



Bruksela, dnia 20.1.2026 r.
COM(2026) 9 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

**w sprawie oceny Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz
Europejskich ram certyfikacji cyberbezpieczeństwa**

{SWD(2026) 2 final}

1. WPROWADZENIE

1.1 Podstawowe informacje o ENISA

Utworzona w 2004 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) początkowo miała na celu zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w UE oraz promowanie kultury uwzględniającej kwestie bezpieczeństwa z korzyścią dla zainteresowanych stron. Na przestrzeni lat mandat i obowiązki Agencji znacznie się zmieniały, aby nadążać za szybko zmieniającą się sytuacją w dziedzinie bezpieczeństwa cyfrowego w Europie. W odpowiedzi na rosnącą złożoność wyzwań związanych z cyberbezpieczeństwem akt o cyberbezpieczeństwie rozszerzył w 2019 r. mandat ENISA i nadał jej ostateczny status w ramach instytucjonalnych UE. To rozszerzenie mandatu jeszcze bardziej wzmocniło rolę ENISA polegającą na wspieraniu zarządzania działaniami w zakresie cyberbezpieczeństwa i ich koordynacji w całej UE, ze skupieniem uwagi na kilku kluczowych obszarach:

- pomoc w opracowywaniu i wdrażaniu polityki i prawa UE w dziedzinie cyberbezpieczeństwa;
- zwiększanie zdolności UE do zapobiegania incydentom cyberbezpieczeństwa, wykrywania ich i reagowania na nie, w szczególności przez udzielanie pomocy operacyjnej i technicznej państwom członkowskim i instytucjom UE;
- wspieranie budowania zdolności i współpracy w zakresie cyberbezpieczeństwa w UE;
- zwiększanie wiedzy na temat ryzyka w cyberprzestrzeni i promowanie najlepszych praktyk wśród społeczeństwa, organizacji i przedsiębiorstw;
- przyczynianie się do ustanowienia i wdrożenia europejskich ram certyfikacji cyberbezpieczeństwa, mających na celu zmniejszenie fragmentacji rynku i zwiększenie cyberbezpieczeństwa produktów, usług i procesów ICT w całej UE oraz
- wspieranie współpracy z partnerami międzynarodowymi zgodnie z polityką zewnętrzną UE.

Działania ENISA obejmują obecnie zalecenia dotyczące podstawowego poziomu bezpieczeństwa, sprawozdania dotyczące krajobrazu zagrożeń, wytyczne normalizacji oraz badania dotyczące najlepszych praktyk w różnych dziedzinach. Agencja organizuje warsztaty, ćwiczenia i programy szkoleniowe w celu zwiększenia wiedzy fachowej wśród specjalistów w dziedzinie cyberbezpieczeństwa i decydentów. Ponadto ENISA odgrywa kluczową rolę w odpowiadaniu na wnioski Komisji i państw członkowskich, wspieraniu zadań związanych z certyfikacją i zapewnianiu dostosowanego do potrzeb doradztwa w zakresie opracowywania i wdrażania polityki cyberbezpieczeństwa.

Oczekiwany wpływ ENISA obejmuje poprawę bezpieczeństwa sieci i informacji w UE, zwiększenie zaufania do jednolitego rynku cyfrowego oraz promowanie współpracy w dziedzinie cyberbezpieczeństwa między kluczowymi zainteresowanymi stronami w Europie. W toku realizacji obecnie przez Europę transformacji cyfrowej strategie adaptacyjne ENISA zapewniają bezpieczeństwo i odporność krajobrazu cyfrowego regionu i odpowiadają na wyzwania, takie jak zagrożenia cyberbezpieczeństwa, napięcia geopolityczne i fragmentacja polityki wśród państw członkowskich.

1.2 Europejskie ramy certyfikacji cyberbezpieczeństwa (ECCF)

Europejskie ramy certyfikacji cyberbezpieczeństwa (ECCF) zostały ustanowione na mocy aktu o cyberbezpieczeństwie, a ich głównym celem jest poprawa sytuacji w zakresie cyberbezpieczeństwa w całej Unii Europejskiej. ECCF mają w zamierzeniu stworzyć jednolite i horyzontalne podejście do certyfikacji cyberbezpieczeństwa we wszystkich państwach członkowskich, a tym samym zmniejszyć fragmentację na rynku wewnętrznym produktów, usług i procesów ICT. W ten sposób wzmacniają zaufanie rynku, wspierają rozwój unijnego rynku cyberbezpieczeństwa i zapewniają solidną odporność i zdolności w zakresie cyberbezpieczeństwa. Ramy te uwzględniają sześć podstawowych potrzeb:

- promowanie zaufania do rynku w całej UE;
- poprawa środków i odporności w zakresie cyberbezpieczeństwa;
- ustanowienie wysokich standardów odporności w ofertach rynkowych;
- zacieśnianie współpracy między zainteresowanymi stronami zajmującymi się cyberbezpieczeństwem;
- zmniejszenie obciążeń związanych z certyfikacją oraz
- podnoszenie wiedzy na temat cyberbezpieczeństwa wśród europejskich obywateli i przedsiębiorstw.

Ponadto ECCF mają zwiększyć przejrzystość w zapewnianiu cyberbezpieczeństwa, gdyż promują uwzględnianie bezpieczeństwa na etapie projektowania i domyślne bezpieczeństwo, co wiąże się z ograniczaniem podatności i przestrzeganiem określonych wymogów bezpieczeństwa.

Aby osiągnąć te cele, ECCF opierają się na kilku kluczowych filarach, a centralnym elementem tych starań jest rozwój europejskich systemów certyfikacji bezpieczeństwa cybernetycznego. W ramach tych położono nacisk na kompleksowe zapewnienie cyberbezpieczeństwa i odporności w całej UE za pośrednictwem tych systemów. Ramy te wspierają budowanie społeczności w celu zapewnienia kluczowego wkładu zainteresowanych stron i ułatwienia współpracy z państwami członkowskimi i między nimi. Akt o cyberbezpieczeństwie określa również obowiązek przeprowadzenia konsultacji publicznych ze wszystkimi odpowiednimi zainteresowanymi stronami w drodze formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji oraz przewiduje utworzenie grup doradczych ad hoc w celu zebrania różnych perspektyw i wiedzy fachowej w ramach procesu opracowywania systemu certyfikacji. ENISA odgrywa kluczową rolę w koordynowaniu tych wysiłków przez systematyczne konsultacje z zainteresowanymi stronami zmierzające do zapewnienia, by wszystkie elementy ustawodawcze zostały uwzględnione przed przekazaniem Komisji Europejskiej ostatecznych propozycji systemów do przyjęcia.

Okoliczności związane z cyberbezpieczeństwem, które leżą u podstaw ustanowienia ECCF, odzwierciedlają szybko zmieniający się krajobraz zagrożeń charakteryzujący się coraz częstszymi cyberatakami wykorzystującymi luki w zabezpieczeniach i niewystarczające praktyki w zakresie bezpieczeństwa, w połączeniu z pojawiającą się fragmentacją certyfikacji w UE. Sytuacja ta uwydatnia potrzebę realizacji misji ECCF polegającej na zapewnieniu integralności, poufności i dostępności danych w całym cyklu życia produktów, usług i procesów ICT. Oczekuje się, że po zakończeniu podstawowych działań ECCF, wygenerują one szereg wyników, w tym dokumenty związane z systemem, publikacje, wydarzenia i usprawnienia strukturalne wspierające wdrażanie. Działania te mają na celu wspieranie powszechniejszego stosowania certyfikacji cyberbezpieczeństwa, usprawnienie procesów, zwiększenie zaufania do rynku wewnętrznego oraz wzmocnienie zdolności zarówno sektora publicznego, jak i prywatnego.

Oczekuje się, że w przyszłości wkład ECCF wzmocni cyberodporność i konkurencyjność UE, zapewni bezpieczne i płynne interakcje cyfrowe w UE, a jednocześnie wyeliminuje pojawiające się wyzwania w zakresie cyberbezpieczeństwa. W perspektywie średnio- i długoterminowej przewiduje się istotne skutki, których pozytywny charakter będzie zależał od dynamicznych czynników wewnętrznych i zewnętrznych, w tym zmian geopolitycznych, zmieniających się krajobrazów bezpieczeństwa i pojawiających się potrzeb rynkowych.

1.3 Cel sprawozdania

Celem niniejszego sprawozdania jest ocena wpływu i skuteczności ENISA i ECCF, z uwzględnieniem zmieniającego się otoczenia technologicznego i regulacyjnego. Zgodnie z art. 67 rozporządzenia (UE) 2019/881, znanego jako akt o cyberbezpieczeństwie, w ocenie tej nie tylko dokonano przeglądu mandatu i działań ENISA, ale także oceniono rolę ECCF we wspieraniu bezpiecznego środowiska cybernetycznego w całej UE do 28 czerwca 2024 r. Przedstawione ustalenia pochodzą z przygotowawczego sprawozdania z oceny ukończonego w grudniu 2024 r.

Analiza obejmuje lata 2017–2023 i służy kilku kluczowym celom. Przede wszystkim jest skoncentrowana na kontroli wyników, zarządzania i praktyk roboczych ENISA i ECCF. Wiąże się to z określeniem stopnia, w jakim osiągnęły one swoje cele i przyczyniły się do poprawy cyberbezpieczeństwa i funkcjonowania rynku wewnętrznego w UE. Ocena koncentruje się na pięciu głównych kryteriach – skuteczności, efektywności, znaczeniu, spójności i unijnej wartości dodanej – i zapewnia tym samym ramy umożliwiające zrozumienie zarówno osiągnięć podmiotów, jak i obszarów wymagających poprawy.

Po przeanalizowaniu tych elementów w sprawozdaniu przedstawiono spostrzeżenia na temat potencjalnych dostosowań mandatu ENISA i strategii na rzecz wzmocnienia wpływu ECCF. Dodatkowo oceny te mają na celu ułatwienie świadomego podejmowania decyzji służących zwiększeniu odporności UE w zakresie cyberbezpieczeństwa. Sprawozdanie podzielone jest na odrębne sekcje, którymi są wprowadzenie dotyczące ENISA i ECCF, analiza ustaleń z oceny oraz podsumowanie wniosków i zaleceń.

Rozporządzenie (UE) 2024/2847 (akt o cyberodporności) wprowadza horyzontalne wymagania w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (sprzęt i oprogramowanie, w tym ich komponenty, gdy są wprowadzane do obrotu oddzielnie). Uzależnia ono ich wprowadzanie do obrotu w Unii od zgodności z zestawem zasadniczych wymagań w zakresie cyberbezpieczeństwa, zgodnie z podejściem przyjętym w nowych ramach prawnych Unii. Akt o cyberodporności wszedł w życie 10 grudnia 2024 r. i będzie stosowany w całości od 11 grudnia 2027 r. Wnioskowi Komisji towarzyszyła kompleksowa ocena skutków, w której przeanalizowano uzasadnienie wprowadzenia takich przepisów. W świetle powyższego oraz biorąc pod uwagę fakt, że stosowanie aktu o cyberodporności nadal znajduje się w okresie przejściowym, nie uznano za konieczne przeprowadzenia w niniejszym sprawozdaniu dalszej oceny trzeciego elementu, o którym mowa w art. 67 ust. 3 aktu o cyberbezpieczeństwie: „Ocena obejmuje ustalenie, czy w celu zapobieżenia wprowadzaniu na rynek wewnętrzny produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa niespełniających podstawowych wymogów cyberbezpieczeństwa konieczne są zasadnicze wymogi cyberbezpieczeństwa dotyczące dostępu do rynku wewnętrznego”.

Ponieważ ustalenia zawarte w niniejszym sprawozdaniu stanowią podstawę celów politycznych związanych z przeglądem aktu o cyberbezpieczeństwie, niniejsze sprawozdanie towarzyszy aktowi ustawodawczemu i w związku z tym należy je przedstawić jako część tego pakietu.

2. GŁÓWNE USTALENIA Z OCENY

2.1 ENISA

W niniejszej sekcji przedstawiono główne ustalenia z oceny ENISA, koncentrując się na jej skuteczności, efektywności, znaczeniu i spójności oraz wartości dodanej, jaką wnosi ona do unijnego krajobrazu cyberbezpieczeństwa. Ponadto przedstawiono dokładniejszą analizę zarządzania wewnętrznego i praktyk wewnętrznych w Agencji, aby wyjaśnić jej dynamikę operacyjną i obszary wymagające poprawy.

Skuteczność

W przygotowawczym sprawozdaniu z oceny podkreślono, że ENISA wypełnia swój mandat, gdyż osiągnęła prawie wszystkie zaplanowane wyniki. Należy jednak wspomnieć, że przy braku wystarczających wskaźników analiza skuteczności opiera się głównie na wywiadach i ankietach przeprowadzonych wśród zainteresowanych stron. W szczególności w trudnych czasach, takich jak okres pandemii COVID-19 i rosyjska wojna napastnicza przeciwko Ukrainie, Agencja wykazała elastyczność i uzyskała pozytywne oceny od zainteresowanych stron. Podczas pandemii COVID-19 ENISA wspierała Komisję i państwa członkowskie przez określanie w krótkim czasie wymogów bezpieczeństwa dotyczące aplikacji COVID. Odegrała również rolę we współpracy z Ukrainą, a jej celem było zapewnienie, aby ataki na infrastrukturę krytyczną i sektory krytyczne, takie jak energetyka, nie miały skutków ubocznych. Skuteczność ENISA wynika z solidnej struktury zarządzania i macierzowego modelu organizacyjnego, który ułatwia realizację zadań i współpracę. ENISA osiągnęła wiele ze swoich celów. Zainteresowane strony ogólnie uznały i doceniły wkład ENISA w zwiększanie odporności UE pod względem cyberbezpieczeństwa. Agencja promowała współpracę i wymianę informacji między państwami członkowskimi i innymi zainteresowanymi stronami, aby wspierać cele UE w zakresie cyberbezpieczeństwa. Szczególnie doceniono wysiłki Agencji na rzecz ułatwienia współpracy technicznej, promowania wspólnych norm cyberbezpieczeństwa i wspierania inicjatyw w zakresie budowania zdolności. W sprawozdaniu z oceny zasugerowano również, że istnieje możliwość poprawy ustalania priorytetów zadań w ramach pracy ENISA. Przez dokonanie ponownej oceny swojego ukierunkowania operacyjnego ENISA może wykorzystać istniejące ramy i informacje zwrotne od zainteresowanych stron, aby jeszcze bardziej usprawnić realizację zadań. Podejście to ma szczególne znaczenie przy realizacji pojawiających się priorytetów bez uszczerbku dla istniejących zobowiązań. Nieustanne dążenie ENISA do angażowania zainteresowanych stron i konsultacji z nimi jest jej atutem, jednak zdolności operacyjne agencji wskazują na niewystarczające zasoby. Wykorzystanie bardziej dynamicznej realokacji zadań i zasobów mogłoby w pewnym stopniu pomóc w zapewnieniu terminowej realizacji nowych wniosków i zwiększeniu zdolności ENISA do reagowania na wyzwania związane z cyberbezpieczeństwem. Cel Agencji, jakim jest utrzymanie i umocnienie jej reputacji w środowisku zajmującym się cyberbezpieczeństwem, można dodatkowo osiągnąć przez zapewnienie, aby zadania były dostosowane nie tylko do celów strategicznych, ale również do zdolności operacyjnych. Takie

ustalenie priorytetów należy ułatwić w ramach współpracy między ENISA, państwami członkowskimi i decydentami politycznymi UE, aby zagwarantować zgodność z celami strategicznymi i zdolnościami operacyjnymi.

Efektywność

W objętym oceną okresie 2017–2023 ENISA wykazała się skutecznymi działaniami w ramach istniejącej struktury zarządzania. Macierzowy model organizacyjny pomagał ENISA w nadawaniu priorytetu zadaniom, optymalizowaniu dostosowania zasobów i wspieraniu współpracy między różnymi działami. Podejście to, w połączeniu z wyważonym połączeniem pracowników operacyjnych i administracyjnych, ułatwiło realizację powierzonych zadań. Istnieje jednak wyraźna możliwość zwiększenia efektywności przez ENISA przez lepsze ustalanie priorytetów, jasne ukierunkowanie działań i bardziej strategiczny przydział zasobów. Efektywność działań Agencji była niekiedy ograniczana przez czynniki zewnętrzne i potrzebę usprawnienia zarządzania wewnętrznego. Wewnętrznie ENISA opracowała innowacyjne rozwiązania, takie jak macierzowy model organizacyjny, aby skuteczniej koordynować funkcje operacyjne i administracyjne.

Mimo to w ocenie zwrócono uwagę na kilka kluczowych obszarów, w których ENISA może poprawić efektywność. Wywiady z pracownikami ENISA, ankiety wśród zainteresowanych stron i dokumentacja wewnętrzna wykazały, że Agencja miała trudności z dotrzymaniem kroku rosnącemu zapotrzebowaniu i obsadzeniem specjalistycznych stanowisk, co zostało spotęgowane globalnym niedoborem specjalistów w dziedzinie IT. Doprowadziło to do opóźnień i zmian priorytetów zadań oraz do okresów dużego stresu i obciążenia pracą. Niemniej jednak pewne dostosowania mogłyby złagodzić te trudności. Niedawne strategiczne decyzje dotyczące realokacji zasobów ludzkich świadczą o pewnej zdolności do reagowania na zmiany priorytetów. Chociaż w 2022 r. dokonano znacznego zwiększenia budżetu o 15 mln EUR w celu uwzględnienia działań wspierających w obszarze cyberbezpieczeństwa, wzrostowi temu nie towarzyszył proporcjonalny wzrost liczby pracowników. Realokacja około 10,5 EPC w 2022 r. w celu uwzględnienia działań wspierających w obszarze cyberbezpieczeństwa pokazuje zdolność do optymalizacji obecnych zasobów w razie potrzeby, mimo że w tym przypadku EPC potrzebne do realizacji działań wspierających zostały faktycznie uzyskane częściowo w drodze zamówień publicznych, a częściowo za pośrednictwem zarządzania personelem kontraktowym, jak podkreślono w przygotowawczym sprawozdaniu z oceny. 10,5 EPC przeniesiono z istniejącego programu prac Agencji, przy czym 4 EPC z działania 4 („Umożliwianie współpracy operacyjnej”), 4 EPC z działania 5 („Wspólna reakcja na poziomie Unii i państw członkowskich”) oraz 2,5 EPC z innych działań. W związku z tym w 2023 r. ENISA podjęła kroki w celu obniżenia priorytetu lub ograniczenia niektórych działań i przesunęła zasoby ludzkie na zadania operacyjne wynikające w szczególności z konkretnych zadań przewidzianych w prawodawstwie, co miało negatywny wpływ na inne zadania, które były mniej jasno określone w mandacie ENISA, np. w obszarze umiejętności i świadomości.

Zarządzanie budżetem również stwarza możliwości poprawy. W latach 2019–2022 Agencja odnotowała tendencję spadkową w zakresie równoważenia zatwierdzonych środków i zaciągniętych zobowiązań, ze względu na opóźnienia w działaniach takich jak działania wspierające w obszarze cyberbezpieczeństwa. Odwrócenie tej tendencji i skierowanie wysiłków w stronę zarządzania wydatkami administracyjnymi, w tym rozwiązanie problemu opóźnień

w zamówieniach publicznych, mogłoby przyczynić się do dalszej poprawy wewnętrznej efektywności.

Znaczenie

Znaczenie ENISA w dziedzinie cyberbezpieczeństwa podkreśla jej zdolność do reagowania na zmieniające się potrzeby zainteresowanych stron oraz elastyczność w dostosowywaniu się do zmieniającej się sytuacji. Agencja konsekwentnie wykazywała zdolność do przeglądu i dostosowania swoich obszarów działania w celu uwzględnienia pojawiających się zmian, a tym samym do utrzymania swojej pozycji jako istotnego elementu unijnych ram cyberbezpieczeństwa. Chociaż zadowolenie zainteresowanych stron z wysiłków ENISA jest ogólnie pozytywne, istnieją obszary, w których można jeszcze bardziej podnieść jej znaczenie. Pomimo zdolności do szybkiego reagowania ENISA mogłaby zwiększyć wsparcie i widoczność wśród różnych sektorów i zainteresowanych stron, w szczególności wśród MŚP, które często mają trudności ze spełnieniem wymagań w zakresie cyberbezpieczeństwa. Zmiana w kierunku zapewniania bardziej bezpośrednich narzędzi i zasobów, które są dostosowane do konkretnych sektorów, a także zapewniają wiedzę i narzędzia do przeciwdziałania pojawiającym się zagrożeniom, może zwiększyć wpływ Agencji. Podejście Agencji do angażowania zainteresowanych stron było skuteczne i polegało na wykorzystaniu forów, komitetów i grup roboczych do aktywnego włączania krajowych ekspertów w działania i publikacje. Złożona zdecentralizowana struktura w niektórych państwach członkowskich stwarzała jednak wyzwania, które można by złagodzić dzięki lepszej organizacji i jaśniejszej koordynacji z organami krajowymi. Bieżące inicjatywy Agencji, w tym opracowywanie wytycznych dotyczących cyberbezpieczeństwa i programów budowania zdolności, odzwierciedlają jej zaangażowanie w promowanie współpracy i wzmacnianie wspólnego podejścia do cyberbezpieczeństwa w UE. Promowanie ściślejszej współpracy między sektorami przemysłu i poprawa dostępu do informacji mogłyby zaradzić niektórym ograniczeniom dostrzeganym przez sektor przemysłu. Znaczny potencjał ENISA do poprawy polega na ponownej ocenie priorytetów, usprawnieniu procesów oraz skutecznym pozyskiwaniu nowych odpowiednich zasobów i maksymalizowaniu istniejących zasobów, a tym samym wzmocnieniu jej podstawowej roli w europejskim ekosystemie cyberbezpieczeństwa. Dzięki strategicznemu dostosowaniu do europejskiej strategii cyberbezpieczeństwa zmienione priorytety ENISA mogłyby stworzyć ścieżki prowadzące do zapewnienia bardziej znaczącego wkładu. Zwiększenie zdolności Agencji do oferowania wsparcia politycznego i technicznego może wymagać większych zasobów i bardziej selektywnego charakteru jej zaangażowania oraz udoskonalenia jej obszarów operacyjnych. Podsumowując, chociaż znaczenie ENISA jest oczywiste, nadal można wprowadzić udoskonalenia. Przez zmianę priorytetów działań oraz zapewnienie większych i optymalizację istniejących zasobów ENISA może podnieść zarówno efektywność, jak i ogólny wpływ, przez ściślejsze dostosowanie się do dynamicznych wymogów europejskiego krajobrazu cyberbezpieczeństwa.

Spójność

W kwestii spójności ENISA w ocenie podkreślono zarówno mocne strony, jak i obszary wymagające poprawy. Zaangażowanie ENISA w promowanie współpracy w zakresie cyberbezpieczeństwa na szczeblu UE jest oczywiste, w szczególności przez ułatwianie i prowadzenie bezpośredniej współpracy z zainteresowanymi stronami. To dwutorowe podejście umożliwiło ENISA wniesienie znacznego wkładu w dziedzinie cyberbezpieczeństwa, zgodnie

z najnowszymi ramami prawnymi. Chociaż rola ENISA jako podmiotu ułatwiającego i koordynującego jest pozytywna, kilka obszarów wymaga jednak poprawy w celu zwiększenia spójności. W ocenie wskazano na potrzebę poprawy synergii między obowiązkami i działaniami ENISA a obowiązkami i działaniami innych organów UE, takich jak Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), a także krajowych organów ds. cyberbezpieczeństwa. Chociaż role te często się uzupełniają, istnieją możliwości dalszego usprawnienia działań i poprawy efektywności organizacyjnej. Przez sformalizowanie uzgodnień dotyczących współpracy z innymi podmiotami, takimi jak EMSA i JRC, ENISA mogłaby lepiej wykorzystać synergie i zapewnić jednolite podejście do inicjatyw w zakresie cyberbezpieczeństwa. Należy również udoskonalić komunikację wewnętrzną i zarządzanie zasobami w ramach ENISA. Współpraca Agencji z zainteresowanymi stronami z sektora prywatnego i partnerami międzynarodowymi musi być bardziej przewidywalna i przejrzysta, aby utrzymać zaufanie i wspierać wspólne wysiłki. Zgodnie z aktem o cyberodporności i dyrektywą NIS 2 jasne określenie zadań ENISA związanych ze wspieraniem wdrażania polityki mogłoby zwiększyć efektywność i zapewnić spójność środków regulacyjnych. Jasność ta poprawiłaby również zdolność ENISA do reagowania na sektorowe wymogi regulacyjne. Podsumowując, chociaż ENISA wykazała, że posiada solidne podstawy w promowaniu spójności cyberbezpieczeństwa w UE, istnieją możliwości zmiany priorytetów jej działań. Takie podejście pomoże jej skutecznie wypełniać mandat i dostosowywać się do zmieniającego się krajobrazu cyberbezpieczeństwa. Przez rozwiązanie obecnych problemów związanych z nieefektywnością i poprawienie koordynacji między agencjami ENISA może skutecznie utrzymać swoją kluczową rolę w unijnych ramach bezpieczeństwa cybernetycznego.

Unijna wartość dodana

ENISA w znacznym stopniu przyczyniła się do wzmocnienia unijnego ekosystemu cyberbezpieczeństwa, ale istnieją możliwości poprawy, które mogłyby zwiększyć jej wpływ. Pełniąc rolę scentralizowanego ośrodka, ENISA ułatwiała kluczową współpracę w całej UE, uzupełniała działania krajowe, zwłaszcza w państwach członkowskich o słabiej rozwiniętej infrastrukturze cyberbezpieczeństwa, oraz dostosowywała praktyki i polityki w zakresie cyberbezpieczeństwa. Wyspecjalizowany mandat ENISA jako zdecentralizowanej agencji UE umożliwił jej konsolidację wiedzy fachowej w zakresie cyberbezpieczeństwa i skuteczną współpracę z państwami członkowskimi, a także odgrywanie kluczowej roli w kształtowaniu europejskiego krajobrazu cyberbezpieczeństwa. W tym kontekście zasadnicze znaczenie ma skupienie uwagi ENISA na państwach członkowskich, ze względu na jej rolę w dostarczaniu informacji na temat pojawiających się zagrożeń oraz rekomendowaniu narzędzi i strategii służących przeciwdziałaniu im. Agencja mogłaby jeszcze bardziej zacieśnić współpracę międzynarodową, zgodnie z priorytetami Unii, w tym z partnerami w państwach trzecich, organizacjami międzynarodowymi i agencjami ds. cyberbezpieczeństwa, aby lepiej reagować na globalny charakter cyberzagrożeń. Ponadto ENISA odgrywa kluczową rolę w promowaniu certyfikacji cyberbezpieczeństwa i wspieraniu działań normalizacyjnych, co pomaga zmniejszyć fragmentację rynku i wspiera solidne praktyki w zakresie cyberbezpieczeństwa w całej UE. Pomimo braku podobnych organów, które dysponowałyby wiedzą fachową i sprawnością organizacyjną ENISA, jej dotychczasowe skupianie uwagi głównie na organach krajowych spotkało się z krytyką ze strony zainteresowanych stron z sektora prywatnego. Informacje zwrotne od dużych podmiotów branżowych wskazują, że można byłoby uczynić więcej, by dostosować informacje do szczególnych wyzwań sektora prywatnego. Chociaż ukierunkowanie przede

wszystkim na organy krajowe ma kluczowe znaczenie, strategiczne zwiększenie zaangażowania zainteresowanych stron i zacieśnienie współpracy z przemysłem mogłoby stanowić odpowiedź na te sygnały. Ponadto w mandacie ENISA mogłyby zostać wprowadzone korzystne zmiany w wyniku strategicznej ponownej oceny jej priorytetów w celu sprawnego dostosowania do zmieniających się wyzwań w zakresie cyberbezpieczeństwa. Umożliwiłoby to ENISA dalsze wnoszenie cennego wkładu w UE, a jednocześnie skuteczne zaspokajanie rosnących potrzeb różnych zainteresowanych stron.

Najważniejsze osiągnięcia i wyzwania

ENISA cieszy się powszechnym uznaniem w unijnej społeczności zajmującej się cyberbezpieczeństwem dzięki solidnej reputacji, wysokiej jakości publikacjom oraz znaczącej roli we wspieraniu współpracy między państwami członkowskimi i innymi podmiotami zajmującymi się cyberbezpieczeństwem. Prace ENISA przyczyniające się do harmonizacji wymagań w zakresie cyberbezpieczeństwa mają kluczowe znaczenie dla ustanowienia spójnego poziomu ochrony we wszystkich państwach członkowskich, ponieważ wnoszą bezpośredni wkład w budowanie zdolności, zwłaszcza w przypadku mniejszych państw członkowskich. Harmonizacja ta nie tylko zapewnia bezpieczne środowisko cyfrowe w całej UE, ale również zwiększa gotowość wszystkich zainteresowanych stron do reagowania w obszarze cyberbezpieczeństwa.

W ocenie wskazano jednak szereg wyzwań, przed którymi stoi ENISA. ENISA ma ograniczoną sprawność w reagowaniu na zmieniające się zagrożenia cyberbezpieczeństwa, co może prowadzić do potencjalnych opóźnień w jej działaniach. Aby złagodzić wyzwania związane z ograniczonymi zasobami, zainteresowane strony, z którymi przeprowadzono konsultacje², podkreśliły m.in. potrzebę poprawy procesów rekrutacji i strategii zarządzania obciążeniem pracą. Rozszerzenie mandatu ENISA w celu wzmocnienia jej roli operacyjnej mogłoby rozwiązać te problemy i umożliwić jej wykorzystanie postępu technologicznego i poprawę ram cyberbezpieczeństwa. Restrukturyzacja ta umożliwiłaby ENISA proaktywne przeciwdziałanie dynamicznym zagrożeniom i zwiększyłaby jej wpływ dzięki wspólnym inicjatywom szkoleniowym i wkładowi w procesy kształtowania polityki.

Ponadto systemy konsultacji z zainteresowanymi stronami i systemy zarządzania ENISA uznaje się za skuteczne w ułatwianiu zarządzania potrzebami i oczekiwaniami zainteresowanych stron, ale konieczne jest zacieśnienie i zwiększenie przejrzystości stosunków z państwami członkowskimi w celu rozszerzenia współpracy i wymiany informacji. Przyszłe priorytety obejmują aktualizację wewnętrznych ram organizacyjnych, umożliwiającą lepsze radzenie sobie z rosnącymi obowiązkami i różnymi wyzwaniami i zapewniającą ENISA zdolność do pełnej realizacji powierzonych jej zadań, z uwzględnieniem liczby zatrudnionych pracowników.

2.2 ECCF

W niniejszej sekcji przedstawiono główne ustalenia z oceny ECCF i skoncentrowano się na ich skuteczności, efektywności, znaczeniu i spójności oraz wartości dodanej, jaką wnoszą one do unijnego krajobrazu cyberbezpieczeństwa. Podsumowano też najważniejsze zidentyfikowane mocne i słabe strony ram na podstawie analizy SWOT.

Skuteczność

ECCF zostały pomyślane jako filar poprawy zapewniania cyberbezpieczeństwa na całym rynku wewnętrznym UE, mający na celu harmonizację certyfikacji produktów, usług i procesów ICT. Zostały one wprowadzone w celu rozwiązania utrzymujących się problemów, takich jak fragmentacja rynku oraz potrzeba zwiększenia przejrzystości rozwiązań cyfrowych i zaufania publicznego do nich. Dzięki ustrukturyzowanemu modelowi zarządzania obejmującemu podmioty takie jak ENISA, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa (ECCG) i sieć krajowych organów ds. certyfikacji cyberbezpieczeństwa ECCF stworzyły podstawy dla zwiększonej koordynacji między zainteresowanymi stronami, w tym państwami członkowskimi i podmiotami prywatnymi. Praktyczna realizacja tych celów wiązała się jednak z licznymi wyzwaniami, które ograniczyły skuteczność ECCF. Istotną słabością obecnych ECCF jest ich niezdolność do skutecznego wyeliminowania fragmentacji systemów certyfikacji w całej UE, głównie ze względu na ograniczenia proceduralne. Fragmentacja ta utrzymuje się pomimo przewidzianego w tych ramach zamiaru harmonizacji procesów certyfikacji, co prowadzi do niespójności i nieefektywności w zapewnianiu cyberbezpieczeństwa. Przejawia się to znacznym opóźnieniem w uruchomieniu pierwszego systemu certyfikacji, tj. wspólnych kryteriów UE (EUCC), które trwało 57 miesięcy od momentu zainicjowania do przyjęcia. Opóźnienie to wskazuje na nieefektywność procesów ECCF, na którą wpływ mają głównie złożone i wieloaspektowe procedury zatwierdzania. Ponadto niejednoznaczność co do odpowiedzialności i rozliczalności wśród zainteresowanych stron jeszcze bardziej skomplikowała realizację celów tych ram. Czynniki zewnętrzne dodatkowo utrudniały realizację celów ECCF. Zmieniający się krajobraz geopolityczny, charakteryzujący się rosnącymi cyberzagrożeniami i napięciami politycznymi związanymi z suwerennością danych i kontrolą cyfrową, wymagał podjęcia środków adaptacyjnych, z których szybkim wdrożeniem w ECCF wystąpiły trudności. Ta presja zewnętrzna spowodowała opóźnienia w przyjmowaniu systemu, co widać na przykładzie EUCS (europejskiego programu certyfikacji cyberbezpieczeństwa dla usług w chmurze), w przypadku którego dyskusje utknęły w martwym punkcie z powodu debat o charakterze nietechnicznym, na przykład w sprawie wymagań dotyczących lokalizacji danych. Pomimo tych przeszkód odnotowano pozytywne wyniki – w szczególności w zwiększaniu wiedzy w państwach członkowskich na temat znaczenia i złożoności certyfikacji cyberbezpieczeństwa. Pandemia COVID-19, która spowodowała opóźnienia operacyjne, podkreśliła również konieczność posiadania odpornej infrastruktury cyfrowej i sprawiła, że cyberbezpieczeństwo znalazło się w centrum polityki. Pandemia COVID-19 miała zarówno negatywny, jak i pozytywny wpływ na ECCF. Jeśli chodzi o aspekty „negatywne”, nagłe przejście na spotkania online przyczyniło się do opóźnień w procesach opracowywania systemu. Jeśli chodzi o aspekty „pozytywne”, pandemia COVID-19 zwiększyła świadomość znaczenia odpornych łańcuchów dostaw, które są mniej zależne od państw trzecich. Jednocześnie w analizie wskazano kluczowe wnioski i zwrócono uwagę na nierównomierny przydział zasobów wśród zainteresowanych stron, w tym państw członkowskich, co utrudnia jednolite opracowywanie i wdrażanie systemów certyfikacji. Wyeliminowanie tych różnic ma zasadnicze znaczenie dla przyszłej efektywności i skuteczności, w szczególności przez zatrzymanie wykwalifikowanego personelu w ENISA i wspieranie stałego dialogu między wszystkimi zaangażowanymi stronami.

Efektywność

Efektywność ECCF była przedmiotem kontroli ze względu na wydłużone terminy przyjmowania systemów certyfikacji cyberbezpieczeństwa i dużą złożoność tych systemów. Pomimo strategicznego zamiaru usprawnienia procesu certyfikacji w całej UE efektywność ECCF była

znacznie ograniczona ze względu na przeciągające się dyskusje i fazy przygotowawcze, które doprowadziły do znacznych opóźnień; pierwszy system przyjęto dopiero na początku 2024 r., prawie pięć lat po wdrożeniu. Te przedłużające się terminy można tłumaczyć wielowymiarowymi wyzwaniami, które obejmują kwestie zarówno polityczne, jak i techniczne.

Wyzwania polityczne, w tym upolitycznienie dyskusji na temat wymogów certyfikacji, utrudniły postępy, gdyż tworzyły środowisko negatywnie oddziałujące na przejrzystość i komunikację. Na przykład na europejski program certyfikacji cyberbezpieczeństwa dla usług w chmurze (EUCS) znaczący wpływ miały debaty dotyczące wymogów suwerenności danych, wywierające presję polityczną ze strony państw trzecich i przemysłu spoza UE, co doprowadziło do przejścia od dyskursu technicznego do politycznego w ramach ECCG.

Złożoność techniczna dodatkowo przyczyniła się do nieefektywności, w szczególności trudności w przełożeniu projektów systemów na akty prawne, ze względu na zróżnicowany i wymagający charakter produktów/usług poddanych certyfikacji, takich jak sieci 5G i przetwarzanie w chmurze. Szeroki zakres wniosków i brak ustalonych norm w niektórych obszarach jeszcze bardziej utrudniły proces przygotowania i przyjęcia, gdyż wymagały od wielu zainteresowanych stron zapewnienia zgodności z istniejącymi politykami i praktykami na wielu etapach. Pomimo tych przypadków nieefektywności ramy dostarczyły kilku pozytywnych elementów. Utworzenie specjalnych grup i forów, w tym Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa (ECCG), grupy roboczej ad hoc (AHWG) zajmującej się konkretnymi systemami oraz grupy zainteresowanych stron ds. certyfikacji cyberbezpieczeństwa (SCCG), ułatwiło niezbędne zaangażowanie zainteresowanych stron. Niemniej jednak nadal pozostaje wiele do zrobienia, jeśli chodzi o zapewnienie optymalnego funkcjonowania tych struktur; na przykład członkowie SCCG zauważyli brak zaangażowania grupy w ECCF. Udoskonalenie wewnętrznego zarządzania ma kluczowe znaczenie dla aktywnego uczestnictwa i strategicznego wkładu zainteresowanych stron.

Znaczenie

ECCF okazują się kluczową odpowiedzią na rosnącą złożoność i coraz większe zaawansowanie cyberzagrożeń w całej UE, gdyż dążą do ustanowienia zharmonizowanych systemów certyfikacji cyberbezpieczeństwa, które zapewniają zaufanie i wspierają bezpieczny rynek cyfrowy. Pomimo obiecującego założenia znaczenie tych ram nadal uznaje się za bardziej potencjalne niż praktyczne, a systemy certyfikacji dopiero niedawno weszły w fazę operacyjną. To opóźnienie w osiągnięciu wymiernych rezultatów uwypukla rozbieżności w realizacji i stawia pod znakiem zapytania obecną pozycję ECCF w krajobrazie cyberbezpieczeństwa. Znaczenie ECCF polega na ich strategicznej roli w podnoszeniu standardów cyberbezpieczeństwa i umożliwianiu wzajemnego uznawania certyfikacji we wszystkich państwach członkowskich, co pozwala obniżyć koszty ponoszone przez poszczególne przedsiębiorstwa i usprawnić funkcjonowanie rynku wewnętrznego. Ramy te mają na celu silną integrację z innymi aktami prawnymi UE, aby usprawnić procedury i ułatwić handel transgraniczny.

Kilka czynników podnosi znaczenie ECCF pomimo wyzwań, jakim muszą sprostać w realizacji zadań. Gwałtowny wzrost liczby cyberzagrożeń znacznie zwiększa potrzebę wspólnej strategii cyberbezpieczeństwa, która będzie mogła szybko dostosowywać się do zmieniających się scenariuszy, na przykład rosnącego znaczenia certyfikacji w obszarach o wysokim poziomie bezpieczeństwa, takich jak usługi w chmurze i infrastruktura 5G. Wymogi dotyczące zamówień publicznych w tych sektorach odzwierciedlają rosnące zapotrzebowanie na jednolite i wiarygodne

ramy certyfikacji – zapotrzebowanie, które ECCF mogą zaspokoić. Ponadto powiązanie ECCF z powstającymi aktami ustawodawczymi, w szczególności z aktem o cyberodporności i dyrektywą NIS 2 (bezpieczeństwo sieci i informacji), podkreśla ich oczekiwaną wartość w zaspokajaniu potrzeb w zakresie infrastruktury krytycznej i zapewnianiu zgodności z prawem w całej UE. Proaktywna rola ENISA i ustanowienie krajowych organów ds. certyfikacji cyberbezpieczeństwa stanowią kluczowe etapy na drodze do zacieśnienia współpracy i promowania stosowania certyfikacji. Jednak nierówności w alokacji zasobów i w wiedzy fachowej między większymi i mniejszymi państwami członkowskimi nadal jednak utrwalają nierównowagę pod względem uczestnictwa i skuteczności, co ma wpływ na rozwój zbiorowych systemów.

Spójność

Na spójność ECCF wpływa również brak jasnych mechanizmów rozliczalności, co utrudnia dostosowanie ich celów do innych środków ustawodawczych. To niedostosowanie stwarza ryzyko nakładania się działań i nieefektywności w obszarze cyberbezpieczeństwa. Pełna spójność ECCF z innymi instrumentami prawnymi UE, w tym dyrektywą NIS 2 i aktem o cyberodporności, ma kluczowe znaczenie dla zapewnienia jednolitego podejścia do cyberbezpieczeństwa. ECCF wykazują teoretyczne dostosowanie do tych środków ustawodawczych, mające na celu uwzględnienie różnych aspektów cyberbezpieczeństwa w krajobrazie UE, jednak ich rzeczywista integracja pozostaje złożona i wymaga starannego nadzoru. Zbliżające się wdrożenie unijnego systemu wspólnych kryteriów (EUCC) stanowi istotny sprawdzian tej spójności, ponieważ jego pomyślne wdrożenie wykaże zdolność ECCF do harmonizacji i skutecznego wykorzystania dodatkowych działań legislacyjnych. Zainteresowane strony podkreśliły potrzebę starannej koordynacji między ECCF a powstającymi aktami regulacyjnymi, aby zapobiec nakładaniu się przepisów, co mogłoby osłabić efektywność i zmniejszyć zamierzone skutki w różnych sektorach. W szczególności pojawiają się obawy dotyczące powiązania między ECCF a aktem o cyberodporności, ponieważ obie inicjatywy mają na celu poprawę norm cyberbezpieczeństwa, ale wiążą się z ryzykiem nadmiarowości, jeżeli nie będą stosowane w pełnej synergii, w ramach której jedno prawodawstwo wspiera i uzupełnia drugie. W wymiarze sektorowym spójność musi obejmować uwzględnianie ciągłego postępu technologicznego oraz zapewnienie odpowiedniego dostosowania inicjatyw w zakresie cyberbezpieczeństwa do potrzeb infrastruktury krytycznej.

Unijna wartość dodana

Pomimo potencjału zawartego w ECCF wystąpiły trudności z urzeczywistnieniem ich wartości dodanej pod względem wspierania jednolitego i skutecznego środowiska cyberbezpieczeństwa w całej UE. ECCF miały na celu znaczną poprawę krajobrazu cyberbezpieczeństwa UE przez wprowadzenie bezprecedensowej procedury rozwoju procesów certyfikacji i struktury zarządzania nimi. W swojej istocie ECCF stanowiły kluczowy krok naprzód w zakresie zdolności UE do stworzenia zharmonizowanego podejścia do certyfikacji produktów, usług i procesów ICT. Nieodłączną unijną wartością dodaną tych ram jest ich potencjał zbliżania rozbieżnych podejść krajowych i wspierania rynku wewnętrznego przez spójne, niezawodne i uznane normy cyberbezpieczeństwa we wszystkich państwach członkowskich. Przedłużające się ramy czasowe i fragmentaryczne wdrażanie systemów ograniczyły jednak możliwość pełnego wykorzystania zakładanej wartości ECCF. W szczególności opóźnienie we wprowadzaniu systemów, czego dowodem jest późne przyjęcie inicjatyw takich jak wspólne kryteria UE (EUCC), ograniczyło

bezpośrednie skutki i spowodowało, że teoretyczny potencjał ECCF pozostał w dużej mierze niewykorzystany. Rozbieżności we wdrażaniu systemowym, potęgowane różnym stopniem gotowości i dostępności zasobów w poszczególnych państwach członkowskich, jeszcze bardziej osłabiają kompleksowy wpływ ram. ECCF ożywiły jednak dynamikę współpracy w całej UE. Przez ustanowienie grup takich jak ECCG zinstytucjonalizowały one działania koordynacyjne i umożliwiły szersze zaangażowanie na różnych szczeblach sprawowania rządów. Ta infrastruktura współpracy zachęca do wymiany informacji i tworzenia wspólnych strategii oraz promuje jednolite podejście do cyberbezpieczeństwa w obliczu ewoluujących zagrożeń. Aby w pełni wykorzystać unijną wartość dodaną ECCF, kluczowe znaczenie ma zwiększony i spójny udział zainteresowanych stron. Wspieranie integracyjnego środowiska, w którym partnerzy branżowi, organy krajowe i organy UE aktywnie uczestniczą w procesie certyfikacji i wyznaczają jego kierunki, zapewni powszechną akceptację i skuteczność norm cyberbezpieczeństwa.

Najważniejsze osiągnięcia i wyzwania

ECCF pełnią rolę kluczowego narzędzia zacieśniania współpracy na szczeblu UE między ENISA, państwami członkowskimi i sektorami przemysłu, co zwiększa ich znaczenie w dynamicznym środowisku cyberbezpieczeństwa. Ich elastyczność ułatwia opracowywanie systemów za pośrednictwem grup roboczych ad hoc i jest zgodna z ramami prawnymi UE, takimi jak NIS2. Potencjał ten, choć znaczący, pozostaje w dużej mierze niewykorzystany ze względu na ograniczone wdrażanie rzeczywistych programów.

ECCF mają kluczowe znaczenie dla przeciwdziałania pojawiającym się zagrożeniom cyberbezpieczeństwa i dla wspierania zgodności z przepisami, w szczególności zaś wykorzystywania nowych technologii, takich jak sztuczna inteligencja. Zainteresowane strony uznają ich rolę w zacieśnianiu współpracy państw członkowskich i poprawie gotowości do reagowania w obszarze cyberbezpieczeństwa. Uznaje się również ich wartość we wspieraniu wymiany na rynku wewnętrznym przez zastępowanie krajowych systemów certyfikacji systemami ogólnounijnymi.

Jednak funkcjonowanie ECCF utrudniają poważne słabości. Długotrwałe procesy przyjmowania systemów ograniczają skuteczność ECCF, a problem ten dodatkowo pogłębia złożoność techniczna i presja polityczna ze strony lobby branżowego. Opóźnienia te podważają zaufanie i uniemożliwiają szybkie przyjęcie europejskich systemów certyfikacji bezpieczeństwa cybernetycznego. ECCF mają szansę wzmocnić ramy UE dotyczące cyberbezpieczeństwa, ale zagrożenia, takie jak ograniczone zasoby i napięcia geopolityczne, stanowią wyzwanie. Zmiany priorytetów politycznych i potencjalne nakładanie się przepisów mogą mieć wpływ na skuteczność ram i stwarzają ryzyko niespójności na rynku. Rozwiązanie tych kwestii ma zasadnicze znaczenie dla zapewnienia przekształcenia ECCF z obiecującej koncepcji w pełni operacyjny mechanizm, który wzmacnia standaryzację i certyfikację cyberbezpieczeństwa w UE.

3. WNIOSKI I ZALECENIA

3.1 ENISA

W ocenie ENISA podkreślono jej kluczową rolę w działaniach na rzecz spójnego krajobrazu cyberbezpieczeństwa w całej UE. ENISA wykazała swoją skuteczność i dostarczyła wartościowe

wyniki. W związku z rosnącymi wymaganiami wobec ENISA ważne jest, aby ponownie ocenić i usprawnić jej działania w celu lepszego dostosowania zasobów i priorytetów, przy dalszym nacisku na wspieranie państw członkowskich w radzeniu sobie z zagrożeniami cyberbezpieczeństwa i wzmacnianiu krajowej infrastruktury cyberbezpieczeństwa. Udoskonalenie procesu sporządzania sprawozdań, zwiększenie ich przyjazności dla użytkownika i dostępności przez zastosowanie pomocy wizualnych i zwięzłych streszczeń mogłoby zwiększyć skuteczność i znaczenie ENISA w obecnym krajobrazie zagrożeń. Wzmocnienie kanałów komunikacji ma zasadnicze znaczenie dla sprawienia, aby działania i usługi ENISA były wyraźnie widoczne dla zainteresowanych stron, w tym podmiotów z branży. Dobrze określona strategia komunikacyjna mogłaby pomóc w budowaniu silniejszych powiązań i współpracy w ramach istniejących sieci cyberbezpieczeństwa, takich jak ISAC.

ENISA może poprawić efektywność przez bardziej strategiczne podejście do ustalania priorytetów zadań, co umożliwi bardziej usprawnione zarządzanie obciążeniem pracą. Aby zwiększyć znaczenie wśród zainteresowanych stron, należy nadal wzmacniać centralną rolę ENISA we wspieraniu państw członkowskich przez poprawę jej zdolności do terminowego dostarczania informacji na temat pojawiających się zagrożeń i strategicznych narzędzi reagowania na nie. Ponadto, jak wskazało wiele zainteresowanych stron, ENISA mogłaby ustanowić bardziej ustrukturyzowane i przejrzyste metody współpracy z podmiotami prywatnymi, w tym wspierania MŚP. Należy dążyć do jasnego określenia roli ENISA we wdrażaniu polityki z innymi instytucjami UE i sprawić, aby współpraca z państwami członkowskimi zajmowała główne miejsce w tych wysiłkach na rzecz zwiększenia spójności jednolitej strategii UE w zakresie cyberbezpieczeństwa, co obejmowałoby również zacieśnienie współpracy z innymi agencjami UE oraz dążenie do synergii z innymi organami ds. cyberbezpieczeństwa na potrzeby wspólnych działań zmierzających do zwiększenia spójności operacyjnej w całej Europie.

Ogólnie rzecz biorąc, utrzymanie statusu ENISA jako wyspecjalizowanej agencji w ramach UE jest ważne, ponieważ zapewnia stałe skupienie się na priorytetach w zakresie cyberbezpieczeństwa. Zalecenia te mają na celu zwiększenie zdolności ENISA do skutecznego zarządzania obowiązkami i potwierdzenie jej roli jako wiodącego podmiotu w dziedzinie cyberbezpieczeństwa.

3.2 ECCF

W ocenie ECCF wskazano szereg zaleceń strategicznych. Po pierwsze, pomimo kluczowej roli ENISA we wspieraniu współpracy i spójności operacyjnej między państwami członkowskimi i innymi zainteresowanymi stronami ograniczenia wydajności i skuteczności ECCF były widoczne głównie ze względu na złożoność procesów przyjmowania systemów. Kwestie te podkreślają konieczność gruntownej zmiany struktur zarządzania w celu zwiększenia przejrzystości działania i rozliczalności na wszystkich szczeblach.

Aby uwzględnić te ustalenia, zaleca się podjęcie szeregu działań w celu optymalizacji wkładu ENISA w ECCF. Należy podjąć wspólne wysiłki w celu zapewnienia spójnego i odpowiedniego podziału zasobów finansowych i ludzkich między ENISA i inne zainteresowane strony w ramach ECCF. Stabilizacja warunków zatrudnienia ma zasadnicze znaczenie dla zmniejszenia rotacji i zwiększenia pamięci instytucjonalnej, a tym samym ułatwienia skutecznego wdrażania systemu i jego bieżącej obsługi. Opracowanie usprawnionych procesów decyzyjnych w ramach ECCF,

które doprecyzowują role i obowiązki, przyczyni się do zwiększenia przejrzystości i efektywności, w szczególności przez zacieśnienie współpracy między państwami członkowskimi, Komisją i ENISA. Przyczyni się to do zwiększenia rozliczalności i zmniejszenia nieefektywności. Zasadnicze znaczenie ma zobowiązanie do ustalania i przestrzegania realistycznych harmonogramów opracowywania i wdrażania systemów certyfikacji. Obejmuje to wspieranie szczegółowej analizy technicznej i intensyfikację działań przygotowawczych w celu skutecznego przewidywania i łagodzenia wpływów politycznych.

Ponadto aktywne inwestowanie w szkolenie i zatrzymywanie wykwalifikowanego personelu w ENISA ma kluczowe znaczenie dla zapewnienia ciągłości i wiedzy fachowej potrzebnej do radzenia sobie ze złożonymi wyzwaniami w zakresie cyberbezpieczeństwa. Długoterminowa stabilność siły roboczej będzie niezbędna do utrzymania skuteczności operacyjnej ECCF. Należy też zwiększać świadomość przemysłu i konsumentów przez ukierunkowane kampanie i strategiczne zaangażowanie oraz podkreślać wartość certyfikowanych produktów i usług. Proaktywne podejście do uzyskiwania wsparcia zainteresowanych stron ma zasadnicze znaczenie dla zwiększenia zapotrzebowania na inicjatywy ECCF i zaufania do nich.