare **le priorità** di finanziamento entro la fine del 2024.

Commissione

- Creare, entro la fine del 2023, un **punto di accesso unico** per le opportunità di finanziamento relative alle competenze in materia di cibersicurezza sulla piattaforma per le

[83] Agenda europea per le competenze - Occupazione, affari sociali e inclusione - Commissione europea (europa.eu).

[84] Strumenti di finanziamento dell'UE per il miglioramento delle competenze e la riqualificazione professionale - Occupazione, affari sociali e inclusione - Commissione europea (europa.eu).

[85] Piano d'azione per l'istruzione digitale 2021-2027.

[86] Regolamento (UE) 2021/697 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il Fondo europeo per la difesa e abroga il regolamento (UE) 2018/1092.

[87] Gli Stati membri si impegnano a offrire formazioni ed esercitazioni congiunte, ad esempio mediante la definizione di progetti di formazione ed esercitazione in ambito informatico nel quadro della cooperazione strutturata permanente (PESCO), come l'Accademia e polo di innovazione dell'UE nel settore dell'informatica (EU CAIH) e i poligoni virtuali federati, e la partecipazione ad essi.

[88] Regolamento (UE) 2021/1058, articolo 3, paragrafo 1, e regolamento (UE) 2021/1057, articolo 4, paragrafo 1, lettera g).

[89] Ad esempio il piano per la ripresa e la resilienza dell'Estonia prevede investimenti (10 milioni di EUR) sulle competenze digitali e comprenderà la revisione dei percorsi formativi disponibili per gli specialisti nelle TIC e il finanziamento di interventi volti al miglioramento delle competenze e alla riqualificazione degli specialisti nelle TIC in materia di cibersicurezza. Contribuirà inoltre allo sviluppo di un programma pilota finalizzato a ridefinire il quadro delle qualifiche di tali specialisti.

[90] I portatori di interessi (ad esempio, gli erogatori di formazione e le imprese che desiderano definire attività di formazione in materia di cibersicurezza o migliorare quelle già esistenti) possono rivolgersi al polo di consulenza InvestEU, che fornisce sostegno tecnico e assistenza anche per lo sviluppo delle capacità agli sviluppatori di progetti e agli enti, e consultare il portale InvestEU.

competenze e le occupazioni digitali.

7. Misurare i progressi compiuti: responsabilità integrata

Nell'ambito dell'Accademia verrà messa a punto una **metodologia** che consentirà di **misurare i progressi compiuti per colmare il divario di competenze in materia di cibersicurezza**.

7.1. Definire gli indicatori di cibersicurezza per monitorare l'andamento del mercato del lavoro in questo settore

L'**indice di digitalizzazione dell'economia e della società (DESI)** sintetizza gli indicatori relativi alle prestazioni digitali dell'Europa e segue i progressi degli Stati membri dell'UE. Nell'ambito dell'Accademia per le competenze in materia di cibersicurezza, l'ENISA, in collaborazione con la Commissione e il gruppo di cooperazione NIS[91], svilupperà degli **indicatori**, anche in relazione al genere, per monitorare i progressi compiuti negli Stati membri dell'UE per incrementare il numero di professionisti nel campo della cibersicurezza, consultando anche gli operatori di mercato pertinenti e i CNC. L'ENISA si baserà sulla metodologia DESI[92] e provvederà affinché gli indicatori siano in linea con gli obiettivi digitali europei riguardanti i professionisti delle TIC e il conseguimento della convergenza di genere nelle TIC. La Commissione si adopererà quindi per integrare tali indicatori nel DESI, consentendo così di monitorare annualmente lo stato delle competenze e del mercato del lavoro nel settore della cibersicurezza.

7.2. Raccolta dei dati e comunicazione

L'ENISA raccoglierà i dati sugli indicatori con il sostegno del progetto ECCO e dei CNC. Sulla base dei dati raccolti, l'ENISA produrrà una **relazione annuale** che contribuirà alla relazione sullo stato del decennio digitale[93], la quale, unitamente al DESI, integrerà ulteriormente l'analisi e le raccomandazioni specifiche per paese del **semestre europeo**[94]. Gli indicatori sulle competenze in materia di cibersicurezza contribuiranno inoltre all'elaborazione della **relazione biennale** dell'ENISA sullo stato della cibersicurezza nell'UE prevista dalla direttiva NIS 2, che riguarda le capacità, la consapevolezza e l'igiene in materia di cibersicurezza nell'UE.

7.3. Preparazione degli indicatori chiave di prestazione (ICP) per la cibersicurezza

Al fine di colmare il divario di talenti nel settore della cibersicurezza in Europa, l' ENISA, in stretta collaborazione con la Commissione e i CNC, proporrà alla Commissione degli indicatori chiave di prestazione, basandosi sulla metodologia del programma strategico per il decennio digitale 2030, nonché sull'esperienza del settore. L'ENISA terrà in debita considerazione gli indicatori chiave di prestazione utilizzati dagli Stati membri per valutare le proprie strategie nazionali per la cibersicurezza[95].

---

[91] Sulla base e a integrazione della metodologia che sarà sviluppata dall'ENISA ai fini della relazione biennale dell'Agenzia sullo stato della cibersicurezza nell'Unione, a norma dell'articolo 18, paragrafo 3, della direttiva NIS 2.

[92] Cfr. la nota metodologica dell'indice di digitalizzazione dell'economia e della società (DESI) 2022, disponibile alla pagina Indice di digitalizzazione dell'economia e della società (DESI) |Plasmare il futuro digitale dell'Europa (europa.eu).

[93] Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030.

[94] Ibidem, considerando 25.

[95] Direttiva NIS 2, articolo 7, paragrafo 4.

Azioni nell'ambito dell'Accademia

ENISA

- Preparare **indicatori e ICP** sulle competenze in materia di cibersicurezza entro la fine del 2023.
- **Raccogliere dati** sugli indicatori e riferire in merito; la prima raccolta dati avrà luogo entro il 2025.

Commissione

- Contribuire all'integrazione degli **indicatori sulla cibersicurezza nel DESI** e nella **relazione sullo stato del decennio digitale**.

8. Conclusioni

La presente comunicazione getta le basi per un rinnovamento dell'approccio dell'UE finalizzato a potenziare le competenze in materia di cibersicurezza dei professionisti dell'UE. L'obiettivo è quello di ridurre il divario di competenze in materia di cibersicurezza e di dotare l'UE della forza lavoro necessaria per consentirle di far fronte al panorama delle minacce in costante evoluzione e di attuare le politiche dell'UE volte a proteggere l'Unione dagli attacchi informatici, nonché di incrementare le opportunità commerciali e la competitività. Una forza lavoro qualificata nel campo della cibersicurezza può giovare alle comunità **civile, della difesa, diplomatica e di contrasto**, agevolando la creazione di sinergie tra di esse.

La Commissione invita gli Stati membri e tutti i portatori di interessi a realizzare l'ambizione dell'Accademia per le competenze in materia di cibersicurezza.