KOMISJA
EUROPEJSKA

Strasburg, dnia 18.4.2023 r.
COM(2023) 207 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE („Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa”)

Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE („Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa”)

1. Pilna potrzeba zmniejszenia ryzyka dzięki zlikwidowaniu niedoboru wykwalifikowanej siły roboczej i luk w umiejętnościach w dziedzinie cyberbezpieczeństwa

Cyberbezpieczeństwo to nie tylko element bezpieczeństwa obywateli, przedsiębiorstw i państw członkowskich. To także konieczność zapewnienia stabilności politycznej UE, stabilności jej demokracji oraz dobrobytu naszemu społeczeństwu i naszym przedsiębiorstwom. **Krajobraz zagrożeń** cyberbezpieczeństwa w ostatnich latach uległ znacznym zmianom, a niepokojącą tendencją jest rosnąca liczba cyberataków wymierzonych w wojskową i cywilną infrastrukturę krytyczną w UE. Agresorzy poszerzają swoje możliwości, co prowadzi do nowych, hybrydowych i pojawiających się zagrożeń, takich jak wykorzystywanie botów i technik opartych na sztucznej inteligencji[1]. W szczególności agresorzy stosujący oprogramowanie szantażujące systematycznie wyrządzają podmiotom znaczne szkody, zarówno finansowe, jak i związane z nadszarpnięciem reputacji[2].

Duża liczba cyberincydentów była także wymierzona w administrację publiczną i rządy w państwach członkowskich, jak również w europejskie instytucje, organy i jednostki organizacyjne[3]. Sektor finansowy[4] i sektor zdrowia[5], które to sektory stanowią fundament społeczeństwa i gospodarki, również były celem systematycznych ataków[6]. Napięcia geopolityczne związane z rosyjską wojną napastniczą przeciwko Ukrainie zwiększyły zagrożenie cyberbezpieczeństwa[7] i mogą zdestabilizować nasze społeczeństwo. Nie można zagwarantować **bezpieczeństwa** Unii bez udziału **najcenniejszego zasobu UE: jej obywateli.** UE pilnie potrzebuje specjalistów posiadających odpowiednie umiejętności i kompetencje, aby zapobiegać cyberatakom, wykrywać i powstrzymywać je oraz bronić UE, w tym jej najbardziej krytycznej infrastruktury, przed takimi cyberatakami, oraz zapewnić **odporność Unii**.

---

[1] ENISA Krajobraz zagrożeń 2022 – ENISA (europa.eu).

[2] Europol, „Internet Organised Crime Threat Assessment (IOCTA)” [„Ocena zagrożenia zorganizowaną przestępczością internetową (IOCTA)”], 2021. Działania takich agresorów opierają się na modelu „oprogramowanie szantażujące jako usługa”. Roczne koszty poniesione przez przedsiębiorstwa w 2022 r. w wyniku tych ataków przekroczyły 18,4 mld EUR (sprawozdanie Cybereason z 2022 r. dotyczące rzeczywistych kosztów oprogramowania szantażującego).

[3] Zob. na przykład Wspólna publikacja ENISA i CERT-UE, JP-23-01, „Sustained activity by specific threat actors” [Stałe ataki określonych agresorów], TLP:CLEAR, 15 lutego 2023 r.

[4] Zob. na przykład w Niemczech 90 % oszustw popełnianych za pośrednictwem poczty elektronicznej zgłoszonych od 1 czerwca 2021 r. do 31 maja 2022 r. stanowiły próby wyłudzenia informacji finansowych lub ataki na przedsiębiorstwa w sektorze finansowym, przy czym dotyczyły one ponad 20 000 zainfekowanych urządzeń ze 125 państw, „The State of IT Security in Germany in 2022” [Stan bezpieczeństwa informatycznego w Niemczech w 2022 r.], Bundesamt für Sicherheit in der Informationstechnik (BSI), 1 stycznia 2023 r.

[5] Zob. na przykład we Francji ataki z wykorzystanie oprogramowania szantażującego na placówki publicznej opieki zdrowotnej takie jak Centre Hospitalier Sud Francilien, które doprowadziły do „wycieku” 11 GB danych osobowych i medycznych oraz danych dotyczących personelu, które to dane zostały następnie upublicznione przez agresorów, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d’information (ANSSI), styczeń 2023 r.

[6] ENISA Krajobraz zagrożeń 2022.

[7] Zob. również: CERT-UE – Wojna Rosji z Ukrainą: rok cyberoperacji (europa.eu); Rosyjskie cyberoperacje przeciwko Ukrainie: oświadczenie wysokiego przedstawiciela wydane w imieniu Unii Europejskiej, 10 maja 2022 r.; Oświadczenie wysokiego przedstawiciela w imieniu Unii Europejskiej w sprawie szkodliwych działań w cyberprzestrzeni prowadzonych przez hakerów i grupy hakerów w kontekście rosyjskiej agresji na Ukrainę, 19 lipca 2022 r.

Niedobór talentów w dziedzinie cyberbezpieczeństwa dodatkowo ogranicza **konkurencyjność** i **wzrost gospodarczy** Europy, które w znacznym stopniu zależą od rozwoju i wykorzystania strategicznych technologii cyfrowych (np. sztucznej inteligencji, sieci 5G i chmury). Aby UE mogła nadal dostarczać kluczowe zaawansowane technologie w skali globalnej, potrzebna jest wykwalifikowana siła robocza w sektorze cyberbezpieczeństwa.

Aby przygotować się na ten zmieniający się krajobraz zagrożeń i stawić mu czoła, a także aby zwiększyć konkurencyjność UE, w ostatnich latach nastąpił znaczny postęp w unijnej polityce cyberbezpieczeństwa, co doprowadziło do przyjęcia szeregu inicjatyw, takich jak strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę[8], zmieniona dyrektywa w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywa NIS 2)[9], unijne przepisy sektorowe dotyczące cyberbezpieczeństwa[10], polityka UE w zakresie cyberobrony[11], akt dotyczący cyberodporności[12] oraz akt w sprawie cybersolidarności zaproponowany przez Komisję wraz z niniejszym komunikatem. Nie da się jednak osiągnąć celów tych aktów prawnych bez niezbędnych wykwalifikowanych osób, które będą je wdrażać. Choć w ramach inicjatyw wspierających rozwój ogólnych umiejętności niezbędnych do uczestnictwa w życiu społecznym uwzględnia się upowszechnianie wśród ogółu społeczeństwa podstawowej wiedzy w dziedzinie cyberbezpieczeństwa[13], kompetentna siła robocza ma zasadnicze znaczenie – zarówno w sektorze publicznym, jak i w prywatnym, na poziomie krajowym i unijnym, w tym w organizacjach normalizacyjnych – **aby umożliwić wypełnienie tych prawnych i politycznych wymogów w zakresie cyberbezpieczeństwa.**

Bezpieczeństwo i konkurencyjność UE zależą zatem od obecności wysoko wykwalifikowanej siły roboczej w sektorze cyberbezpieczeństwa. UE stoi jednak w obliczu bardzo dużego niedoboru wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa, co naraża UE, jej państwa członkowskie, przedsiębiorstwa i obywateli na ryzyko wystąpienia cyberincydentów. W 2022 r. niedobór specjalistów w dziedzinie cyberbezpieczeństwa w Unii Europejskiej wynosił **od 260 000**[14] **do 500 000**[15], podczas gdy zapotrzebowanie na siłę roboczą w sektorze cyberbezpieczeństwa w UE szacowano na 883

[8] Wspólny komunikat do Parlamentu Europejskiego i Rady „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę", JOIN(2020) 18 final.

[9] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

[10] Na przykład w sektorze finansowym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (rozporządzenie DORA).

[11] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

[12] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020, COM(2022) 454 final.

[13] Wśród istotnych inicjatyw dotyczących rozwoju ogólnych umiejętności cyfrowych społeczeństwa można wymienić: Plan działania na rzecz Europejskiego filaru praw socjalnych oraz cyfrowy kompas (a zwłaszcza zapisany w nich cel, zgodnie z którym 80 % populacji ma nabyć podstawowe umiejętności cyfrowe do 2030 r.), Plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027, ramy kompetencji cyfrowych dla obywateli lub wniosek dotyczący zalecenia Rady w sprawie poprawy oferty kształcenia i szkolenia w zakresie umiejętności cyfrowych.

[14] (ISC)² w webinarium ENISA, Assessing Cyber Skills on the basis of the ECSF [Ocena umiejętności w dziedzinie cyberbezpieczeństwa na podstawie europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa], 16 lutego 2023 r.

[15] Według Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO), jak stwierdzono we wspólnym komunikacie do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

000 specjalistów[16], co świadczy o braku równowagi między dostępnymi kompetencjami a tymi potrzebnymi na rynku pracy. Do niedoboru siły roboczej w sektorze cyberbezpieczeństwa przyczynia się również to, że dziedzina ta jest błędnie kojarzona ze specjalizacją techniczną, przez co wciąż nie udaje się przyciągnąć do tego sektora **kobiet**, które stanowią 20 % absolwentów kierunków związanych z cyberbezpieczeństwem[17] i 19 % specjalistów ds. technologii informacyjno-komunikacyjnych (ICT)[18]. Aby temu zaradzić, w europejskim **programie polityki „Droga ku cyfrowej dekadzie" do 2030 r.**[19] wyznaczono cel, jakim jest zwiększenie do 2030 r. liczby specjalistów w dziedzinie ICT do 20 mln, przy jednoczesnym osiągnięciu równowagi między płciami. Ponadto wdrażanie pojawiających się unijnych strategii politycznych wymaga odpowiednio wykwalifikowanej i wystarczająco licznej siły roboczej. Przykładowo ponad 42 % kierowników wyższego szczebla ds. IT w branży usług finansowych podkreśliło, że brak umiejętności i wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa stanowi kluczowe wyzwanie, z jakim zmaga się ich przedsiębiorstwo, jeśli chodzi o obronę w obszarze cyberbezpieczeństwa i zarządzanie incydentami[20], i to w momencie, gdy czeka ich obowiązkowe wdrożenie sektorowych przepisów dotyczących cyberbezpieczeństwa, takich jak akt w sprawie operacyjnej odporności cyfrowej (rozporządzenie DORA).

Do ograniczenia rynku pracy dodatkowo przyczynia się fakt, że pracodawcy niechętnie inwestują w kapitał ludzki, a poszukują natomiast już wyszkolonych i doświadczonych specjalistów[21]. Niedobór ten wpływa negatywnie na wszystkie rodzaje przedsiębiorstw, w tym na małe i średnie przedsiębiorstwa (**MŚP**), które stanowią 99 % wszystkich przedsiębiorstw w UE[22]. Duże wyzwanie stoi także przed **administracjami publicznymi**, które często stają się celem cyberincydentów i najbardziej odczuwają ich skutki[23].

Wyeliminowanie niedoboru utalentowanych specjalistów w dziedzinie cyberbezpieczeństwa w UE wymaga zatem pilnych działań, ponieważ stawką są bezpieczeństwo i konkurencyjność UE.

2. Brak synergii i skoordynowanych działań zmierzających do zniwelowania luki w umiejętnościach w dziedzinie cyberbezpieczeństwa

Na poziomie europejskim i krajowym podmioty publiczne i prywatne realizują szeroką gamę inicjatyw mających na celu rozwiązanie problemu niedoborów na rynku pracy w sektorze cyberbezpieczeństwa. Są one jednak rozproszone i jak dotąd nie udało im się osiągnąć masy krytycznej, aby faktycznie zmienić istniejącą sytuację.

Przede wszystkim brakuje obecnie pełnego powszechnego zrozumienia struktury siły roboczej w sektorze cyberbezpieczeństwa w UE i związanych z tym umiejętności, podczas

[16] (ISC)² w webinarium ENISA, Assessing Cyber Skills on the basis of the ECSF [Ocena umiejętności w dziedzinie cyberbezpieczeństwa na podstawie europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa], 16 lutego 2023 r.

[17] Baza danych szkolnictwa wyższego w zakresie cyberbezpieczeństwa (CyberHEAD).

[18] Kobiety stanowią zaledwie 19 % specjalistów w dziedzinie ICT w UE – Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) 2022 | Kształtowanie cyfrowej przyszłości Europy (europa.eu). Nie ma dostępnych danych liczbowych dotyczących kobiet zatrudnionych w sektorze cyberbezpieczeństwa w Unii.

[19] Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r., na mocy której utworzono mechanizm monitorowania i współpracy służący osiągnięciu wspólnych celów na drodze do transformacji cyfrowej Europy, jak określono w cyfrowym kompasie na 2030 r., w tym w obszarze umiejętności.

[20] Raport S-RM dotyczący cyberbezpieczeństwa za 2022 r.

[21] ENISA, Rozwój umiejętności w dziedzinie cyberbezpieczeństwa w UE, grudzień 2019 r.

[22] Definicja MŚP (europa.eu)

[23] ENISA Krajobraz zagrożeń 2022 – ENISA (europa.eu).

gdy podobne profile zawodowe w dziedzinie cyberbezpieczeństwa powinny wiązać się z takim samym zestawem umiejętności. Niski poziom korzystania przez właściwe podmioty ze wspólnych **europejskich ram odniesienia dotyczących specjalistów w dziedzinie cyberbezpieczeństwa** przekłada się na brak narzędzia, które umożliwiłoby wymianę informacji między pracodawcami, dydaktykami i decydentami, oraz powoduje niezdolność do prowadzenia pomiarów i oceny luk na rynku pracy w sektorze cyberbezpieczeństwa. Ponadto uniemożliwia to opracowywanie programów kształcenia i szkolenia oraz tworzenie ścieżek kariery odpowiadających potrzebom polityki i rynku dla osób zainteresowanych wykonywaniem tego zawodu. **Podnoszenie i zmiana kwalifikacji** siły roboczej opiera się w dużej mierze na szkoleniach i certyfikacji w zakresie cyberbezpieczeństwa, zwykle oferowanych przez prywatnych organizatorów. Zainteresowane osoby mają jednak trudności z uzyskaniem informacji na temat jakości oferowanych szkoleń w zakresie cyberbezpieczeństwa i wydawanych w związku z nimi certyfikatów.

Choć kształcenie i szkolenie oraz tworzenie ścieżek kariery są niezbędne do wzmocnienia strony podażowej rynku pracy, obecnie niedoceniana jest rola **strony popytowej** w szkoleniu własnej siły roboczej i dostosowywaniu się do zmian w tym względzie. Pracodawcom z sektora przemysłu i sektora publicznego brakuje wspólnych forów i miejsc, gdzie mogliby dzielić się pomysłami na temat tego, jak najlepiej szkolić siłę roboczą i jak **lepiej oceniać umiejętności**, zwłaszcza w procesie rekrutacji. Najbardziej pożądane **umiejętności twarde** mogą być związane z cyberbezpieczeństwem[24], jak np. tworzenie oprogramowania lub przetwarzanie w chmurze[25], ale **umiejętności przekrojowe** są nadal niesłusznie lekceważone. Myślenie krytyczne i umiejętność analizowania, rozwiązywanie problemów i samozarządzanie to grupy umiejętności, które są coraz bardziej pożądane przez pracodawców[26] i zyskują na znaczeniu w perspektywie 2025 r.[27]

Istnieje już wiele inicjatyw w zakresie inwestycji publicznych i prywatnych związanych z umiejętnościami w dziedzinie cyberbezpieczeństwa, a UE oferuje znaczne **finansowanie** projektów w ramach różnych instrumentów[28]. Utrzymujący się niedobór umiejętności w UE budzi jednak wątpliwości co do widoczności i wpływu tych inicjatyw oraz sugeruje, że mogą one nie odpowiadać w ujęciu systemowym potrzebom rynku, które należy pilnie określić na poziomie UE. Ponadto istnienie kilku źródeł finansowania prowadzi do powielania działań, przez co traci się możliwość zwiększenia skali i wywarcia rzeczywistego wpływu. Co więcej, osoby, które potrzebują inwestycji, nie zawsze potrafią ustalić źródła najbardziej odpowiadające ich potrzebom.

Zainteresowane strony próbują rozwiązać złożony i wieloaspektowy problem niedoboru umiejętności w dziedzinie cyberbezpieczeństwa. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) opracowuje instrumenty związane z profilami ról czy szkolnictwem wyższym[29], Europejskie Centrum Kompetencji w dziedzinie

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most [Najbardziej pożądane umiejętności w 2023 r.: dowiedz się, jakich umiejętności najczęściej szukają pracodawcy].

[25] ISACA, infografika „Stan cyberbezpieczeństwa w 2022 r.”.

[26] Np. narzędzie Cedefop: Skills-OVATE | Cedefop (europa.eu).

[27] Sprawozdawanie Światowego Forum Ekonomicznego na temat przyszłości miejsc pracy, październik 2020 r.

[28] Na przykład: Sojusz na rzecz umiejętności w dziedzinie cyberbezpieczeństwa – nowa wizja dla Europy – projekt REWIRE (finansowany z programu Erasmus+); projekty wspierające Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (finansowane z programu „Horyzont 2020”), projekt Cybersecpro (finansowany z programu „Cyfrowa Europa”)).

[29] W szczególności: europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa; CyberHEAD – baza danych szkolnictwa wyższego w zakresie cyberbezpieczeństwa; platforma ćwiczeń w zakresie cyberbezpieczeństwa (CEP); europejskie wyzwanie dotyczące cyberbezpieczeństwa; Europejski Miesiąc Cyberbezpieczeństwa.

Cyberbezpieczeństwa (ECCC)[30] zajmuje się umiejętnościami w dziedzinie cyberbezpieczeństwa w ramach specjalnej grupy roboczej, Europejskie Kolegium Bezpieczeństwa i Obrony (EKBiO) pracuje nad umiejętnościami w dziedzinie cyberbezpieczeństwa wśród cywilnej i wojskowej siły roboczej w kontekście wspólnej polityki bezpieczeństwa i obrony[31], również organizacje prywatne starają się rozwiązać omawiany problem[32], branża certyfikacji cyberbezpieczeństwa opracowuje plan działania i szkolenia ukierunkowane na wyeliminowanie niedoboru kwalifikacji[33]. Państwa członkowskie także próbują rozwiązać ten problem za pomocą różnych inicjatyw, od inicjatyw regulacyjnych[34] po inicjatywy zakładające tworzenie akademii umiejętności w dziedzinie cyberbezpieczeństwa[35], cyberkampusów[36] lub centrów doskonałości zajmujących się cyberprzestępczością[37], czy też w ramach partnerstw publiczno-prywatnych[38]. W pracach wszystkich tych zainteresowanych stron często brakuje jednak koordynacji i synergii, przez co nie osiągnęły one pełni potencjału, który pozwoliłby im w znacznym stopniu zmienić sytuację na rynku pracy, czego dowodem jest rosnący niedobór siły roboczej w sektorze cyberbezpieczeństwa w UE. Konieczne jest również zwiększenie synergii między społecznościami zajmującymi się cyberbezpieczeństwem, ponieważ zestawy umiejętności niezbędne do utrzymania cyberbezpieczeństwa, zwalczania **cyberprzestępczości** lub budowania **cyberobrony** mają często podobny charakter.

Ponadto UE ma obecnie ograniczone możliwości oceny **stanu i rozwoju rynku pracy w sektorze cyberbezpieczeństwa** oraz umiejętności, jakimi dysponują pracownicy w tym sektorze. Państwa członkowskie oraz europejskie instytucje, organy i jednostki organizacyjne opierają się na danych na temat specjalistów w dziedzinie ICT gromadzonych przez podmioty prywatne albo na szerszym zestawie danych na ten temat gromadzonych przez UE, w szczególności przez Eurostat[39] i Europejskie Centrum Rozwoju Kształcenia Zawodowego (Cedefop)[40]. Innymi słowy, UE ma tylko częściowy i fragmentaryczny obraz potrzeb w tym względzie, co uniemożliwia uzyskanie kompleksowego oglądu stanu rynku pracy w sektorze cyberbezpieczeństwa.

3. Skoordynowana reakcja w skali UE: Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa

3.1.Cel

Aby sprostać wyzwaniu związanemu z rozwojem umiejętności w dziedzinie cyberbezpieczeństwa i zniwelować lukę na rynku pracy, Komisja proponuje utworzenie

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji.

[31] W szczególności platforma kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa (ETEE).

[32] Na przykład grupa robocza 5 Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO) ds. „Edukacji, szkolenia, świadomości, cyberpoligonów, czynników ludzkich"; organizacja DIGITALEUROPE.

[33] Na przykład SANS Institute, (ISC)², ISACA.

[34] Na przykład w ramach strategii krajowych na rzecz edukacji lub cyberbezpieczeństwa.

[35] Na przykład C-Academy w Portugalii.

[36] Na przykład cyberkampusy we Francji.

[37] Na przykład litewskie centrum doskonałości zajmujące się szkoleniami, badaniem i edukacją w dziedzinie cyberprzestępczości (L3CE).

[38] Na przykład inicjatywa Microsoftu dotycząca umiejętności w dziedzinie cyberbezpieczeństwa.

[39] Zatrudnienie wśród specjalistów w dziedzinie ICT – Statistics Explained (europa.eu)

[40] Np. narzędzie Cedefop: Skills-OVATE | Cedefop (europa.eu).

Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa, zgodnie z zapowiedzią przewodniczącej Komisji Europejskiej zawartą w liście intencyjnym dołączonym do orędzia o stanie Unii z 2022 r.[41,, 42] oraz w kontekście Europejskiego Roku Umiejętności.

Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa (w skrócie „Akademia") ma stanowić **pojedynczy punktu dostępu i synergii** na potrzeby oferty edukacyjnej i szkoleniowej w dziedzinie cyberbezpieczeństwa, a także możliwości finansowania i konkretnych działań wspierających rozwój umiejętności w dziedzinie cyberbezpieczeństwa. Umożliwi ona zwiększanie skali inicjatyw realizowanych przez zainteresowane strony i pozwoli osiągnąć masę krytyczną, która spowoduje pozytywne zmiany na rynku pracy, w tym z korzyścią dla sektora obronnego. Działania te byłyby dostosowane do wspólnych celów i kluczowych wskaźników wydajności, co pozwoliłoby na uzyskanie większego wpływu.

Akademia będzie ukierunkowana na zdobywanie umiejętności przez **specjalistów w dziedzinie cyberbezpieczeństwa**. Działalność Akademii będzie stanowić wkład w politykę UE w zakresie cyberbezpieczeństwa, a także w edukację i uczenie się przez całe życie. Stanowi ona uzupełnienie dwóch zaleceń Rady dotyczących edukacji i umiejętności cyfrowych, które są przedmiotem wniosków Komisji i które Komisja przedstawia w tym samym czasie co niniejszy komunikat[43].

Akademia będzie się opierać na czterech filarach: 1) wspieranie **generowania wiedzy za pomocą kształcenia i szkolenia** dzięki opracowaniu wspólnych ram dotyczących profili ról w sektorze cyberbezpieczeństwa i powiązanych umiejętności, wzbogaceniu europejskiej oferty kształcenia i szkolenia w celu zaspokojenia potrzeb, tworzeniu ścieżek kariery oraz zapewnieniu widoczności i przejrzystości szkoleń i certyfikacji w zakresie cyberbezpieczeństwa w celu wzmocnienia strony podażowej rynku pracy; 2) zapewnienie lepszego ukierunkowania i lepszej widoczności dostępnych **możliwości finansowania** działań związanych z umiejętnościami, aby zmaksymalizować ich wpływ; 3) zachęcanie zainteresowanych stron **do podejmowania działań** oraz 4) określenie wskaźników **umożliwiających monitorowanie zmian na rynku** oraz ocenę skuteczności podejmowanych działań.

Akademia powstanie dzięki dofinansowaniu w wysokości 10 mln EUR z programu „Cyfrowa Europa"[44].

3.2.Zarządzanie Akademią

Aby zapewnić infrastrukturę, która posłuży jako **pojedynczy punkt dostępu** sprzyjający współpracy między środowiskiem akademickim, organizatorami szkoleń i przedstawicielami przemysłu, w ramach której mogłyby się spotykać i szkolić strona podażowa i strona popytowa unijnego ekosystemu cyberbezpieczeństwa, Akademia mogłaby przyjąć formę **konsorcjum na rzecz europejskiej infrastruktury cyfrowej (EDIC)**[45]. Instrument ten umożliwiłby państwom członkowskim wspólne działania na rzecz zniwelowania luki

[41] Orędzie o stanie Unii – list intencyjny do przewodniczącej Roberty Metsoli i do premiera Petra Fiali z 2022 r.

[42] Wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

[43] Wnioski dotyczące zaleceń Rady w sprawie kluczowych czynników sprzyjających skuteczności kształcenia i szkolenia cyfrowego oraz w sprawie poprawy oferty kształcenia i szkolenia w zakresie umiejętności cyfrowych.

[44] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240.

[45] Możliwość ustanawiania EDIC przewidziano w art. 13 i nast. decyzji Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiającej program polityki „Droga ku cyfrowej dekadzie" do 2030 r.

w umiejętnościach w dziedzinie cyberbezpieczeństwa, a także ścisłą współpracę z Komisją, ENISA i Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), zgodnie z ich mandatami i kompetencjami, oraz włączenie w te działania wszystkich odpowiednich zainteresowanych stron, a także ukierunkowanie europejskich, krajowych i prywatnych inwestycji na realizację wspólnego celu. W związku z tym zachęca się zainteresowane państwa członkowskie do wstępnego powiadomienia Komisji do 30 maja 2023 r. o swoim zamiarze przystąpienia do przyszłego wniosku o utworzenie takiego EDIC. To dobrowolne wstępne powiadomienie pozwoliłoby Komisji na wczesne przedstawienie uwag na temat projektu wniosku o utworzenie EDIC, co umożliwi szybsze dopracowanie i formalne złożenie wniosku. Podczas całego procesu i w zakresie, w jakim zwrócą się o to państwa członkowskie, Komisja, działając jako akcelerator projektów wielokrajowych, będzie ułatwiać przygotowanie wniosku o utworzenie EDIC. W kolejnym kroku, po pozytywnej ocenie wniosku przez Komisję i zatwierdzeniu go przez Komitet ds. programu polityki „Droga ku cyfrowej dekadzie" do 2030 r., Komisja wyda decyzję w sprawie ustanowienia EDIC, a następnie pomoże w koordynowaniu procesu tworzenia EDIC[46].

W międzyczasie i w okresie formalnego tworzenia EDIC Komisja utworzy wirtualny pojedynczy punkt dostępu w drodze rozbudowy **platformy Komisji na rzecz umiejętności cyfrowych i zatrudnienia**[47] przy wsparciu ze strony projektu wsparcia europejskich społeczności zajmujących się cyberbezpieczeństwem (ECCO)[48].

ENISA będzie wspierać wdrożenie Akademii zgodnie z celami agencji[49], szczególnie w zakresie pomocy w kształceniu i szkoleniu w dziedzinie cyberbezpieczeństwa, a także z uwzględnieniem swoich obowiązków w zakresie zgłaszania incydentów wynikających z dyrektywy NIS 2[50]. Również **ECCC** będzie działać zgodnie ze swoim strategicznym programem działań w celu wspierania wdrożenia Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. W szczególności ECCC będzie realizować strategiczny cel nr 3 (cyberbezpieczeństwo) programu „Cyfrowa Europa". Będzie przy tym korzystać ze wsparcia Komisji i państw członkowskich za pośrednictwem **Krajowych Ośrodków Koordynacji (NCC)**. W stosownych przypadkach **Grupa Współpracy** ustanowiona w dyrektywie NIS 2[51] będzie proszona o pomoc. Ponadto do osiągnięcia celu Akademii, jakim jest zniwelowanie luki w umiejętnościach w dziedzinie cyberbezpieczeństwa, niezbędne będzie połączenie sił z **przemysłem** i **środowiskiem akademickim**.

4. Generowanie wiedzy i szkolenie: ustanowienie wspólnego unijnego podejścia do szkolenia w zakresie cyberbezpieczeństwa

[46] Ibidem, art. 12.

[47] Home | Platforma na rzecz umiejętności cyfrowych i zatrudnienia (europa.eu)

[48] Zob. Europejskie Centrum i Sieć Kompetencji w dziedzinie Cyberbezpieczeństwa: nowy projekt finansowany przez UE na rzecz wsparcia społeczności zajmującej się cyberbezpieczeństwem (europa.eu). W grudniu 2022 r. Komisja Europejska podpisała umowę o wartości 3 mln EUR dotyczącą wsparcia unijnej społeczności zajmującej się cyberbezpieczeństwem w ramach Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa. Projekt ten przyczyni się do osiągnięcia unijnych celów w zakresie tworzenia społeczności i budowania zdolności w zakresie badań, innowacji, wykorzystania rozwiązań i bazy przemysłowej w dziedzinie cyberbezpieczeństwa.

[49] „ENISA wspiera budowanie potencjału i gotowości w całej Unii, pomagając instytucjom, organom i jednostkom organizacyjnym Unii, jak również państwom członkowskim oraz interesariuszom z sektora publicznego i prywatnego [...] w rozwijaniu umiejętności i kompetencji w dziedzinie cyberbezpieczeństwa" – art. 4 ust. 3 aktu o cyberbezpieczeństwie.

[50] Art. 18 dyrektywy NIS 2.

[51] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

W ramach filaru Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa dotyczącego generowania wiedzy i szkolenia wypracowane zostanie uporządkowane podejście, którego celem będzie zwiększenie **liczby** osób mających umiejętności w dziedzinie cyberbezpieczeństwa w UE, lepsze ukierunkowanie szkoleń na **potrzeby rynku** oraz zapewnienie widoczności **ścieżek kariery**.

4.1. Wspólny język: wspólne podejście do profili ról w sektorze cyberbezpieczeństwa i powiązanych umiejętności

ENISA prowadzi już prace nad określeniem profili ról specjalistów w dziedzinie cyberbezpieczeństwa w ramach **europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa**[52]. Ramy te powinny stanowić dla Akademii podstawę, na której określi ona i oceni odpowiednie umiejętności, będzie monitorować rozwój sytuacji w odniesieniu do niedoboru wykwalifikowanej siły roboczej i dostarczy wskazówek dotyczących nowych potrzeb. W odniesieniu do każdej roli z zakresu cyberbezpieczeństwa przewidzianej w europejskich ramach umiejętności w dziedzinie cyberbezpieczeństwa zestaw odpowiednich kompetencji z europejskich ram e-kompetencji[53] zawarto jako element opisu danego profilu[54].

W związku z tym ENISA dokona przeglądu europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa i **określi zmieniające się potrzeby i luki w tym zakresie** w odniesieniu do siły roboczej w sektorze cyberbezpieczeństwa, w tym za pomocą zaawansowanych narzędzi (np. sztucznej inteligencji, dużych zbiorów danych[55], eksploracji danych). W tym celu ENISA będzie prowadzić prace pod kierownictwem EDIC (gdy to konsorcjum zostanie ustanowione) oraz ECCC, wraz z NCC, Komisją, projektem ECCO i uczestnikami rynku[56]. W przypadku siły roboczej w dziedzinie cyberobrony ENISA należycie uwzględni prace wykonane przez EKBiO. Podobnie w obszarze zwalczania cyberprzestępczości ENISA uwzględni działania prowadzone przez Agencję Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (CEPOL) i Europol w celu opracowania analizy potrzeb w zakresie szkolenia operacyjnego[57] w dziedzinie cyberataków.

Europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa będą regularnie uzupełniane i poddawane przeglądowi w ramach Akademii w cyklu dwuletnim. Ponadto Komisja i Europejska Służba Działań Zewnętrznych pomogą w określaniu konkretnych

[52] Europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa – ENISA (europa.eu). Europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa pomagają w określaniu i formułowaniu zadań, kompetencji, umiejętności i wiedzy związanych z rolami europejskich specjalistów w dziedzinie cyberbezpieczeństwa. Podsumowują wszystkie role związane z cyberbezpieczeństwem w formie profili, które są indywidualnie analizowane pod kątem szczegółowych elementów odpowiadających im obowiązków, umiejętności, synergii i współzależności.

[53] Europejskie ramy e-kompetencji (e-CF) | ESCO (europa.eu). e-CF zapewniają spójne połączenia w kontekście kwalifikacji w dziedzinie ICT i innych ram istotnych dla tego sektora, w tym ram kompetencji cyfrowych dla obywateli.

[54] Zob. w tym względzie Podręcznik użytkownika – europejskie ramy umiejętności w dziedzinie cyberbezpieczeństwa – wrzesień 2022 r..

[55] Zob. na przykład narzędzie Skills-OVATE opracowane przez Cedefop.

[56] Agencja będzie ponadto korzystać z wyników innych projektów finansowanych przez UE (np. REWIRE, przestrzeń danych dotyczących umiejętności (DS4S), CyberSecPro, Concordia) i metod stosowanych w podobnych inicjatywach (np. „Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States" – sprawozdanie OECD opublikowane 21 marca 2023 r.) w celu zapewnienia w przyszłości aktualnej wizji potrzeb w środowisku, w którym zapotrzebowanie stale się zmienia.

[57] Ocena potrzeb w zakresie szkolenia operacyjnego CEPOL

profili i powiązanych umiejętności dla poszczególnych sektorów, w zależności od potrzeb, przy wsparciu agencji i organów UE, takich jak EKBiO[58], Europol i CEPOL[59].

Zostaną również utworzone powiązania między europejskimi ramami umiejętności w dziedzinie cyberbezpieczeństwa a odpowiednimi instrumentami unijnej polityki zatrudnienia[60]. W szczególności określone w europejskich ramach umiejętności w dziedzinie cyberbezpieczeństwa profile zawodowe oraz powiązane umiejętności zostaną włączone do **europejskiej klasyfikacji umiejętności, kompetencji, kwalifikacji i zawodów**. Poprawi to klasyfikację i powiązania między zawodami i umiejętnościami w dziedzinie cyberbezpieczeństwa, co ułatwi pracownikom podnoszenie i zmianę kwalifikacji oraz wspomoże oparte na umiejętnościach kojarzenie ofert pracy z poszukującymi zatrudnienia i mobilność transgraniczną.

4.2. Rozwijanie współpracy w celu opracowania programów kształcenia i szkolenia w dziedzinie cyberbezpieczeństwa

Po ustanowieniu EDIC Akademia powinna otrzymać wsparcie od państw członkowskich, które pozwoli jej stać się **miejscem odniesienia w Europie w zakresie opracowywania i oferowania szkoleń w zakresie cyberbezpieczeństwa**, które dotyczą najbardziej pożądanych umiejętności, oraz zapewniać możliwości szkoleń w miejscu pracy i staży dla przedsiębiorstw typu start-up i MŚP oraz dla administracji publicznych w innowacyjnych przedsiębiorstwach w sektorze cyberbezpieczeństwa i centrach kompetencji w dziedzinie cyberbezpieczeństwa. W celu opracowania takich szkoleń EDIC powinno współpracować ze wszystkimi zainteresowanymi stronami, w tym z przedstawicielami przemysłu, a także opierać się na projektach takich jak finansowany z programu „Cyfrowa Europa" **CyberSecPro**[61], w którym uczestniczy 17 instytucji szkolnictwa wyższego i 13 przedsiębiorstw zajmujących się bezpieczeństwem z 16 państw członkowskich, aby oferować najlepsze praktyki w odniesieniu do wszystkich programów szkoleniowych w zakresie cyberbezpieczeństwa.

Akademia będzie współpracować ze wszystkimi zainteresowanymi stronami, aby **zachęcić młode pokolenia** do podjęcia pracy w sektorze cyberbezpieczeństwa. Zgodnie z wnioskiem dotyczącym zalecenia Rady w sprawie poprawy oferty kształcenia i szkolenia w zakresie umiejętności cyfrowych państwa członkowskie powinny ustanowić i udoskonalić środki mające na celu rekrutację i szkolenie wyspecjalizowanych nauczycieli i instruktorów oraz ułatwić nabywanie umiejętności w dziedzinie cyberbezpieczeństwa, w tym poprzez praktyki zawodowe. Należy zachęcać do włączania cyberbezpieczeństwa do programów kształcenia i szkolenia, przy jednoczesnym zapewnieniu ich dostępności, rozwijaniu oferty **praktyk zawodowych** i staży, wspieraniu innowacyjnych podejść, w tym np. gier poważnych i wspólnych platform do symulacji, organizowaniu tygodni immersji w zawodach

[58] Zob. w tym względzie wspólny komunikat do Parlamentu Europejskiego i Rady „Polityka UE w zakresie cyberobrony", JOIN(2022) 49 final.

[59] W tym względzie szczególna uwaga zostanie poświęcona trwającym obecnie pracom nad ramami kompetencji szkoleniowych w dziedzinie cyberprzestępczości (TCF).

[60] Takimi jak europejska klasyfikacja umiejętności, kompetencji, kwalifikacji i zawodów (ESCO), Europass czy europejska sieć służb zatrudnienia (EURES).

[61] CyberSecPro. W ramach projektu przeprowadzona zostanie m.in. analiza programów, kursów i szkół letnich w dziedzinie cyberbezpieczeństwa oferowanych na uczelniach oraz stosowanych tabel ocen europejskiego systemu transferu i akumulacji punktów (ECTS). W projekcie w okresie trzech lat docelowo uczestniczyć będzie ponad 530 stażystów i przeszkolone zostaną osoby z zewnątrz z różnych branż i sektorów.

związanych z cyberbezpieczeństwem oraz wyjaśnianiu profili ról innych niż techniczne. Należy również wspierać grupy, do których trudno dotrzeć, takie jak osoby młode z niepełnosprawnościami, mieszkające w regionach oddalonych lub na obszarach wiejskich oraz pochodzące z innych grup mniejszościowych, aby umożliwić im skorzystanie z dostępnej oferty szkoleniowej w dziedzinie cyberbezpieczeństwa.

Komisja będzie nadal udzielać wsparcia na rzecz rozwoju mikropoświadczeń, kształcenia zawodowego i programów szkoleniowych. W szczególności w ramach programu Erasmus+ finansowane będą **wspólne programy studiów licencjackich i magisterskich, wspólne kursy lub moduły, które mogą prowadzić do uzyskania mikropoświadczeń**, oraz **mieszane programy intensywne**[62] dotyczące wszystkich tematów, w tym **cyberbezpieczeństwa**. Wspierane będzie także dalsze rozwijanie inicjatywy **„Uniwersytety Europejskie”**[63] i **centrów doskonałości zawodowej**[64] w celu zachęcania do ściślejszej współpracy między instytucjami szkolnictwa wyższego a odpowiednimi instytucjami kształcenia i szkolenia zawodowego w całej Europie. Unijne programy finansowania, w tym Erasmus+ i program „Cyfrowa Europa”, będą wspomagać realizację tego celu, jakim jest pogłębiona współpraca, podobnie jak fundusze UE przewidziane na rozwój **indywidualnych rachunków szkoleniowych**[65].

Aby ułatwić współpracę na poziomie krajowym między środowiskiem akademickim i organizatorami szkoleń w zakresie umiejętności w dziedzinie cyberbezpieczeństwa a pracodawcami z sektora prywatnego i publicznego oraz wspierać synergię między sektorem publicznym i prywatnym, zachęca się NCC do zbadania możliwości utworzenia w państwach członkowskich **cyberkampusów**. Celem tych cyberkampusów byłoby zapewnienie biegunów doskonałości na poziomie krajowym dla społeczności zajmujących się cyberbezpieczeństwem, a Akademia pomagałaby im w tworzeniu sieci kontaktów i dalszej koordynacji ich działań.

ENISA rozszerzy również swoją ofertę szkoleń w zakresie cyberbezpieczeństwa, dostosowując **swój katalog kursów**[66] do profili określonych w europejskich ramach umiejętności w dziedzinie cyberbezpieczeństwa i opracowując moduły szkoleniowe dla poszczególnych profili, co może wzbogacić oferty szkoleń w państwach członkowskich. Ponadto ENISA rozszerzy swój program **szkoleń dla instruktorów**[67], ukierunkowując go na potrzeby zawodowe europejskich instytucji, organów i jednostek organizacyjnych, organów publicznych państw członkowskich oraz **publicznych i prywatnych operatorów krytycznych** objętych zakresem dyrektywy NIS 2.

Oprócz tego inne organy i jednostki organizacyjne UE także wzbogacą swoją ofertę szkoleń w zakresie cyberbezpieczeństwa. Na przykład w ramach wdrażania polityki UE w zakresie cyberobrony **EKBiO** opracuje nowy zestaw kursów z zakresu cyberbezpieczeństwa i dostosuje niektóre ze swoich obecnych kursów do europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa. Kursy te będą prowadziły do certyfikacji efektów uczenia

[62] Mieszane programy intensywne łączą nauczanie zdalne z krótkim okresem fizycznej mobilności.

[63] Inicjatywa dotycząca europejskich szkół wyższych | Europejski obszar edukacji (europa.eu).

[64] Centra doskonałości zawodowej | Erasmus+ (europa.eu).

[65] Zgodnie z zaleceniem Rady z dnia 16 czerwca 2022 r. w sprawie indywidualnych rachunków szkoleniowych.

[66] Kursy szkoleniowe – ENISA (europa.eu).

[67] Program szkoleń dla instruktorów – ENISA (europa.eu).

się[68]. We współpracy z Komisją EKBiO zbada możliwość włączenia certyfikatów do unijnego portfela tożsamości cyfrowej. EKBiO będzie dalej poszukiwać możliwych mechanizmów oceny umiejętności, na podstawie których wydawane będą certyfikaty. Podobnie w obszarze zwalczania cyberprzestępczości dążyć się będzie do ścisłego powiązania z **Akademią Zwalczania Cyberprzestępczości CEPOL-u**[69] w celu wspierania synergii i komplementarności w projektowaniu i realizacji programów szkolenia.

4.3. Tworzenie synergii i zapewnienie widoczności szkoleń i certyfikacji w zakresie cyberbezpieczeństwa w państwach członkowskich

Akademia powinna zająć się problemem widoczności i synergii w obszarach szkoleń i certyfikacji. Byłoby to korzystne dla społeczności zajmujących się cyberbezpieczeństwem w sektorze cywilnym, obronnym, związanym z egzekwowaniem prawa i dyplomatycznym, ponieważ wszystkie sektory w wielu przypadkach wymagają tej samej wiedzy specjalistycznej opartej na podobnych programach nauczania i efektach uczenia się.

Akademia stanowiłaby **pojedynczy punkt dostępu** dla osób zainteresowanych karierą w dziedzinie cyberbezpieczeństwa. W krótkoterminowej perspektywie realizację tego założenia umożliwi rozbudowa **platformy Komisji na rzecz umiejętności cyfrowych i zatrudnienia** przy wsparciu ze strony projektu ECCO. Specjalna sekcja poświęcona karierze w dziedzinie cyberbezpieczeństwa będzie łączyć się z istniejącymi narzędziami, począwszy od programów szkolnictwa wyższego, poprzez możliwości w zakresie szkoleń, w tym kursy prowadzące do uzyskania mikropoświadczeń oraz programy kształcenia i szkolenia zawodowego, aż po oferty pracy. Cel ten zostanie osiągnięty poprzez odniesienie się do bieżących prac i inicjatyw lub ich integrację z platformą, takich jak działania ENISA, która we współpracy ze środowiskiem akademickim stworzyła **mapę instytucji edukacyjnych** oferujących programy w zakresie cyberbezpieczeństwa. Zostanie ona jeszcze bardziej rozbudowana przy wsparciu NCC. Ponadto ENISA opracuje i skonsoliduje **dwa repozytoria istniejących szkoleń z sektora publicznego i prywatnego oraz certyfikacji cyberbezpieczeństwa**, przy wsparciu NCC, Komisji i projektu ECCO oraz we współpracy z podmiotami wydającymi certyfikaty, korzystając również z innych istotnych inicjatyw[70]. Zostaną one również zintegrowane z pojedynczym punktem dostępu w ramach platformy na rzecz umiejętności cyfrowych i zatrudnienia. Z prac tych skorzystają również NCC, których zadaniem jest przede wszystkim promowanie i rozpowszechnianie programów edukacyjnych w zakresie cyberbezpieczeństwa[71].

Konieczne jest również danie specjalistom gwarancji, że szkolenia, które podejmują, mają wymaganą jakość. W związku z tym ENISA opracuje **projekt pilotażowy**, w ramach którego przeanalizuje możliwość utworzenia europejskiego systemu atestacji umiejętności w dziedzinie cyberbezpieczeństwa.

---

[68] Zgodnie z art. 20 ust. 4 decyzji Rady (WPZiB) 2020/1515 z dnia 19 października 2020 r. w sprawie ustanowienia Europejskiego Kolegium Bezpieczeństwa i Obrony oraz uchylenia decyzji (WPZiB) 2016/2382.

[69] Akademię Zwalczania Cyberprzestępczości CEPOL-u ustanowiono w 2019 r. w celu utworzenia najnowocześniejszej platformy umożliwiającej pogłębianie wiedzy na temat cyberprzestępczości i zwiększanie zdolności cyfrowych w Europie.

[70] Na przykład W4C Academy – Women4Cyber lub projekt na rzecz ogólnoświatowej certyfikacji kompetencji niezbędnych w walce z cyberprzestępczością dla organów ścigania i organów sądowych.

[71] „1. Krajowe ośrodki koordynacji mają następujące zadania: [...] g) bez uszczerbku dla kompetencji państw członkowskich w dziedzinie edukacji i z uwzględnieniem odpowiednich zadań agencji ENISA – nawiązywanie kontaktów z organami krajowymi z myślą o potencjalnym wkładzie w promowanie i upowszechnianie programów kształcenia w dziedzinie cyberbezpieczeństwa", art. 7 ust. 1 lit. g) rozporządzenia w sprawie Europejskiego Centrum Kompetencji w Dziedzinie Cyberbezpieczeństwa. Zob. również powiązany motyw 28.

Ponadto określenie umiejętności i szkoleń oraz powiązanie ich z profilem stanowiska ma zasadnicze znaczenie, ale ważne jest również zapewnienie, aby usługi w zakresie cyberbezpieczeństwa były świadczone z zachowaniem wymaganych kompetencji, wiedzy specjalistycznej i doświadczenia. Dotyczy to w szczególności dostawców usług zarządzanych w zakresie bezpieczeństwa w takich obszarach jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. W dyrektywie NIS 2 i we wniosku dotyczącym aktu w sprawie cybersolidarności określono konkretne zadania dla takich dostawców usług zarządzanych w zakresie bezpieczeństwa. W związku z tym Komisja proponuje również **ukierunkowaną zmianę aktu o cyberbezpieczeństwie**[72], aby umożliwić wprowadzenie programów certyfikacji zarządzanych usług w zakresie bezpieczeństwa na poziomie UE. Takie programy certyfikacji powinny mieć na celu m.in. zagwarantowanie, że usługi te są świadczone przez personel o bardzo wysokim poziomie wiedzy technicznej i kompetencji w odpowiednich dziedzinach.

Mechanizmy zapewniania jakości i uznawania mikropoświadczeń[73] ułatwiają zapewnienie przejrzystości, porównywalności i możliwość przenoszenia efektów uczenia się. Zgodnie z zaleceniem Rady w sprawie europejskiego podejścia do mikropoświadczeń[74] zachęca się państwa członkowskie do włączenia mikropoświadczeń w zakresie cyberbezpieczeństwa do krajowych ram kwalifikacji. Dzięki temu mogłyby odnosić mikropoświadczenia w zakresie cyberbezpieczeństwa do europejskich ram kwalifikacji[75].Infrastruktura europejskich poświadczeń cyfrowych w dziedzinie uczenia się może wydawać cyfrowo podpisane kwalifikacje i mikropoświadczenia w zakresie cyberbezpieczeństwa dotyczące osób fizycznych. Zawierają one kompleksowe dane, w tym dotyczące efektów uczenia się w zakresie cyberbezpieczeństwa, i mogą być przechowywane w przyszłym **cyfrowym portfelu EUeID**[76].

Działania w ramach Akademii

Państwa członkowskie i przemysł

- Zapewnienie wsparcia dla rozwoju i uznawania **mikropoświadczeń** wyników uczenia się w zakresie cyberbezpieczeństwa, zgodnie z zaleceniem Rady w sprawie europejskiego podejścia do mikropoświadczeń.
- Włączenie kwalifikacji w zakresie cyberbezpieczeństwa, w tym mikropoświadczeń, do **krajowych ram kwalifikacji**.
- Zapewnienie możliwości **zdobywania kwalifikacji w trakcie pracy** poprzez praktyki zawodowe dla osób uczestniczących w inicjatywach na rzecz rozwoju umiejętności w dziedzinie cyberbezpieczeństwa.

[72] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

[73] Na przykład udokumentowanie lub certyfikaty efektów uczenia się, które osoby nabywają po małych szkoleniach.

[74] Wniosek dotyczący zalecenia Rady w sprawie europejskiego podejścia do mikropoświadczeń na potrzeby uczenia się przez całe życie i zdolności do zatrudnienia.

[75] Zalecenie Rady z dnia 22 maja 2017 r. w sprawie europejskich ram kwalifikacji dla uczenia się przez całe życie i uchylające zalecenie Parlamentu Europejskiego i Rady z dnia 23 kwietnia 2008 r. w sprawie ustanowienia europejskich ram kwalifikacji dla uczenia się przez całe życie.

[76] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej.

Komisja

- W perspektywie krótkoterminowej – utworzenie do końca 2023 r. **pojedynczego punktu dostępu** na potrzeby programów dotyczących cyberbezpieczeństwa, istniejących szkoleń oraz certyfikacji cyberbezpieczeństwa za pośrednictwem **platformy na rzecz umiejętności cyfrowych i zatrudnienia**.
- 18 kwietnia 2023 r. – zaproponowanie zmiany w **akcie o cyberbezpieczeństwie** umożliwiającej certyfikację dostawców usług zarządzanych w zakresie bezpieczeństwa.

Organy i agencje UE

- Ustanowienie **europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa** jako wspólnego podejścia do profili ról w sektorze cyberbezpieczeństwa i powiązanych umiejętności do końca 2023 r.
- W II kwartale 2023 r. ENISA ma zainicjować opracowanie projektu pilotażowego ustanawiającego **europejski system atestacji** umiejętności w dziedzinie cyberbezpieczeństwa.
- Do końca 2023 r. ENISA ma dokonać przeglądu swojego **katalogu kursów** i otworzyć swój **program szkolenia instruktorów** dla publicznych i prywatnych operatorów krytycznych.
- Zakończenie **dostosowywania programów nauczania EKBiO do europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa** do połowy 2023 r.

5. Zaangażowanie zainteresowanych stron: podjęcie zobowiązania do zniwelowania luki w umiejętnościach w dziedzinie cyberbezpieczeństwa

W ramach Akademii opracowane zostanie skoordynowane podejście do zaangażowania zainteresowanych stron w celu rozwiązania problemu luki w umiejętnościach w dziedzinie cyberbezpieczeństwa. Celem będzie maksymalizacja widoczności i wpływu zobowiązań podjętych przez poszczególne zainteresowane strony mających na celu zmniejszenie luki w umiejętnościach w dziedzinie cyberbezpieczeństwa.

Komisja wzywa zainteresowane strony do podjęcia konkretnych zobowiązań w postaci deklaracji o umożliwieniu pracownikom podnoszenia i zmiany swoich kwalifikacji poprzez specjalne działania opierające się w jak największym stopniu na zidentyfikowanej luce w umiejętnościach w dziedzinie cyberbezpieczeństwa. Takie **deklaracje zainteresowanych stron dotyczące cyberbezpieczeństwa** powinny być zgłaszane na **platformie na rzecz umiejętności cyfrowych i zatrudnienia**, podobnie jak inne deklaracje cyfrowe już widoczne na platformie. Komisja zachęca ponadto zainteresowane strony, które składają deklaracje dotyczące cyberbezpieczeństwa na platformie, aby przystąpiły do **partnerstwa cyfrowego na dużą skalę w ramach paktu na rzecz umiejętności**[77]. Zachęca się, aby zobowiązania dotyczące cyberbezpieczeństwa podejmowane w ramach partnerstwa cyfrowego na dużą skalę składano z wykorzystaniem platformy na rzecz umiejętności cyfrowych i zatrudnienia. Podobnie zachęca się do tego, aby zobowiązania podejmowane w ramach platformy na rzecz umiejętności cyfrowych i zatrudnienia zgłaszano w kontekście partnerstwa cyfrowego na dużą skalę w ramach paktu na rzecz umiejętności.

[77] Nowe partnerstwa europejskie uruchomione w celu zrealizowania ambicji UE na cyfrową dekadę | Kształtowanie cyfrowej przyszłości Europy (europa.eu), utworzone w ramach paktu na rzecz umiejętności, aby wyeliminować problem niedoboru technologii informacyjno-komunikacyjnych (ICT).

Komisja wzywa ponadto państwa członkowskie do **kontynuowania działań na rzecz wdrażania deklaracji w sprawie kobiet w sektorze cyfrowym**[78]**,** aby zachęcić kobiety do odgrywania aktywnej i znaczącej roli w sektorze technologii cyfrowych oraz osiągnąć konwergencję płci na stanowiskach związanych z cyberbezpieczeństwem. Komisja zachęca również państwa członkowskie do rozwijania synergii z ich programami realizowanymi w ramach **Europejskiego Funduszu Społecznego+** (EFS+) w celu dalszego wspierania celu, jakim jest równość płci w zakresie udziału w rynku pracy[79], na przykład poprzez tworzenie **programów mentorskich dla dziewcząt i kobiet**. Mogą one ułatwić tworzenie wzorców, aby przyciągnąć dziewczęta do zawodów związanych z cyberbezpieczeństwem, zwalczając jednocześnie stereotypy związane z płcią. Działania te zachęcają również do podnoszenia i zmiany kwalifikacji kobiet oraz sprzyjają rozwojowi społeczności, która może wspierać kobiety we wchodzeniu na rynek pracy w dziedzinie cyberbezpieczeństwa lub w ich późniejszym awansie.

Państwa członkowskie powinny przyjąć, w ramach **swoich krajowych strategii cyberbezpieczeństwa, konkretne środki w celu złagodzenia niedoboru umiejętności w dziedzinie cyberbezpieczeństwa**[80], zidentyfikowania i lepszego ukierunkowania działań mających na celu wyeliminowanie przypadków niedoboru kwalifikacji, a ostatecznie zapewnienia właściwej realizacji zobowiązań wynikających z dyrektywy NIS 2.

Niektóre państwa członkowskie wykorzystują **synergię między inicjatywami cywilnymi, obronnymi i związanymi z egzekwowaniem prawa**. Na przykład zwiększenie puli siły roboczej z wykorzystaniem krajowej obowiązkowej służby wojskowej lub wykorzystanie rezerwistów cybernetycznych, którzy są przeszkolonymi pod kątem wojskowym obywatelami obsadzającymi stanowiska związane z cyberbezpieczeństwem w siłach zbrojnych[81], pozwala społeczeństwu, a zwłaszcza młodym dorosłym, zwiększyć swoje umiejętności w zakresie cyberbezpieczeństwa i cyberobrony. To samo dotyczy obszaru **zwalczania cyberprzestępczości**, ponieważ istnieje wiele podobieństw między ogólnymi działaniami na rzecz cyberbezpieczeństwa a działaniami organów ścigania w zakresie reagowania na cyberincydenty. Komisja zachęca państwa członkowskie do podejmowania między sobą dyskusji na temat takich inicjatyw oraz do oceny, jak wykwalifikowana siła robocza może najlepiej służyć społecznościom zajmującym się cyberbezpieczeństwem zarówno w sektorze cywilnym, jak i w sektorze obronnym.

Komisja rozważy propozycje dotyczące sposobu zniwelowania istniejących i przewidywanych luk wskazanych w przeglądzie potrzeb europejskich instytucji, organów i jednostek organizacyjnych. W szczególności będzie zachęcać pracowników do skorzystania z dostępnego wkrótce **stypendium UE–USA w zakresie cyberbezpieczeństwa** ustanowionego w ramach dialogu między Unią a Stanami Zjednoczonymi.

[78] Państwa UE zobowiązują się do zwiększenia udziału kobiet w obszarze cyfrowym | Kształtowanie cyfrowej przyszłości Europy (europa.eu).

[79] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013, art. 4 ust. 1 lit. c).

[80] Art. 7 ust. 2 lit. f) dyrektywy NIS 2.

[81] Report - Cyber Conscription: Experience and Best Practice from Selected Countries, Martin Hurt i Tiia Sõmer, Międzynarodowe Centrum Obrony i Bezpieczeństwa, luty 2021 r.

Działania w ramach Akademii

Przemysł

- Składanie konkretnych **deklaracji dotyczących cyberbezpieczeństwa** na platformie na rzecz umiejętności cyfrowych i zatrudnienia począwszy od 18 kwietnia 2023 r.

Państwa członkowskie

- Włączenie do **krajowych strategii cyberbezpieczeństwa** konkretnych środków mających na celu rozwiązanie problemu luki w umiejętnościach w dziedzinie cyberbezpieczeństwa.

Państwa członkowskie i przemysł

- Wdrożenie deklaracji w sprawie kobiet w sektorze cyfrowym i osiągnięcie **konwergencji płci na stanowiskach związanych z cyberbezpieczeństwem** do 2030 r.

6. Finansowanie: tworzenie synergii w celu maksymalizacji wpływu wydatków na rozwój umiejętności w dziedzinie cyberbezpieczeństwa

W ramach Akademii wpływ inwestycji w umiejętności w dziedzinie cyberbezpieczeństwa zostanie zmaksymalizowany dzięki zapewnieniu wspólnego punktu wejścia, ułatwieniu lepszego ukierunkowania funduszy na potrzeby rynku oraz maksymalnie efektywnego ich wykorzystania, ułatwienie synergii między różnymi instrumentami przy jednoczesnym unikaniu powielania wysiłków[82].

6.1.Dopasowanie funduszy do potrzeb

W ramach Akademii ECCC, przy wsparciu Komisji, projektu ECCO i NCC, będzie gromadzić **informacje na temat sposobu wykorzystania funduszy UE do finansowania umiejętności w dziedzinie cyberbezpieczeństwa** oraz oceni, w jaki sposób fundusze UE wspierają zmniejszanie luki w umiejętnościach w dziedzinie cyberbezpieczeństwa. Biorąc pod uwagę te zbiorcze informacje, ECCC będzie dążyć do zapewnienia lepszego ukierunkowania funduszy UE na zidentyfikowane potrzeby. Będzie finansować działania, które pozwolą zlikwidować najpilniejsze braki siły roboczej w sektorze cyberbezpieczeństwa, w tym luki związane z realizacją potrzeb w zakresie polityki cyberbezpieczeństwa.

6.2.Zapewnienie widoczności dostępnych funduszy i inicjatyw partnerskich dotyczących umiejętności w dziedzinie cyberbezpieczeństwa

W perspektywie krótkoterminowej **platforma na rzecz umiejętności cyfrowych i zatrudnienia** stanie się pojedynczym punktem dostępu dla zainteresowanych stron, w którym dostępne będą wszystkie informacje dotyczące możliwości finansowania umiejętności w dziedzinie cyberbezpieczeństwa.

UE inwestuje w ludzi i ich umiejętności oraz wykorzystuje partnerstwa, zwłaszcza z branżą, do mobilizowania działań w zakresie podnoszenia i zmiany kwalifikacji przy pomocy szeregu instrumentów określonych w ramach **europejskiego programu na rzecz**

[82] Możliwości finansowania (europa.eu) Usługi wsparcia w ramach paktu na rzecz umiejętności stanowią pojedynczy punkt dostępu pozwalający uzyskać informacje o finansowaniu umiejętności, w tym w odniesieniu do ekosystemu cyfrowego. Usługi wsparcia w ramach paktu zapewniają ogólne informacje na temat instrumentów finansowania, które nie są ukierunkowane konkretnie na umiejętności w dziedzinie cyberbezpieczeństwa, niemniej jednak Akademia powinna uwzględnić te ich pracę, aby uniknąć powielania.

umiejętności[83], w szczególności **paktu na rzecz umiejętności**[84] oraz **Planu działania w dziedzinie edukacji cyfrowej**[85]. W ramach **programu „Cyfrowa Europa"** finansuje się możliwości w zakresie umiejętności w dziedzinie cyberbezpieczeństwa, zwłaszcza poprzez projekty inicjowane przez wiele krajów, co wyraźnie uzupełnia wsparcie oferowane w ramach programu „Horyzont Europa" na rzecz badań i innowacyjnych rozwiązań technologicznych w zakresie cyberbezpieczeństwa. **Europejski Fundusz Obronny**[86] finansuje badania naukowe i rozwój technologii w celu prowadzenia skutecznych operacji z zakresu cyberbezpieczeństwa, w tym szkolenia i ćwiczenia[87]. Program **Erasmus+** będzie nadal wspierał takie inicjatywy, w tym poprzez intensywne programy łączone oraz projekty współpracy.

Zachęca się państwa członkowskie do uruchomienia funduszy UE, którymi bezpośrednio zarządzają, w celu wspierania umiejętności i zatrudnienia w dziedzinie cyberbezpieczeństwa. Fundusze polityki spójności, takie jak **Europejski Fundusz Rozwoju Regionalnego (EFRR)** i **EFS+**, niosą ze sobą istotny potencjał synergii w tym zakresie[88]. Zakres działań w ramach **Instrumentu na rzecz Odbudowy i Zwiększania Odporności** (RRF)[89] oraz **InvestEU**[90] obejmuje kolejne kluczowe elementy uzupełniające potrzebne do osiągnięcie celów Akademii.

Działania w ramach Akademii

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa i ENISA

- **Tworzenie zestawień** istniejącego finansowania unijnego na rzecz umiejętności w dziedzinie cyberbezpieczeństwa w odniesieniu do potrzeb rynku, ocena **skuteczności** i określenie **priorytetów** finansowania do końca 2024 r.

Komisja

- Utworzenie **pojedynczego punktu dostępu** do możliwości finansowania umiejętności w dziedzinie cyberbezpieczeństwa na platformie na rzecz umiejętności cyfrowych i zatrudnienia do końca 2023 r.

[83] Europejski program na rzecz umiejętności – Zatrudnienie, sprawy społeczne i włączenie społeczne – Komisja Europejska (europa.eu).

[84] Instrumenty finansowania unijnego na rzecz podnoszenia i zmiany kwalifikacji – Zatrudnienie, sprawy społeczne i włączenie społeczne – Komisja Europejska (europa.eu).

[85] Plan działania w dziedzinie edukacji cyfrowej na lata 2021–2027.

[86] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/697 z dnia 29 kwietnia 2021 r. ustanawiające Europejski Fundusz Obronny i uchylające rozporządzenie (UE) 2018/1092.

[87] Państwa członkowskie są zaangażowane we wspólne szkolenia i ćwiczenia, na przykład przez ustanowienie projektów dotyczących szkoleń i ćwiczeń w dziedzinie cyberbezpieczeństwa w ramach stałej współpracy strukturalnej (PESCO), takich jak Cyberakademia i centrum innowacji UE (EU CAIH) oraz Federacje cyberpoligonowe, i uczestnictwo w tych projektach.

[88] Art. 3 ust. 1 rozporządzenia (UE) 2021/1058 i art. 4 ust. 1 lit. g) rozporządzenia (UE) 2021/1057.

[89] Na przykład w estońskim planie odbudowy i zwiększania odporności przewidziano inwestycje (10 mln EUR) w umiejętności cyfrowe, które obejmą przegląd szkoleń dostępnych dla specjalistów w dziedzinie ICT, posłużą do sfinansowania podnoszenia i zmiany kwalifikacji specjalistów w dziedzinie ICT w zakresie cyberbezpieczeństwa oraz przyczynią się do opracowania programu pilotażowego mającego na celu zmianę ram kwalifikacji dla specjalistów w dziedzinie ICT.

[90] Zainteresowane strony (np. organizatorzy szkoleń i firmy chcące opracować lub udoskonalić swoje działania szkoleniowe w zakresie cyberbezpieczeństwa) mogą zwrócić się do Centrum Doradztwa InvestEU, które zapewnia wsparcie i pomoc techniczną, w tym pomoc w budowaniu zdolności, dla twórców projektów i podmiotów; potrzebne informacje można znaleźć na portalu InvestEU.

7. Pomiar postępów: nieodłączna odpowiedzialność

W ramach Akademii zostanie opracowana **metodyka**, która pozwoli mierzyć **postępy w niwelowaniu luki w umiejętnościach w dziedzinie cyberbezpieczeństwa**.

7.1. Określenie wskaźników cyberbezpieczeństwa do celów monitorowania zmian na rynku pracy w sektorze cyberbezpieczeństwa

Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) podsumowuje wskaźniki dotyczące wyników cyfrowych Europy i śledzi postępy państw członkowskich UE. W ramach Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa ENISA, we współpracy z Komisją i Grupą Współpracy NIS[91], opracuje **wskaźniki**, w tym dotyczące płci, w celu śledzenia postępów poczynionych w państwach członkowskich UE w zakresie zwiększenia liczby specjalistów w dziedzinie cyberbezpieczeństwa, konsultując się również z odpowiednimi podmiotami rynkowymi i NCC. ENISA będzie korzystać z metodyki DESI[92] i dopilnuje, aby wskaźniki były zgodne z europejskimi celami cyfrowymi dotyczącymi specjalistów w dziedzinie ICT oraz osiągnięcia konwergencji płci w dziedzinie ICT. Komisja będzie następnie pracować nad włączeniem tych wskaźników do DESI, co pozwoli na coroczne śledzenie stanu umiejętności w dziedzinie cyberbezpieczeństwa i rynku pracy w tym sektorze.

7.2. Gromadzenie danych i sprawozdawczość

ENISA będzie gromadzić dane dotyczące wskaźników przy wsparciu projektu ECCO i NCC. Na podstawie zgromadzonych danych ENISA sporządzi **roczne sprawozdanie**, które będzie stanowić wkład w sprawozdanie dotyczące stanu cyfrowej dekady[93], które wraz z DESI zostanie następnie wykorzystane w analizie i zaleceniach dla poszczególnych krajów w ramach **europejskiego semestru**[94]. Ponadto wskaźniki dotyczące umiejętności w dziedzinie cyberbezpieczeństwa będą stanowiły wkład do **sporządzanego co dwa lata sprawozdania** ENISA o stanie cyberbezpieczeństwa w UE, przewidzianego w dyrektywie NIS 2, obejmującego zdolności w zakresie cyberbezpieczeństwa, wiedzę o cyberbezpieczeństwie i cyberhigienie w całej UE.

7.3. Przygotowanie kluczowych wskaźników skuteczności działania (KPI) dotyczących cyberbezpieczeństwa

W celu zniwelowania niedoboru talentów w Europie pod względem cyberbezpieczeństwa ENISA, w ścisłej współpracy z Komisją i NCC, zaproponuje Komisji kluczowe wskaźniki skuteczności działania, opierając się na metodyce programu polityki „Droga ku cyfrowej dekadzie" do 2030 r., a także na doświadczeniach branży. ENISA uwzględni w należyty

[91] Czerpanie z metodyki, która zostanie opracowana przez ENISA na potrzeby przygotowywanego co dwa lata sprawozdania agencji o stanie cyberbezpieczeństwa w Unii zgodnie z art. 18 ust. 3 dyrektywy NIS 2, oraz jej uzupełnienie.

[92] Zob. nota metodyczna dotycząca indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) za 2022 r., dostępna na stronie indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) | Kształtowanie cyfrowej przyszłości Europy (europa.eu).

[93] Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r.

[94] Ibidem, motyw 25.

sposób kluczowe wskaźniki skuteczności działania stosowane przez państwa członkowskie do oceny ich krajowych strategii cyberbezpieczeństwa[95].

Działania w ramach Akademii

ENISA

- Przygotowanie **wskaźników oraz kluczowych wskaźników skuteczności działania** dotyczących umiejętności w dziedzinie cyberbezpieczeństwa do końca 2023 r.
- **Zbieranie danych** na temat wskaźników i przekazywanie sprawozdań na ich temat, przy czym dane muszą zostać zebrane po raz pierwszy do 2025 r.

Komisja

- Praca na rzecz włączenia **wskaźników dotyczących cyberbezpieczeństwa do DESI** oraz do **sprawozdania dotyczącego stanu cyfrowej dekady**.

8. Wnioski

W niniejszym komunikacie określono podstawy zmiany podejścia UE do zwiększania umiejętności w dziedzinie cyberbezpieczeństwa wśród specjalistów w UE. Celem jest zmniejszenie luki w umiejętnościach w dziedzinie cyberbezpieczeństwa oraz wyposażenie UE w niezbędną siłę roboczą, która umożliwi jej reagowanie na stale zmieniający się krajobraz zagrożeń, realizację polityk UE mających na celu ochronę UE przed cyberatakami oraz zwiększenie możliwości rynkowych i konkurencyjności. Wykwalifikowana siła robocza w sektorze cyberbezpieczeństwa może przynieść korzyści **społecznościom zajmującym się cyberbezpieczeństwem w sektorze cywilnym, obronnym, dyplomatycznym i związanym z egzekwowaniem prawa**, ułatwiając powstanie synergii między nimi.

Komisja wzywa państwa członkowskie i wszystkie zainteresowane strony do realizacji ambitnych założeń Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa.

[95] Art. 7 ust. 4 dyrektywy NIS 2.