

Wykrywanie cyberincydentów i reagowanie na nie

Budowa unijnych ram współpracy postępuje, ale są one tylko częściowo skuteczne ze względu na opóźnienia we wdrażaniu i niewielką wymianę informacji



EUROPEJSKI
TRYBUNAŁ
OBRACHUNKOWY

Spis treści

Punkty

01-23 | **Najważniejsze informacje o kontroli**

01-07 | Dlaczego Trybunał skontrolował ten obszar?

08-23 | Co ustalił i zaleca Trybunał?

24-01 | **Omówienie uwag Trybunału**

24-74 | Unijne sieci i mechanizmy cyberbezpieczeństwa ułatwiają współpracę i reagowanie, lecz niewielki zakres wymiany informacji i niepełne wdrożenie zmniejszają skuteczność wprowadzonych rozwiązań

24-51 | Unijne sieci umożliwiają współpracę między państwami członkowskimi, ale niewielki zakres wymiany informacji zmniejsza wartość dodaną tych sieci

52-61 | Unijna rezerwa cyberbezpieczeństwa umożliwia szybkie skorzystanie z usług reagowania na incydenty

62-74 | Europejski system cyberostrzeżeń ma na celu udoskonalenie wykrywania zagrożeń, ale jeszcze nie funkcjonuje

75-01 | Niektóre projekty finansowane przez UE w ramach programu „Cyfrowa Europa” mają na celu wzmocnienie cyberbezpieczeństwa, ale kontrolerzy odnotowali problemy, jeśli chodzi o wdrożenie i sprawozdawczość

75-81 | Opóźnienia w ustanowieniu społeczności kompetentnej w zakresie cyberbezpieczeństwa uniemożliwiły jej wzięcie udziału w ukształtowaniu programu „Cyfrowa Europa”, tak aby uwzględnił jej potrzeby

82-96 | Projekty finansowane przez UE służą realizacji odpowiednich celów, ale w przypadku wielu z nich występują trudności operacyjne

97-01 | W przypadku większości projektów finansowanych przez UE przyjęte ramy wykonania są nieodpowiednie, a dane dotyczące wyników programu „Cyfrowa Europa” związanych z cyberbezpieczeństwem nie są poprawne

Załączniki

Załącznik I – O kontroli

Załącznik II – Środowisko UE w dziedzinie cyberbezpieczeństwa

Załącznik III – Wybrane działania w zakresie cyberbezpieczeństwa

Załącznik IV – Przeprowadzona przez Trybunał ocena projektów w dziedzinie cyberbezpieczeństwa sfinansowanych ze środków UE

Akronimy

Glosariusz

Odpowiedzi Komisji

Odpowiedzi Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC)

Odpowiedzi Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

Kalendarium

Zespół kontrolny

Najważniejsze informacje o kontroli

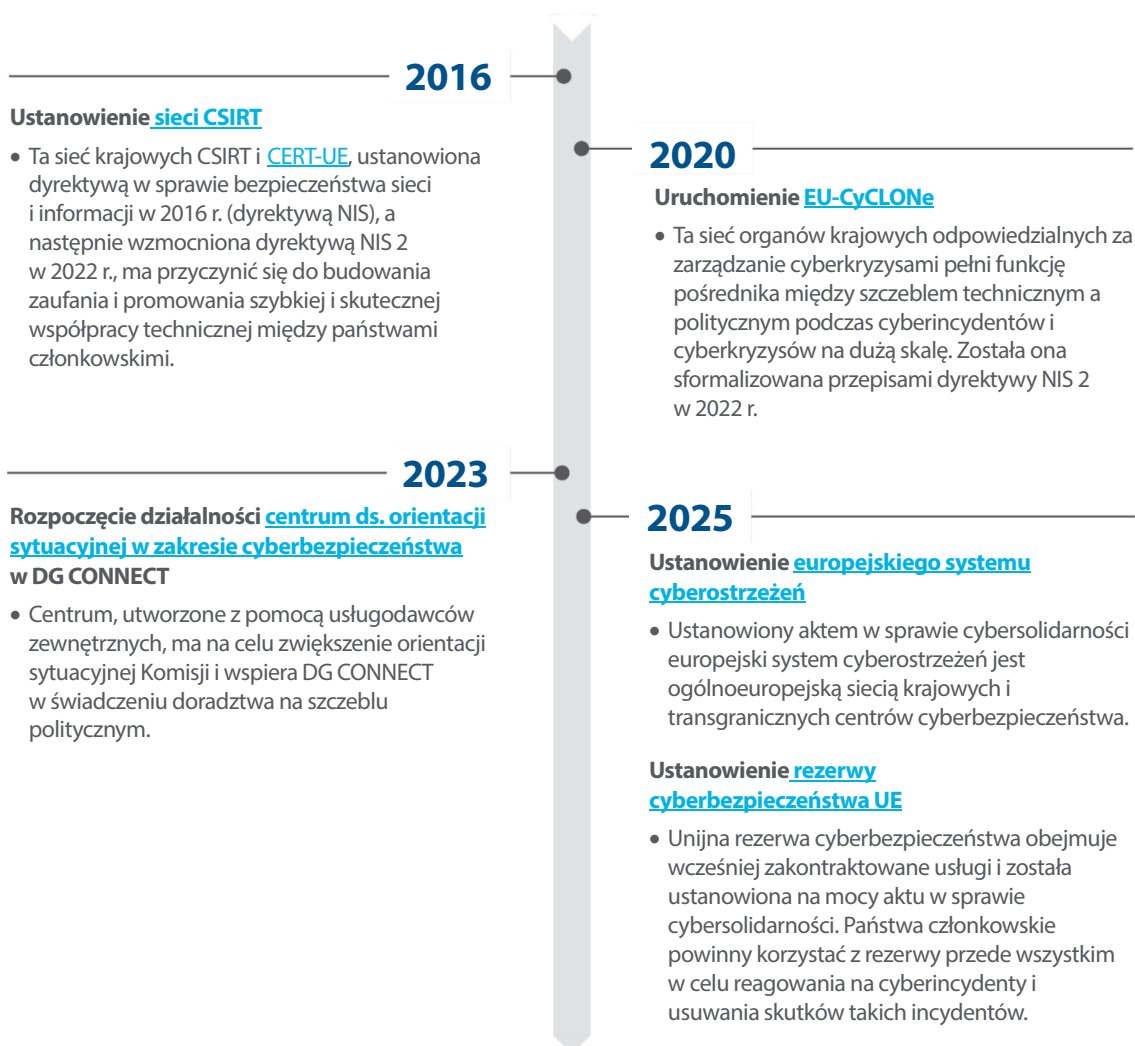
Dlaczego Trybunał skontrolował ten obszar?

- 01** Wraz z postępującą cyfryzacją europejskiej gospodarki i codziennego życia rośnie ryzyko cyberataków. Cyberbezpieczeństwo definiuje się jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”¹. Zapewnienie cyberbezpieczeństwa wymaga przyjęcia całościowego podejścia do zapobiegania cyberzagrożeniom, ich wykrywania, reagowania na nie i usuwania ich skutków.
- 02** W UE w zapewnianie cyberbezpieczeństwa są zaangażowane liczne cywilne podmioty publiczne i prywatne na szczeblu regionalnym, krajowym i unijnym. Cyberbezpieczeństwo jest ponadto kluczowym elementem bezpieczeństwa narodowego i obrony narodowej.
- 03** Odpowiedzialność za zapobieganie incydentom i sytuacjom kryzysowym związanym z cyberbezpieczeństwem oraz przygotowywanie się i reagowanie na nie ponoszą przede wszystkim państwa członkowskie, których dany incydent bądź sytuacja kryzysowa dotyczą. Ponieważ incydenty te mogą mieć wpływ na sprawne funkcjonowanie rynku wewnętrznego, również UE ma do odegrania ważną rolę w przypadku wystąpienia poważnego incydentu lub kryzysu. W ostatnich latach UE doskonaliła i wciąż aktualizowała ramy regulacyjne w zakresie cyberbezpieczeństwa² oraz ustanowiła odpowiednie sieci i mechanizmy. Informacje na ten temat przedstawiono na **rys. 1** poniżej i w **załączniku II**.

¹ Rozporządzenie (UE) 2019/881 („akt o cyberbezpieczeństwie”).

² Na przykład w listopadzie 2025 r. Komisja zaproponowała **akt zbiorczy prawa cyfrowego**, a w styczniu 2026 r. – zmieniony **unijny akt o cyberbezpieczeństwie**.

Rys. 1 | Unijne sieci i mechanizmy w zakresie cyberbezpieczeństwa w latach 2016–2025



CSIRT – zespoły reagowania na incydenty bezpieczeństwa komputerowego

DG CONNECT – Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii

EU-CyCLONe – europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa

Dyrektywa w sprawie bezpieczeństwa sieci i informacji (dyrektywa NIS) – dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

Dyrektywa NIS 2 – dyrektywa (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii

Źródło: Europejski Trybunał Obrachunkowy.

- 04** W bieżących wieloletnich ramach finansowych na lata 2021–2027 głównym źródłem finansowania na rzecz cyberbezpieczeństwa jest [program „Cyfrowa Europa”](#). Całkowity budżet programu wynosi 8,1 mld euro, z czego 1,4 mld euro przewidziano na poprawę cyberbezpieczeństwa.
- 05** Celem kontroli Trybunału była ocena, na ile skutecznie działania UE ułatwiają wykrywanie poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, a także reagowanie na nie. Trybunał przeanalizował sytuację w odniesieniu do:
- sieci i mechanizmów funkcjonujących na szczeblu UE (tj. sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego – sieci CSIRT, europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa – EU-CyCLONe, europejskiego systemu cyberostrzeżeń, centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa oraz rezerwy cyberbezpieczeństwa UE);
 - działań sfinansowanych w ramach programu „Cyfrowa Europa”.
- 06** Trybunał oczekuje, że ustalenia zawarte w niniejszym sprawozdaniu przyczynią się do poprawy cyberodporności UE dzięki zwiększeniu skuteczności i efektywności unijnych sieci i mechanizmów, a także dzięki usprawnieniu procesu wyboru i monitorowania działań finansowanych przez UE.
- 07** Przeprowadzona kontrola objęła lata 2022–2025. Ustalenia sformułowano na podstawie przeglądu dokumentacji i analizy odpowiednich dokumentów, wizyt kontrolnych w trzech państwach członkowskich (w Irlandii, Grecji i we Włoszech) oraz na podstawie pisemnych kwestionariuszy i wywiadów z odpowiednimi zainteresowanymi stronami. Więcej informacji na temat skontrolowanego zagadnienia, zakresu kontroli i podejścia kontrolnego można znaleźć w [załączniku I](#).

Co ustalił i zaleca Trybunał?

- 08** Ogólnie rzecz biorąc, Trybunał stwierdził, że działania UE jedynie częściowo ułatwiają wykrywanie poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, a także reagowanie na nie. Chociaż budowanie ram współpracy stopniowo postępuje, prace nad stworzeniem pełnej struktury cyberbezpieczeństwa nie są jeszcze zakończone. Niewielki zakres wymiany informacji, uchybienia w zakresie sprawozdawczości i znaczne opóźnienia we wdrażaniu uniemożliwiają pełne wykorzystanie potencjału unijnych sieci i mechanizmów. Projekty finansowane w ramach programu „Cyfrowa Europa” służą realizacji zamierzonych celów, ale w przypadku szeregu z nich Trybunał odnotował problemy operacyjne i opóźnienia. Ponadto kontrolerzy wykryli uchybienia w ogólnych ramach monitorowania wyników.
- 09** Obecną strukturę unijnych sieci i mechanizmów ułatwiających wykrywanie poważnych incydentów w cyberbezpieczeństwie i reagowanie na nie budowano stopniowo. W 2025 r. Rada przyjęła [plan na rzecz cyberbezpieczeństwa](#), w którym określono unijne ramy zarządzania cyberkryzysami. Trybunał stwierdził, że w planie tym w dużej mierze wyjaśniono role i obowiązki poszczególnych podmiotów w zakresie zarządzania cyberkryzysami w UE. Niemniej nie określono jeszcze formalnie, w jaki sposób sieć CSIRT (ustanowiona w 2016 r.) i sieć EU-CyCLONe (formalnie ustanowiona w 2023 r.) powinny ze sobą współpracować (pkt [24–30](#)).
- 10** Trybunał stwierdził, że wymiana informacji za pośrednictwem tych sieci ma jedynie ograniczony zakres. Wynika to głównie z opóźnień w transpozycji [dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii](#) (dyrektywy NIS 2), z trudności w ustaleniu, czy incydent ma skutki transgraniczne, a także z krajowych przepisów w dziedzinie bezpieczeństwa uniemożliwiających wymianę informacji. Wartość dodana sieci jest znacznie mniejsza, jeśli państwa członkowskie nie są skłonne do dzielenia się w odpowiednim momencie informacjami, które pozwoliłyby innym podmiotom podjąć działania (pkt [31–44](#)).



Zalecenie 1

Zintensyfikowanie wymiany informacji między państwami członkowskimi

Aby usprawnić wykrywanie cyberincydentów i reagowanie na nie, Komisja przy wsparciu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) powinna:

- a) zaproponować grupie współpracy ds. bezpieczeństwa sieci i systemów informatycznych, by przeprowadziła ona szczegółową analizę ograniczeń podyktowanych względami bezpieczeństwa narodowego, które zawężają zakres wymiany informacji i wpływają na cyberodporność UE, oraz by wskazała ona rozwiązania prawne i techniczne w celu zwiększenia wymiany informacji przy jednoczesnym poszanowaniu kwestii bezpieczeństwa narodowego;
- b) bez uszczerbku dla decyzji współprawodawców zapewnić – we współpracy z państwami członkowskimi – by pojedynczy punkt kontaktowy do zgłaszania incydentów zaproponowany w akcie zbiorczym prawa cyfrowego był w stanie wykrywać potencjalne incydenty transgraniczne;
- c) podjąć prace nad rozwiązaniami, które umożliwiłyby zgłaszanie ENISA incydentów w czasie rzeczywistym.

Termin realizacji: lit. a) i b) – 2027 r., lit. c) – 2028 r.

- 11** W 2022 r. Komisja utworzyła centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa, aby zwiększyć swoją orientację sytuacyjną w tej dziedzinie. Centrum miało ułatwić Komisji wypełnianie ciężących na niej obowiązków instytucjonalnych w zakresie zarządzania kryzysowego. Funkcjonowanie centrum wspierane jest w znacznym stopniu przez usługodawców zewnętrznych zatrudnionych na podstawie umowy. Trybunał stwierdził, że prace prowadzone przez usługodawców zewnętrznych częściowo pokrywają się z kompetencjami Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) w zakresie orientacji sytuacyjnej i monitorowania zagrożeń. Kontrolerzy stoją na stanowisku, że przy ustanawianiu centrum nie wykorzystano w wystarczającym stopniu możliwości optymalizacji i nie przewidziano korzystania z informacji już dostępnych w Komisji i ENISA. Ponadto brak kompleksowego, szczegółowego planu na okres po wygaśnięciu umowy stanowi zagrożenie dla funkcjonowania centrum po 2026 r. (pkt 45–51).



Zalecenie 2

Optymalne wykorzystanie unijnych zdolności w zakresie orientacji sytuacyjnej w dziedzinie cyberbezpieczeństwa i usprawnienie rozpowszechniania informacji

Aby zwiększyć efektywność, Komisja powinna we współpracy z ENISA ocenić wykonalność wspólnego pozyskiwania i analizy informacji na potrzeby orientacji sytuacyjnej. Powinna również udostępniać te informacje i powiązane sprawozdania dotyczące cyberzagrożeń we wszystkich odpowiednich służbach i agencjach UE.

Termin realizacji: 2027 r.

- 12** W [akcie o cybersolidarności](#) przyjętym w 2024 r. ustanowiono unijną rezerwę cyberbezpieczeństwa, której celem jest wspieranie państw członkowskich w reagowaniu na poważne incydenty w cyberbezpieczeństwie i usuwaniu skutków takich incydentów. Rezerwa składa się z wybranych usługodawców z każdego państwa członkowskiego, którzy są w stanie reagować na incydenty przez całą dobę. Wprowadzie takie rozwiązanie pomaga spełnić szczególne wymagania różnych państw członkowskich i budować zaufanie, lecz dostępny budżet jest równo podzielony między państwa i nie uwzględnia szczególnych potrzeb danego państwa członkowskiego (pkt [52–57](#)).
- 13** Trybunał odnotowuje, że wcześniejsze zawarcie umów z dostawcami umożliwia szybkie skorzystanie z usług reagowania na incydenty. Unijna rezerwa cyberbezpieczeństwa ma przede wszystkim na celu wspieranie reagowania na incydenty i usuwania ich skutków, lecz jeśli nie zostanie wykorzystana do reagowania na incydenty, można ją wykorzystać do zapewnienia gotowości. To elastyczne podejście pozwala zapobiec sytuacji, w której wcześniej opłacone usługi pozostałyby niewykorzystane. Istnieje jednak ryzyko, że rezerwa będzie wykorzystywana głównie do celów zapewnienia gotowości, a nie do reagowania na incydenty, co byłoby sprzeczne z jej zamierzonym celem (pkt [58–61](#)).
- 14** Europejski system cyberostrzeżeń to sieć krajowych i transgranicznych centrów cyberbezpieczeństwa, których celem jest usprawnienie wykrywania i analizy cyberzagrożeń oraz reagowania na takie zagrożenia. Trybunał stwierdził, że w momencie przeprowadzania kontroli ze względu na znaczne opóźnienia w zamawianiu narzędzi i usług działalność operacyjna dwóch centrów (ATHENA i ENSOC) jeszcze się nie rozpoczęła, a europejski system cyberostrzeżeń jeszcze nie funkcjonował (pkt [62–70](#)).

- 15** Jednym z kluczowych celów europejskiego systemu cyberostrzeżeń jest zachęcanie do konstruktywnej wymiany informacji między grupami państw członkowskich. Mogłoby to rozwiązać niektóre problemy związane z wymianą informacji, lecz włączenie centrów w zakresie cyberbezpieczeństwa do już bardzo złożonego środowiska cyberbezpieczeństwa nastręcza dużych trudności. Trybunał stwierdził, że nie wprowadzono jeszcze wymaganych umów o współpracy, wspólnej klasyfikacji zdarzeń i incydentów oraz standardów interoperacyjności niezbędnych do funkcjonowania europejskiego systemu cyberostrzeżeń w pełnym zakresie (pkt 71–74).



Zalecenie 3

Włączenie europejskiego systemu cyberostrzeżeń do unijnego środowiska cyberbezpieczeństwa

Komisja powinna wraz z ENISA i państwami członkowskimi zagwarantować, że zostaną opracowane rozwiązania w zakresie współpracy oraz standardy interoperacyjności, tak aby ułatwić wymianę informacji między centrami transgranicznymi, które są częścią europejskiego systemu cyberostrzeżeń, siecią CSIRT i EU-CyCLONe.

Termin realizacji: 2028 r.

- 16** W 2018 r. Komisja zaproponowała utworzenie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC). Miało ono zarządzać, począwszy od 2021 r., komponentem programu „Cyfrowa Europa” dotyczącym cyberbezpieczeństwa. W [rozporządzeniu w sprawie ECCC](#) wezwano do utworzenia społeczności kompetentnej w zakresie cyberbezpieczeństwa, w skład której wchodziłoby przedstawiciele branży oraz organizacji akademickich i badawczych. Wybrani członkowie społeczności mieliby następnie stworzyć Strategiczną Grupę Doradczą (pkt 75–76).
- 17** Trybunał stwierdził opóźnienia w osiągnięciu autonomii finansowej przez ECCC oraz w tworzeniu społeczności kompetentnej w zakresie cyberbezpieczeństwa i Strategicznej Grupy Doradczej. Opóźnienia te oznaczają, że społeczność i grupa doradcza nie mogły wnieść wkładu w kształtowanie programów prac w ramach programu „Cyfrowa Europa”. Trybunał uznaje to za straconą szansę (pkt 77–81).
- 18** Kontrolerzy ustalili, że wszystkie skontrolowane projekty służyły realizacji odpowiednich celów i przyczyniają się do osiągnięcia celów programu „Cyfrowa Europa” w zakresie cyberbezpieczeństwa. Trybunał wykrył jednak przypadki, w których jakość projektów lub osiągnięte rezultaty nie były zadowalające głównie ze względu na opóźnienia we wdrażaniu (pkt 82–87).

- 19** Rozporządzenie w sprawie programu „Cyfrowa Europa” stanowi, że ze względów bezpieczeństwa przyznawanie finansowania na rzecz cyberbezpieczeństwa może zostać ograniczone do podmiotów mających siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich UE. Centralny Dział ds. Zatwierdzeń Europejskiej Agencji Wykonawczej ds. Badań Naukowych przeprowadza stosowną ocenę struktury własności i kontroli w imieniu ECCC (pkt 88–91).
- 20** W przypadku przyznania wsparcia finansowego na rzecz osób trzecich ocena struktury własności i kontroli należy do obowiązków beneficjentów projektu, którzy dokonują jej w oparciu o własne podejście i metodykę. Trybunał stwierdził, że ECCC nie zatwierdza tej metodyki ani nie przeprowadza kontroli w celu zapewnienia, by wybrane osoby trzecie były własnością podmiotów z UE i były przez nie kontrolowane. Kontrolerzy uważają, że istnieje znaczne ryzyko, iż beneficjenci nie są w stanie prawidłowo przeprowadzić koniecznych weryfikacji. Ryzyko to nie zostało odpowiednio ograniczone i może skutkować narażeniem wrażliwej infrastruktury, danych operacyjnych i technologii o kluczowym znaczeniu dla bezpieczeństwa (pkt 92–96).



Zalecenie 4

Zapewnienie rzetelnej oceny struktury własności i kontroli podmiotów otrzymujących finansowanie unijne w ramach programu „Cyfrowa Europa”

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa powinno:

- a) uzyskać wystarczającą pewność co do tego, że beneficjenci odpowiedzialni za udzielanie wsparcia finansowego podmiotom trzecim posiadają zdolności administracyjne i techniczne niezbędne do przeprowadzenia odpowiednich ocen struktury własności i kontroli. Oceny takie powinny być przeprowadzane w oparciu o metodykę udostępnioną tym beneficjentom;
- b) weryfikować na podstawie badania próby, czy wyłącznie kwalifikowalne podmioty otrzymują finansowanie unijne.

Termin realizacji: lit. a) – 2026 r.; lit b) – 2027 r.

- 21** Beneficjenci zarządzający projektami finansowanymi przez UE muszą składać ECCC sprawozdania z osiągniętych postępów i wypracowanych rezultatów. Opierają się przy tym na ustalonych kamieniach milowych i oczekiwanych produktach. Mają one kluczowe znaczenie dla monitorowania projektów i powinny zostać odpowiednio zdefiniowane. Trybunał ustalił tymczasem, że w niemal żadnym z projektów objętych próbą nie stosowano się do instrukcji dotyczących sposobu definiowania kamieni milowych i produktów oraz że wiele z nich nie było przydatnych do śledzenia postępów (pkt [97–99](#)).
- 22** Trybunał stwierdził, że wiele wskaźników wykonania stosowanych przez beneficjentów jest nieadekwatnych bądź niemierzalnych. Nie określono też poziomów wyjściowych ani docelowych. Ponadto sprawozdawczość dotycząca tych wskaźników była nieodpowiednia i w związku z tym nie może służyć jako podstawa do oceny wyników wypracowanych w projektach (pkt [100–102](#)).
- 23** Aby można było monitorować osiągnięcia programu „Cyfrowa Europa” jako całości, we wszystkich projektach obowiązuje wymóg przekazywania informacji na temat wskaźników specyficznych dla programu. Są one następnie uwzględniane w rocznych [zestawieniach wyników programów](#) sporządzanych przez Komisję. ECCC jest odpowiedzialne za gromadzenie i weryfikację danych na temat tych wskaźników. Trybunał wykrył szereg problemów związanych ze sposobem gromadzenia danych i ogólnie ich jakością. Kontrolerzy nie znaleźli dowodów na to, że ECCC zweryfikowało poprawność zgłoszonych danych. Na podstawie kontroli wyrywkowych Trybunał stwierdza, że przedstawione dane nie odzwierciedlają dokładnie osiągniętych rezultatów (pkt [103–106](#)).



Zalecenie 5

Udoskonalenie ram monitorowania wyników wypracowanych w komponencie programu „Cyfrowa Europa” dotyczącym cyberbezpieczeństwa

Aby umożliwić odpowiednie monitorowanie postępów i wyników, Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa powinno:

- a) zagwarantować, że przed podpisaniem umowy o udzielenie dotacji we wszystkich projektach określone zostaną kamienie milowe, oczekiwane produkty i wskaźniki wykonania, które będą zgodne z instrukcjami zawartymi w formularzu wniosku;
- b) zaprojektować i wdrożyć solidny system gromadzenia, zapewniania identyfikowalności, weryfikacji i agregacji danych na potrzeby wskaźników wykonania obowiązujących w komponencie programu „Cyfrowa Europa” dotyczącym cyberbezpieczeństwa, tak aby zagwarantować poprawne odzwierciedlenie osiągniętych rezultatów we wskaźnikach.

Termin realizacji: 2027 r.

Omówienie uwag Trybunału

Unijne sieci i mechanizmy cyberbezpieczeństwa ułatwiają współpracę i reagowanie, lecz niewielki zakres wymiany informacji i niepełne wdrożenie zmniejszają skuteczność wprowadzonych rozwiązań

Unijne sieci umożliwiają współpracę między państwami członkowskimi, ale niewielki zakres wymiany informacji zmniejsza wartość dodaną tych sieci

- 24** Obowiązujące unijne ramy dotyczące sieci i mechanizmów ułatwiających wykrywanie poważnych incydentów w cyberbezpieczeństwie i reagowanie na nie stworzono stopniowo, począwszy od [dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii](#)³ (dyrektywa NIS), która weszła w życie w sierpniu 2016 r. W [załączniku II](#) przedstawiono obecną sytuację w UE w tej dziedzinie.

³ Dyrektywa (UE) 2016/1148.

Unijne sieci umożliwiają państwom członkowskim współpracę w wymiarze technicznym i operacyjnym

- 25** Dyrektywą NIS ustanowiono sieć CSIRT, w skład której wchodzi CERT-UE (Służba ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii) oraz zespoły CSIRT wyznaczone przez państwa członkowskie. Sieć ta ma na celu budowanie zaufania między krajowymi zespołami CSIRT oraz promowanie szybkiej i skutecznej współpracy operacyjnej między państwami członkowskimi.
- 26** EU-CyCLONe ustanowiono w 2020 r. jako nieformalną sieć współpracy organów krajowych odpowiedzialnych za zarządzanie cyberkryzysami. Służy ona jako pomost między wymiarem technicznym, czyli siecią CSIRT, a wymiarem politycznym – Radą Unii Europejskiej i przyjętymi przez nią zintegrowanymi uzgodnieniami dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych. Wejście w życie dyrektywy NIS 2 w 2023 r. sformalizowało rolę EU-CyCLONe – zyskała ona wyraźny mandat.
- 27** Trybunał ocenił, czy role i obowiązki wspomnianych wyżej sieci na szczeblu UE zostały dobrze określone i czy ułatwiają one współpracę państw członkowskich.
- 28** ENISA pełni funkcję sekretariatu sieci CSIRT i EU-CyCLONe oraz zapewnia im zasoby, wiedzę specjalistyczną, infrastrukturę i narzędzia informatyczne niezbędne do współpracy i bezpiecznej komunikacji na potrzeby wymiany informacji. W ankiecie badającej zadowolenie zainteresowanych stron⁴ przeprowadzonej na początku 2025 r. ENISA uzyskała dobre wyniki, jeśli chodzi o pełnienie funkcji sekretariatu obu tych sieci. Te dobre wyniki znalazły również potwierdzenie w toku wizyt kontrolnych Trybunału, podczas których przedstawiciele krajowych organów odpowiedzialnych za cyberbezpieczeństwo wyrazili swoje zadowolenie z działalności ENISA.

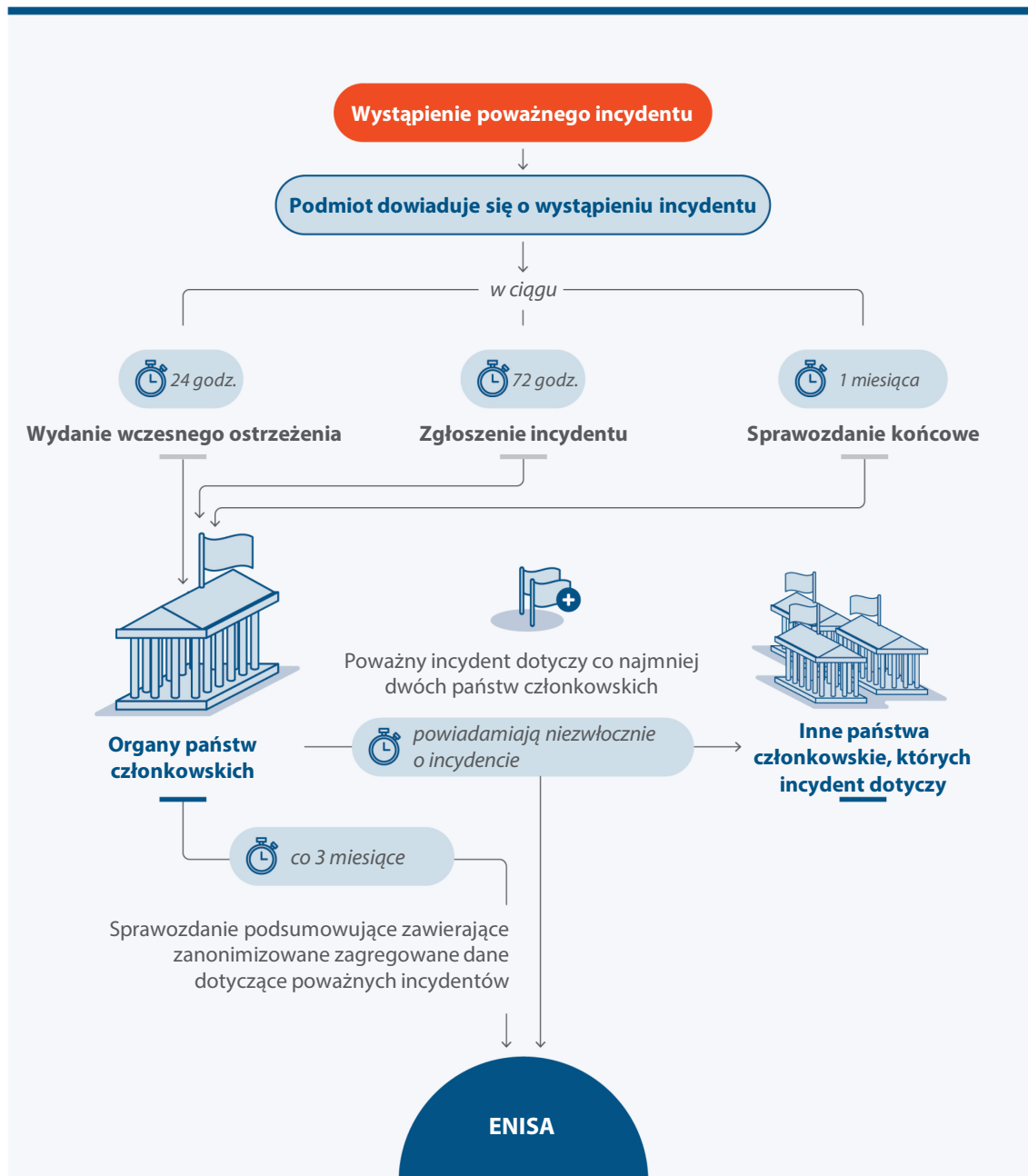
⁴ Skonsolidowane roczne sprawozdanie z działalności ENISA za 2024 r., s. 33 i 36.

- 29** W 2025 r. Rada przyjęła [plan na rzecz cyberbezpieczeństwa](#), w którym określono role i obowiązki kluczowych podmiotów (w tym sieci CSIRT i EU-CyCLONe) oraz mechanizmy uruchamiane w razie wystąpienia cyberincydentów na dużą skalę lub cyberkryzysów. Kontrolerzy stwierdzili, że w planie na rzecz cyberbezpieczeństwa w dużej mierze wyjaśniono role i obowiązki w zakresie zarządzania w razie wystąpienia cyberkryzysu w UE oraz uwzględniono zmiany, jakie zaszły w tym obszarze od czasu przyjęcia pierwszego planu w 2017 r. Określono w nim trzy poziomy współpracy: techniczny, operacyjny i polityczny. Wyszczególniono także nowe sieci i struktury ustanowione od 2017 r. – takie jak EU-CyCLONe, unijne zespoły szybkiego reagowania na zagrożenia hybrydowe i europejski system cyberostrzeżeń – oraz omówiono, w jaki sposób zarządzanie cyberkryzysami powinno zostać włączone do szerszych ram reagowania kryzysowego UE.
- 30** Pomimo oficjalnego ustanowienia sieci CSIRT w 2016 r. i EU-CyCLONe w 2023 r. obie sieci muszą jeszcze sformalizować ustalenia proceduralne dotyczące sposobu współpracy. Nie uzgodniły również kryteriów, na podstawie których sieć CSIRT miałaby informować EU-CyCLONe, że zaobserwowany cyberincydent stanowi potencjalny lub trwający incydent na dużą skalę. Obie sieci muszą również uzgodnić wspólną klasyfikację poziomów dotkliwości incydentów i kluczowe pojęcia – takie jak „zagrożenie”, „podmiot stwarzający zagrożenie”, „incydent” lub „wpływ” – które są niezbędne do zautomatyzowanej wymiany informacji. Obecnie istnieje pewna swoboda interpretacji co do tego, kiedy dany incydent kwalifikuje się jako poważny lub na dużą skalę. Przedstawiciele organów odpowiedzialnych za cyberbezpieczeństwo we wszystkich trzech państwach członkowskich, w których Trybunał przeprowadził wizyty kontrolne, wspomnieli o braku wspólnej klasyfikacji w tym zakresie.

Ograniczony zakres wymiany informacji i sprawozdawczości znacznie zmniejszają wartość dodaną wspomnianych sieci

- 31** Granice geograficzne nie stanowią żadnej przeszkody, jeśli chodzi o występowanie i rozprzestrzenianie się cyberincydentów i cyberataków. Wymiana informacji między państwami członkowskimi – na przykład na temat taktyk i technik stosowanych przez podmioty stwarzające zagrożenia oraz na temat poszlak cyfrowych wskazujących na naruszenie sieci lub systemu informatycznego („oznaki naruszenia integralności systemu”) – może w znacznym stopniu przyczynić się do poprawy cyberbezpieczeństwa.
- 32** Trybunał stwierdził, że wymiana informacji ma ograniczony zakres, co znacznie zmniejsza wartość dodaną wspomnianych sieci. Ograniczenia zaobserwowane przez kontrolerów dotyczą głównie: opóźnień w transpozycji dyrektywy NIS 2; problemów z ustaleniem, czy incydent ma skutki transgraniczne; przepisów dotyczących bezpieczeństwa narodowego ograniczających wymianę informacji; braku zaufania. W dyrektywie NIS 2 wprowadzono szereg wymogów sprawozdawczych dla podmiotów objętych jej zakresem oraz dla organów państw członkowskich, jak pokazano na [rys. 2](#).

Rys. 2 | Ramy czasowe zgłaszania incydentów na podstawie dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE (NIS 2)



Źródło: Europejski Trybunał Obrachunkowy na podstawie informacji przekazanych przez ENISA.

- 33** Państwa członkowskie miały czas do października 2024 r. na [transpozycję dyrektywy NIS 2](#) do przepisów prawa krajowego, lecz jedynie dwa państwa dotrzymały tego terminu. Opóźnienia w transpozycji mają istotny wpływ na wymianę informacji, ponieważ do momentu dokonania transpozycji podmioty objęte dyrektywą NIS 2 nie są prawnie zobowiązane do zgłaszania incydentów. Komisja oszacowała⁵, że dyrektywa NIS obejmuje 15 500 podmiotów, a ponad 110 000 wchodzi w zakres dyrektywy NIS 2. Na przykład administracja publiczna – sektor będący najczęstszym obiektem ataków w UE, jak wynika ze [sprawozdania ENISA z 2025 r. dotyczącego sytuacji w zakresie zagrożeń](#) – nie miała obowiązku zgłaszania incydentów na podstawie dyrektywy NIS.
- 34** Zgłaszanie ENISA danych dotyczących incydentów co trzy miesiące (tj. długo po wystąpieniu incydu) zmniejsza wartość dodaną tej sprawozdawczości. Dane te służą głównie do celów statystycznych i odnotowywania trendów na przestrzeni czasu, a nie do poprawy wykrywania incydentów i reagowania na nie. ENISA udostępnia państwom członkowskim [narzędzie internetowe](#) do przekazywania informacji sprawozdawczych. Formularz sprawozdawczy przewiduje minimalny zestaw danych, które należy przekazać, takich jak rodzaj incydu i sektor, którego dotyczy incydu. Ponadto ENISA sugeruje państwom członkowskim, aby przekazywały dodatkowe informacje umożliwiające bardziej dogłębną analizę danych, na przykład przez powiązanie incydentów z konkretnymi podatnościami. Nie wszystkie państwa członkowskie decydują się jednak na przekazywanie tych informacji, co znacznie obniża jakość i wartość dodaną gromadzonych danych.
- 35** ENISA w swoim [sprawozdaniu z 2024 r. na temat sytuacji w zakresie cyberbezpieczeństwa w UE](#) stwierdziła, że sprawozdawczość nie obejmuje prawdopodobnie wszystkich incydentów, ponieważ liczba zgłoszeń wydaje się niska. W latach 2018–2021 państwa członkowskie zgłaszały ENISA od 100 do 500 incydentów rocznie. Liczba ta stopniowo rosła, a w 2024 r. wyniosła 1 276⁶.

⁵ Komisja Europejska, [sprawozdanie z oceny skutków](#) z 2020 r.

⁶ Dane CIRAS za 2024 r.

- 36** W [sprawozdaniu z 2025 r. dotyczącym sytuacji w zakresie zagrożeń](#), które objęło okres od czerwca 2024 r. do czerwca 2025 r., ENISA zidentyfikowała około 4 800 cyberincydentów⁷, korzystając z ogólnodostępnych źródeł informacji takich jak artykuły w mediach. Nie wszystkie te incydenty podlegałyby zgłoszeniu na podstawie dyrektywy NIS 2, ponieważ przy gromadzeniu danych ENISA uwzględnia szerszy zakres incydentów. Z drugiej strony wiele istotnych incydentów nie jest odnotowywanych w ogólnodostępnych źródłach. Ponieważ dane zgłaszane przez państwa członkowskie są anonimizowane, ENISA nie może powiązać zidentyfikowanych przez siebie incydentów z incydentami zgłaszanymi przez państwa członkowskie. W związku z tym nie jest możliwe dokładne określenie, jaka część cyberincydentów pozostaje niezgłoszona. Trybunał uważa jednak, że różnica między liczbą incydentów zgłoszonych przez państwa członkowskie a liczbą incydentów zgłoszonych w sprawozdaniu dotyczącym sytuacji w zakresie zagrożeń pokazuje, że nie wszystkie poważne incydenty są zgłaszane.
- 37** Kolejną oznaką niezgłaszania incydentów jest liczba zgłoszeń dotyczących poważnych incydentów transgranicznych. Zgłoszenia te są przekazywane innym państwom członkowskim dotkniętym incydem oraz ENISA. Podobny wymóg wprowadzono dyrektywą NIS, ale został on uznany za nieskuteczny, ponieważ w 2020 r. Komisja stwierdziła⁸, że pomimo obowiązku rzadko wysyłano stosowne powiadomienia. Komisja uznała wówczas, że niewysyłanie powiadomień wynika z braku jasnych zasad dotyczących wymiany informacji oraz wspólnych celów, które zachęciłyby do takiej wymiany.
- 38** Obowiązek informowania innych państw członkowskich ma kluczowe znaczenie dla zapobiegania dalszemu rozprzestrzenianiu się incydentów – nieinformowanie niekorzystnie wpływa na cyberbezpieczeństwo UE. W 2025 r. zgłoszono jedynie 14 poważnych incydentów transgranicznych (zgłoszeń dokonało łącznie siedem państw). W 2024 r. państwa członkowskie przedłożyły dwa sprawozdania z incydentów, które mogą mieć skutki transgraniczne (w 2023 r. – żadnego takiego sprawozdania, a w 2022 r. – trzy). Pokazuje to, że liczba zgłaszanych poważnych incydentów transgranicznych jest bardzo niska i nie odzwierciedla rzeczywistego zasięgu takich ataków. Wystarczy spojrzeć na dane zawarte w [sprawozdaniu ENISA z 2024 r. dotyczącym sytuacji w zakresie zagrożeń](#) – zidentyfikowano w nim 322 incydenty wymierzone w więcej niż jedno państwo członkowskie. Incydent dotyczący Collins Aerospace (zob. [ramka 1](#)) jest przykładem tego, że państwa członkowskie nie zgłaszają incydentów, mimo że mają one istotne skutki transgraniczne.

⁷ [Sprawozdanie ENISA z 2025 r. dotyczące sytuacji w zakresie zagrożeń](#).

⁸ Komisja Europejska, [sprawozdanie z oceny skutków](#) z 2020 r.

Ramka 1

Cyberincydent zakłócający funkcjonowanie portów lotniczych

We wrześniu 2025 r. Collins Aerospace, ważny dostawca technologii dla przemysłu lotniczego, stał się obiektem poważnego ataku z użyciem oprogramowania szantażującego (ransomware). Atak był wymierzony w oprogramowanie służące do przetwarzania danych pasażerów. Incydent ten zmusił duże europejskie porty lotnicze do manualnego przetwarzania danych, co spowodowało powszechne opóźnienia i odwołania lotów. Najpoważniejsze zakłócenia wystąpiły w porcie lotniczym Londyn Heathrow oraz na lotniskach w Brukseli (Brussels Airport), Berlinie (Berlin Brandenburg) i Dublinie (Dublin Airport).

Zgodnie z dyrektywą NIS 2 incydent uznaje się za „poważny”, między innymi jeśli powoduje dotkliwe zakłócenia operacyjne w świadczeniu usług lub straty finansowe dla danego podmiotu. Tymczasem żadne państwo członkowskie nie potraktowało tego incydentu jako poważnego ani jako incydentu transgranicznego na dużą skalę. W związku z tym żadne z państw członkowskich dotkniętych tym incydentem nie powiadomiło formalnie ENISA ani innych państw członkowskich o incydencie. Sieć CSIRT nie poinformowała sieci EU-CyCLONe, która w rezultacie nie wspierała skoordynowanego zarządzania incydentem.

Źródło: analiza przeprowadzona przez Europejski Trybunał Obrachunkowy na podstawie wywiadów z pracownikami ENISA.

- 39** Innym powodem niedostatecznej liczby zgłoszeń o incydentach transgranicznych jest fakt, że to do kompetencji danych organów państw członkowskich należy ustalenie, czy zgłoszony incydent ma skutki transgraniczne, oraz zidentyfikowanie pozostałych państw członkowskich, których dotyczy incydent. Podmiot zgłaszający lub organ państwa członkowskiego opierają się jedynie na dostępnych im informacjach i mogą nie być świadome transgranicznego charakteru niektórych ataków. Obecnie nie funkcjonuje żadna ogólnounijna platforma, która przyjmowałaby zgłoszenia o incydentach w czasie rzeczywistym od wszystkich państw członkowskich i pozwalała zestawiać informacje na temat sektorów lub oznak naruszenia integralności systemu w celu wykrywania incydentów transgranicznych. Istnieje zatem znaczne ryzyko, że niektóre incydenty transgraniczne mogą nie zostać zidentyfikowane ani zgłoszone.
- 40** Od 2016 r. żadne państwo członkowskie nie uznało żadnego cyberincydentu za cyberincydent na dużą skalę. Co do zasady termin ten obejmuje każdy incydent, który ma znaczący wpływ na co najmniej dwa państwa członkowskie. Niemniej nawet cyberincydenty, które spowodowały globalne przestoje w działalności i znaczne szkody, takie jak te omówione na [rys. 3](#), nie zostały uznane za incydenty na dużą skalę. W rezultacie procedura eskalacji EU-CyCLONe po wystąpieniu incydentu w cyberbezpieczeństwie na dużą skalę nigdy nie została w pełni uruchomiona.

Rys. 3 | Przykłady znaczących cyberincydentów



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych Cloudflare, ENISA, Europolu, Wired, IBM i CrowdStrike.

- 41** Obok nałożenia na podmioty i państwa członkowskie obowiązku zgłaszania incydentów utworzono również – w celu ułatwienia wymiany informacji – sieć CSIRT. Wzajemne zaufanie państw członkowskich leży u podstaw sieci CSIRT, w ramach której wymiana informacji odbywa się na zasadzie dobrowolności. Wartość dodana sieci jest znacznie mniejsza, jeśli państwa członkowskie nie są skłonne do dzielenia się w odpowiednim momencie informacjami, które pozwoliłyby innym podmiotom podjąć działania.
- 42** Wymiana informacji na szczeblu UE jest ograniczona przepisami poszczególnych państw członkowskich dotyczącymi bezpieczeństwa narodowego. Jeśli państwo członkowskie uzna, że informacje dotyczące cyberataku na podmiot krytyczny są niejawnie lub że zgłoszenie konkretnego incydentu byłoby ze szkodą dla bezpieczeństwa narodowego, nie ma obowiązku udostępniania odnośnych informacji. Podczas wizyt kontrolnych Trybunału w państwach członkowskich przedstawiciele sieci CSIRT i EU-CyCLONe stwierdzili, że wymiana informacji może odbywać się wyłącznie w granicach przepisów dotyczących bezpieczeństwa narodowego. Na szczeblu UE nie przeprowadzono analizy stosownych przepisów krajowych ani wpływu tych przepisów na wymianę informacji.
- 43** W 2016 r. sieć CSIRT składała się z 28 krajowych CSIRT. W skład sieci wchodziło po dwóch przedstawicieli z każdego państwa członkowskiego. Brak wymiany informacji jest nawracającym problemem. W [ocenie dyrektywy NIS](#) Komisja uznała, że państwa członkowskie nie wymieniają się systematycznie informacjami, co szczególnie osłabia skuteczność środków w zakresie cyberbezpieczeństwa i niekorzystnie wpływa na wspólną orientację sytuacyjną na szczeblu UE. Zgodnie z dyrektywą NIS 2 oprócz krajowych CSIRT wiele państw członkowskich wyznaczyło sektorowe CSIRT, w związku z czym sieć została znacznie rozbudowana. W momencie przeprowadzania kontroli w jej skład wchodziły 42 zespoły CSIRT i ponad 700 indywidualnych uczestników. Budowanie zaufania staje się przez to jeszcze większym wyzwaniem, ponieważ utrzymywanie bliskich kontaktów między wszystkimi członkami sieci jest trudne.
- 44** Przedstawiciele sieci CSIRT są świadomi trudności w zakresie wymiany informacji i rozważają podjęcie różnych działań mających na celu pogłębienie zaufania w ramach rozrastającej się sieci. Stworzenie mniejszych klastrów państw członkowskich powołujących centra transgraniczne (zob. pkt [62–74](#)) jest alternatywnym podejściem do ogólnounijnej sieci, które może pomóc w sprostaniu wyzwaniom związanym z budowaniem zaufania.

Usługi zamówione przez centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa częściowo powielają już istniejące zdolności, a przyszłe funkcjonowanie centrum stoi pod znakiem zapytania

- 45** Zgodnie z dyrektywą NIS 2 w przypadkach, w których potencjalny lub trwający incydent w cyberbezpieczeństwie na dużą skalę ma lub może wywrzeć poważny wpływ, Komisja staje się członkiem EU-CyCLONe⁹. Ta nowa rola oraz zmieniające się zagrożenia skłoniły Komisję do ustanowienia w 2022 r. grupy zadaniowej ds. koordynacji w zakresie cyberbezpieczeństwa w DG CONNECT. W skład grupy wchodzi centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa, które miało pomóc Komisji lepiej orientować się w bieżącej sytuacji w zakresie cyberbezpieczeństwa. Dzięki temu Komisja miała zyskać pomoc w wypełnianiu ciężących na niej obowiązków instytucjonalnych w zakresie zarządzania kryzysowego. Powinno to również pomóc DG CONNECT w świadczeniu doradztwa na szczeblu politycznym.
- 46** Aby utworzyć centrum, Komisja w dużej mierze skorzystała z usług świadczonych przez dostawców zewnętrznych, z którymi w grudniu 2022 r. [zawarła umowę](#) na kwotę prawie 18 mln euro na okres czterech lat. Trybunał ocenił proces tworzenia centrum, wypracowane przez nie wyniki oraz plany Komisji dotyczące jego przyszłego funkcjonowania.
- 47** W ramach świadczonych usług wykonawcy stworzyli panel monitorowania cyberzagrożeń oparty na komercyjnych danych. Ma on służyć przedstawianiu i wymianie informacji na temat zagrożeń. Opracowują również różne raporty na temat cyberzagrożeń, w tym codzienne i cotygodniowe sprawozdania oraz sprawozdania tematyczne dotyczące poszczególnych państw lub sektorów gospodarki. W jednym z budynków Komisji utworzono fizyczną siedzibę centrum – pomieszczenie wyposażone w stanowiska robocze zdalnie połączone z panelem obsługiwany przez wykonawców. W momencie przeprowadzania kontroli w centrum zatrudniona była niewielka liczba pracowników Komisji, wspieranych przez wielu analityków zatrudnionych przez wykonawców, a także przez ekspertów z ENISA.

⁹ Art. 16 ust. 2 [dyrektywy NIS 2](#).

- 48** Trybunał stwierdził, że prace świadczone przez zewnętrznych usługodawców na rzecz centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa częściowo pokrywają się z zakresem działalności ENISA. ENISA prowadzi rutynowo działania w zakresie orientacji sytuacyjnej i monitorowania zagrożeń. Regularnie publikuje sprawozdania dotyczące cyberzagrożeń, w tym doraźne sprawozdania na temat konkretnych incydentów oraz cotygodniowe sprawozdania zawierające przegląd zagrożeń. Sprawozdania te opierają się na ogólnodostępnych informacjach i są podobne do sprawozdań sporządzanych przez wykonawców. Ponadto w sytuacjach kryzysowych ENISA przygotowuje briefingi dla decydentów lub uczestniczy w przygotowaniu takich dokumentów. Centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa opracowuje podobne publikacje.
- 49** Co więcej, informacje wykorzystywane przez centrum ds. orientacji sytuacyjnej w zakresie cyberbezpieczeństwa do sporządzania wspomnianych wyżej sprawozdań opierają się na danych komercyjnych i są podobne do danych wykorzystywanych przez inne służby Komisji (takie jak Dyrekcja Generalna ds. Usług Cyfrowych i CERT-UE). Kontrolerzy stoją na stanowisku, że przy ustanawianiu centrum nie wykorzystano w wystarczającym stopniu możliwości optymalizacji i nie przewidziano korzystania z informacji już dostępnych w Komisji i ENISA.
- 50** Umowa wygasa w grudniu 2026 r., po czym wykonawcy przestaną świadczyć usługi na rzecz centrum. Usługi te obejmują dostarczanie danych przedstawianych w panelu monitorowania cyberzagrożeń, sporządzanie sprawozdań dotyczących zagrożeń oraz zapewnienie większości pracowników centrum. Panel zostanie przekazany Komisji, ale nie będzie wnosił żadnej wartości dodanej, jeśli nie będzie stale aktualizowany za pomocą danych na temat cyberzagrożeń.
- 51** W momencie przeprowadzania kontroli Komisja nie miała planów, jeśli chodzi o świadczenie dalszego wsparcia na rzecz centrum przez usługodawców zewnętrznych już po wygaśnięciu umowy. Trybunał uznaje, że brak kompleksowego, szczegółowego planu na okres po wygaśnięciu umowy stanowi zagrożenie dla funkcjonowania centrum po 2026 r.

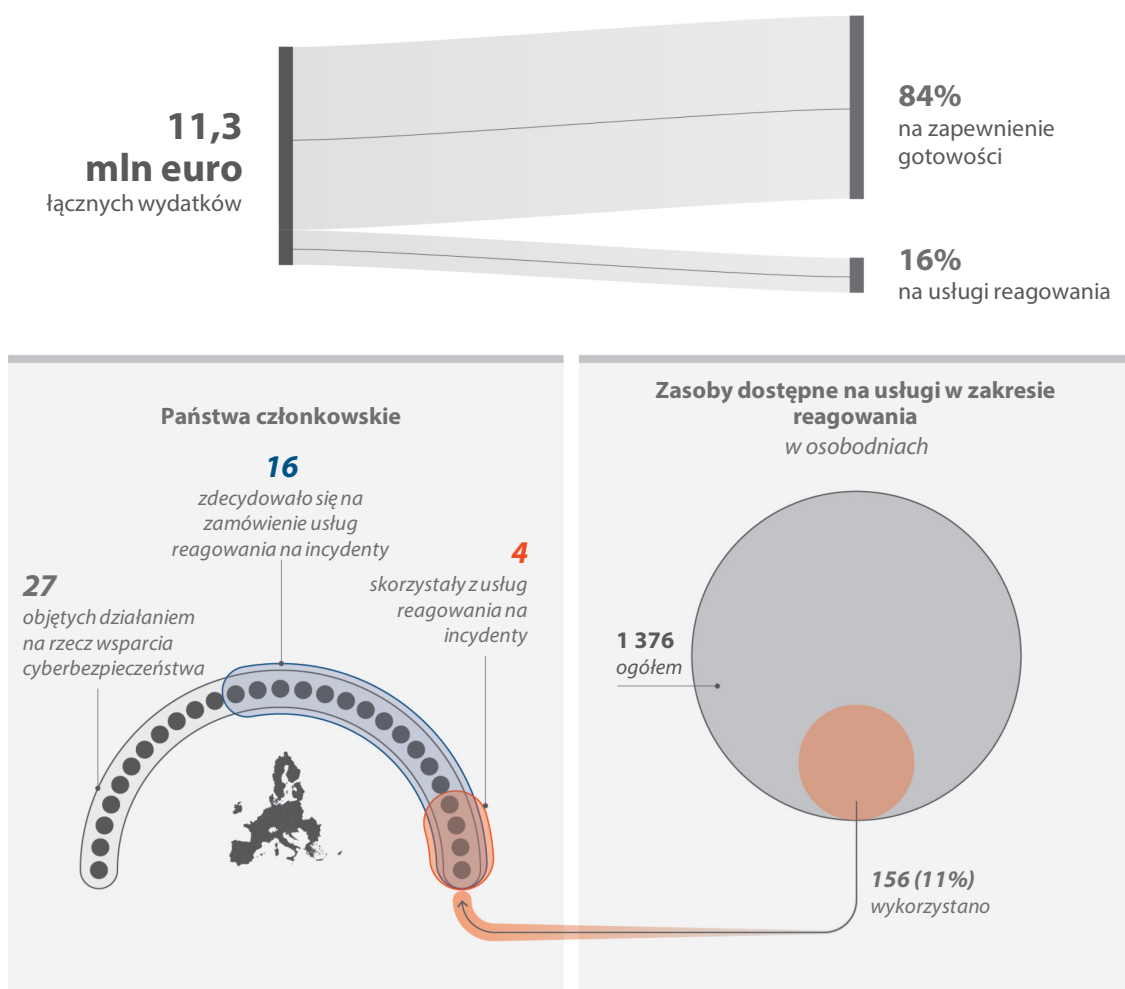
Unijna rezerwa cyberbezpieczeństwa umożliwia szybkie skorzystanie z usług reagowania na incydenty

- 52** W 2022 r. – bezpośrednio po agresji Rosji na Ukrainę i wobec rosnącej częstotliwości cyberataków na dużą skalę – Komisja przekazała ENISA 15 mln euro w formie nadzwyczajnego finansowania na pilotaż [działania na rzecz wsparcia cyberbezpieczeństwa](#). Realizacja działania rozpoczęła się w 2023 r. W 2023 r. Komisja zapewniła dodatkowe środki finansowe (około 20 mln euro) na przedłużenie tego programu do końca 2026 r.

- 53** Z myślą o przygotowaniu się do ewentualnych cyberincydentów na dużą skalę Komisja zaproponowała również [akt w sprawie cybersolidarności](#), który został przyjęty w grudniu 2024 r. W akcie ustanowiono unijną rezerwę cyberbezpieczeństwa, która obejmuje usługi reagowania na incydenty świadczone przez zaufanych dostawców. Rezerwa stopniowo rozpoczęła działalność w 2025 r., a jej budżet na lata 2025–2027 wynosił prawie 36 mln euro.
- 54** Trybunał ocenił, w jaki sposób zorganizowano program działań na rzecz wsparcia cyberbezpieczeństwa, ponieważ stanowi on podstawę unijnej rezerwy cyberbezpieczeństwa. Kontrolerzy sprawdzili również, czy przy opracowywaniu rezerwy wykorzystano wnioski wyciągnięte w okresie od 2022 r.
- 55** W zamyśle ENISA działanie na rzecz wsparcia cyberbezpieczeństwa ma być mechanizmem świadczenia usług wspierających zapewnienie gotowości i reagowanie państw członkowskich na cyberincydenty lub cyberkryzysy na dużą skalę. Wszystkie usługi zostały wstępnie zakontraktowane przez ENISA, co oznacza, że usługodawcy mogą rozpocząć świadczenie usług, gdy tylko państwa członkowskie tego zażądata. Takie natychmiastowe reagowanie zapewniają też rozwiązania przyjęte przez ENISA – Agencja zapewnia całodobową dyżurną osobę odpowiedzialną za obsługę wniosków o świadczenie usług przesyłanych przez państwa członkowskie.
- 56** ENISA postanowiła rozdzielić dostępny budżet równo między państwa członkowskie. W praktyce Agencja przeprowadziła otwartą procedurę przetargową podzieloną na 27 części, po jednej na każde państwo członkowskie, aby wybrać maksymalnie trzech prywatnych dostawców, którzy mieli świadczyć usługi w zakresie cyberbezpieczeństwa w okresie do końca 2026 r. Ponadto ENISA wybrała pewnych dostawców w ramach ogólnoeuropejskiej części przetargu. Mieli oni świadczyć usługi na rzecz kwalifikujących się państw trzecich, a także instytucji, organów i agencji UE, lub wspierać reagowanie na incydenty transgraniczne.
- 57** Podejście to umożliwiło ENISA uwzględnienie szczególnych wymogów krajowych, w tym wymogów językowych, wymogów dotyczących krajowych poświadczeń bezpieczeństwa lub obowiązku prowadzenia faktycznej działalności w danym państwie członkowskim. Z drugiej strony, ponieważ usługodawcy nie zostali wybrani do świadczenia usług w całej UE, przyjęte przez ENISA podejście ma jedną zasadniczą wadę: jeśli dane państwo członkowskie nie skorzysta z wcześniej zakontraktowanych usług, budżetu przewidzianego na takie usługi na rzecz jednego państwa członkowskiego nie można wykorzystać na pomoc innemu państwu członkowskiemu.

- 58** W przypadku działania na rzecz wsparcia cyberbezpieczeństwa państwa członkowskie mogą wybrać między usługami w zakresie zapewnienia gotowości lub reagowania na incydenty bądź połączeniem obu tych rodzajów usług. Państwa członkowskie zdecydowały się wykorzystać dostępne środki finansowe przede wszystkim do poprawy gotowości (84% wydatków w 2023 r.). Państwa członkowskie, które zdecydowały się na zakontraktowanie podmiotu świadczącego usługi reagowania na incydenty (tj. wcześniej określoną umowę z dostawcą, która zapewnia państwu członkowskiemu dostęp na żądanie do usług dostawcy w celu szybkiego reagowania na cyberincydenty), korzystały z niego oszczędnie, jak pokazano na [rys. 4](#). W trzech państwach członkowskich, w których przeprowadzono wizyty kontrolne, organy wyraziły uznanie dla zarządzania przez ENISA działaniem na rzecz wsparcia cyberbezpieczeństwa.

Rys. 4 | Działanie ENISA na rzecz wsparcia cyberbezpieczeństwa w okresie do 2023 r.



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych ENISA.

- 59** W latach 2024–2026 tylko dziewięć państw członkowskich zwróciło się o zakontraktowanie podmiotu świadczącego usługi reagowania na incydenty. Jak wynika z przeprowadzonych przez Trybunał wywiadów z przedstawicielami ENISA i organów w trzech państwach członkowskich, zdecydowanie preferowane są działania w zakresie zapewnienia gotowości.
- 60** Chociaż unijna rezerwa cyberbezpieczeństwa ma przede wszystkim na celu wspieranie reagowania na poważne incydenty w cyberbezpieczeństwie i usuwania skutków tych incydentów, wcześniej zakontraktowane usługi z unijnej rezerwy cyberbezpieczeństwa, które nie są wykorzystywane do reagowania na incydenty, można przekształcić w usługi w zakresie zapewnienia gotowości. To elastyczne podejście pozwala zapobiec sytuacji, w której wcześniej opłacone usługi pozostałyby niewykorzystane.
- 61** Trybunał odnotowuje, że model wybrany na potrzeby unijnej rezerwy cyberbezpieczeństwa opiera się na wnioskach wyciągniętych z programu działań na rzecz wsparcia cyberbezpieczeństwa. Niemniej dane dotyczące wykorzystania programu działań na rzecz wsparcia cyberbezpieczeństwa wskazują na ryzyko, że rezerwa może być wykorzystywana przede wszystkim na potrzeby zapewnienia gotowości, a nie reagowania, wbrew celowi określonemu w akcie w sprawie cybersolidarności.

Europejski system cyberostrzeżeń ma na celu udoskonalenie wykrywania zagrożeń, ale jeszcze nie funkcjonuje

- 62** Jednym z najważniejszych celów europejskiego systemu cyberostrzeżeń jest zachęcanie do konstruktywnej wymiany informacji, tak aby udoskonalić wykrywanie i analizę cyberzagrożeń oraz reagowanie na nie. Uczestnictwo w systemie ostrzegania jest dobrowolne, ale państwa członkowskie, które zdecydują się dołączyć do transgranicznego centrum cyberbezpieczeństwa, muszą zobowiązać się do wymiany istotnych informacji z pozostałymi członkami. Współpracując w obrębie klastrów w zaufanym i bezpiecznym środowisku, państwa członkowskie mogą uniknąć niektórych problemów związanych z wymianą informacji, o których mowa w pkt [31–44](#).
- 63** W momencie przeprowadzania kontroli 13 państw członkowskich zdecydowało się na udział w europejskim systemie cyberostrzeżeń, powołując dwa centra transgraniczne: ATHENA i ENSOC. Środki finansowe na utworzenie trzeciego transgranicznego centrum cyberbezpieczeństwa, NBCC, przydzielono w 2026 r. W rezultacie liczba członków sieci wzrosła do 20 państw (18 państw członkowskich oraz Islandia i Norwegia¹⁰). Stosowne informacje przedstawiono na [rys. 5](#).

¹⁰ Stowarzyszone państwa trzecie zgodnie z art. 10 ust. 1 lit. a) rozporządzenia (UE) 2021/694.

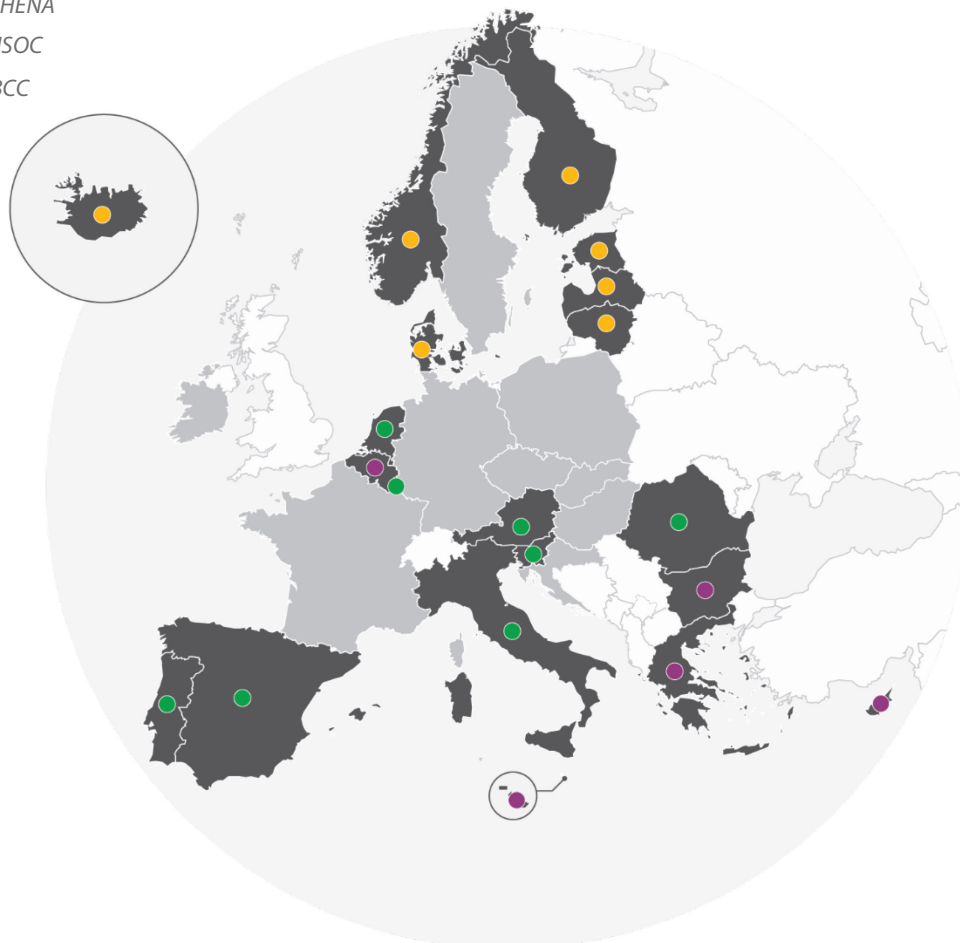
Rys. 5 | Państwa uczestniczące w europejskim systemie cyberostrzeżeń

■ Państwa uczestniczące w europejskim systemie cyberostrzeżeń

● ATHENA

● ENSOC

● NBCC



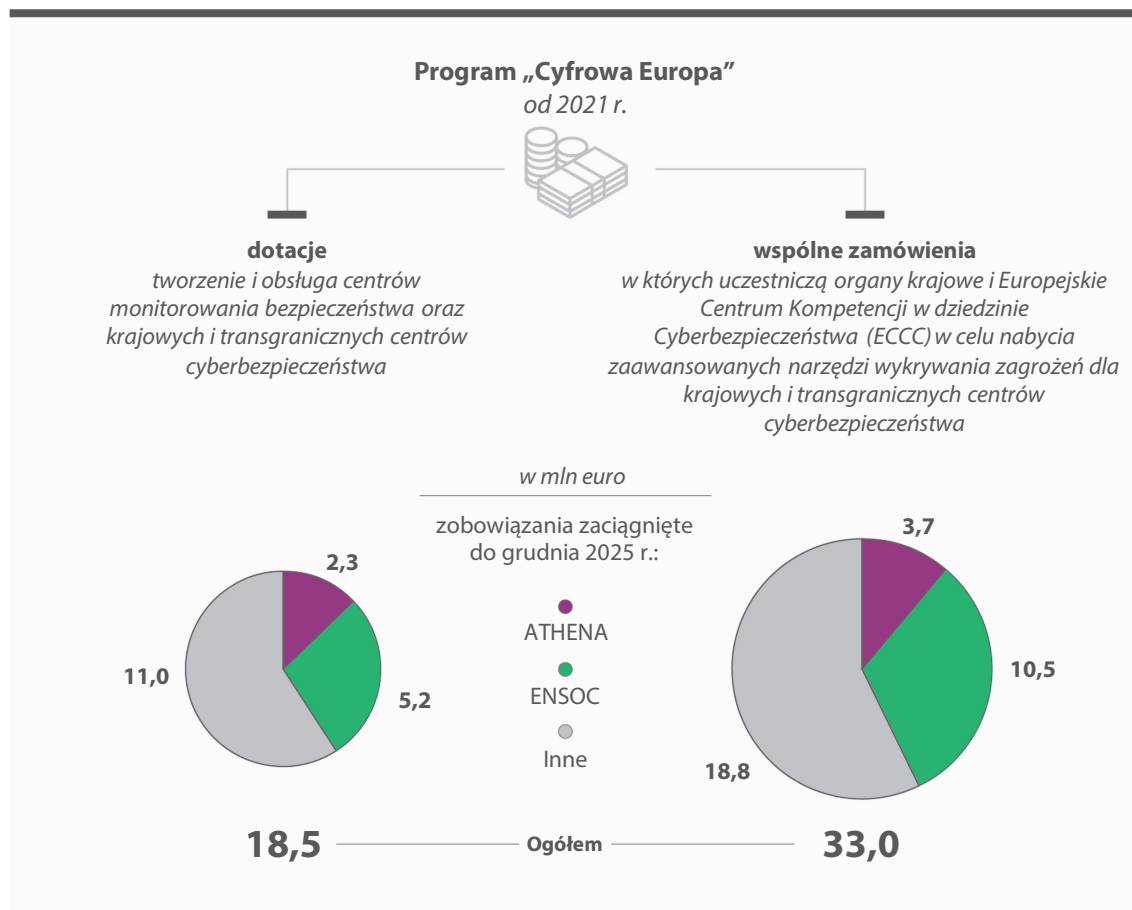
Źródło: Europejski Trybunał Obrachunkowy.

- 64** Trybunał ocenił, w jaki sposób utworzono pierwsze dwa transgraniczne centra cyberbezpieczeństwa, a także ocenił postępy w realizacji celów europejskiego systemu cyberostrzeżeń. Kontrolerzy zbadali również, w jaki sposób utworzone transgraniczne centra cyberbezpieczeństwa wpisują się w szerszą architekturę w dziedzinie cyberbezpieczeństwa i jak współdziałają z istniejącymi sieciami i strukturami.

Do tej pory nie wypracowano konkretnych rezultatów ze względu na znaczne opóźnienia w zamówieniach publicznych

- 65** Od 2021 r. za pośrednictwem platformy programu „Cyfrowa Europa” udostępnia się finansowanie wspierające tworzenie krajowych i transgranicznych centrów cyberbezpieczeństwa. Finansowanie to jest udostępniane w drodze złożonej procedury obejmującej dwa równoległe strumienie: tradycyjne dotacje wspierające tworzenie i funkcjonowanie centrów oraz wspólne zamówienia na zakup zaawansowanych narzędzi wykrywania zagrożeń (stosowne informacje zamieszczono na [rys. 6](#)). Po zaproszeniu do składania wniosków opublikowanym w listopadzie 2022 r. ATHENA i ENSOC rozpoczęły funkcjonowanie w styczniu 2024 r.

Rys. 6 | Finansowanie centrów cyberbezpieczeństwa w ramach programu „Cyfrowa Europa”



Źródło: Europejski Trybunał Obrachunkowy na podstawie danych ECCC.

- 66** Dwuetapowe ograniczone postępowania o udzielenie zamówienia¹¹ zostały zorganizowane przez członków ATHENA i ENSOC, a także DG CONNECT (pierwszy etap) i nowo utworzone ECCC (drugi etap). Podejście dwuetapowe ma na celu ograniczenie obiegu informacji szczególnie chronionych – szczegółowe specyfikacje techniczne zostały przekazane wyłącznie kandydatom wybranym na pierwszym etapie.
- 67** Pierwszy etap rozpoczął się w maju 2024 r. w przypadku ENSOC i w lipcu 2024 r. w przypadku ATHENA. Zainteresowane przedsiębiorstwa miały miesiąc na złożenie ofert. Wybrani oferenci zostali jednak powiadomieni dopiero w kwietniu 2025 r., prawie rok po rozpoczęciu procedury.
- 68** Ponadto procedury udzielania zamówień publicznych nie mogły wówczas przejść do drugiego etapu ani w przypadku ENSOC, ani w przypadku ATHENA, ponieważ członkowie centrów i ECCC nie byli w stanie dostarczyć przedsiębiorstwom umieszczonym na krótkiej liście specyfikacji technicznych niezbędnych do złożenia oferty. Prace nad tymi specyfikacjami nadal trwały.
- 69** Drugi etap postępowań o udzielenie zamówienia rozpoczął się dopiero w sierpniu 2025 r. w odniesieniu do niektórych części zamówienia ENSOC. W przypadku centrum ATHENA drugi etap zaplanowano na początek 2026 r. W momencie przeprowadzania kontroli – 18 miesięcy po wszczęciu postępowania o udzielenie zamówienia – nie podpisano umów w odniesieniu do żadnej z części zamówienia. Trybunał uważa, że brak odpowiedniego przygotowania i złożoność postępowań o udzielenie zamówienia miały negatywny wpływ na ich terminowe zakończenie.
- 70** W związku z tym kontrolerzy stwierdzili, że transgraniczne centra cyberbezpieczeństwa nie są na dobrej drodze do osiągnięcia założonych celów. Wobec braku narzędzi do wykrywania zagrożeń i wymiany informacji działalność operacyjna centrów jest wstrzymana, a europejski system cyberostrzeżeń jeszcze nie funkcjonuje, co opóźnia skuteczny rozwój zaawansowanych zdolności w zakresie wykrywania cyberzagrożeń i cyberincydentów oraz zapobiegania im. W celu przedłużenia okresu obowiązywania umowy o udzielenie dotacji podpisano odpowiednie aneksy, tak aby uwzględnić dotychczasowe opóźnienia w postępowaniach o udzielenie zamówienia (15 miesięcy w przypadku centrum ATHENA i 18 miesięcy w przypadku ENSOC).

¹¹ Zaproszenie do składania ofert ENSOC i zaproszenie do składania ofert ATHENA.

Transgraniczne centra cyberbezpieczeństwa oznaczają utworzenie dodatkowych kanałów komunikacji, co jeszcze bardziej zwiększa złożoność

- 71** Jednym z najważniejszych zadań transgranicznych centrów cyberbezpieczeństwa jest wymiana istotnych informacji w celu poprawy wykrywania zagrożeń i reagowania na nie. Wymiana ta obejmuje informacje na temat cyberzagrożeń, podatności, oznak naruszenia integralności systemu i podmiotów dopuszczających się ataków. Zadania transgranicznych centrów cyberbezpieczeństwa częściowo pokrywają się z zadaniami krajowych CSIRT i sieci CSIRT, w szczególności w odniesieniu do wymiany informacji na temat cyberzagrożeń i podatności na zagrożenia. Nie wytyczono wyraźnej granicy między rolą transgranicznych centrów cyberbezpieczeństwa a rolą zespołów CSIRT. Zgodnie z planem na rzecz cyberbezpieczeństwa z 2025 r. (pkt 29) transgraniczne centra cyberbezpieczeństwa mają działać zarówno na poziomie technicznym (np. krajowe CSIRT i sieć CSIRT), jak i operacyjnym (np. EU-CyCLONe).
- 72** Akt w sprawie cybersolidarności zobowiązuje transgraniczne centra cyberbezpieczeństwa do podpisywania między sobą umów o współpracy. Ma to ułatwić wymianę informacji. Zgodnie z wymogami aktu ENISA powinna była wydać wytyczne dotyczące interoperacyjności między centrami do lutego 2026 r. W międzyczasie w grudniu 2025 r. ECCC przyznało dotację konsorcjum (w tym niektórym członkom centrów ENSOC i ATHENA) w celu określenia technicznych ram interoperacyjności między transgranicznymi centrami cyberbezpieczeństwa. Wytyczne i ramy zostaną jednak sfinalizowane dopiero, gdy centra rozpoczną działalność. Jak wskazał Trybunał w opinii z 2023 r. w sprawie wniosku dotyczącego aktu w sprawie cybersolidarności¹², istnieje ryzyko, że bez szybkiego porozumienia w tej kwestii opracowane zostaną systemy, które będą ze sobą niekompatybilne. To z kolei przełoży się na wzrost kosztów.
- 73** Transgraniczne centra cyberbezpieczeństwa są również zobowiązane do natychmiastowego dzielenia się informacjami na temat incydentów w cyberbezpieczeństwie na dużą skalę z EU-CyCLONe i siecią CSIRT. Na szczeblu państw członkowskich utworzenie krajowych centrów cyberbezpieczeństwa i uczestnictwo w transgranicznych centrach cyberbezpieczeństwa oznacza stworzenie dodatkowych poziomów komunikacji. Koordynacja działań z państwami spoza UE¹³, które nie są członkami sieci CSIRT ani EU-CyCLONe, również zwiększa złożoność.

¹² [Opinia 02/2023](#) w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty, pkt 26.

¹³ Chodzi o Islandię i Norwegię.

- 74** Konieczne byłoby zawarcie jasnych umów o współpracy, tak aby uzgodnić wspólną klasyfikację i sposób wymiany informacji oraz zapewnić interoperacyjność. Wnioski wyciągnięte z działalności sieci CSIRT pokazują, że nastęcza to dużych trudności. Trybunał stwierdził, że do momentu przeprowadzania kontroli nie uzgodniono żadnych procedur dotyczących współpracy i wymiany informacji. Kontrolerzy stoją na stanowisku, że utworzenie krajowych i transgranicznych centrów cyberbezpieczeństwa mogłoby przyczynić się do skuteczniejszej wymiany informacji. Integracja centrów transgranicznych w ramach już i tak bardzo złożonego środowiska cyberbezpieczeństwa będzie jednak wyzwaniem i wymaga ustanowienia dodatkowych kanałów komunikacji oraz zawarcia porozumień dotyczących współpracy.

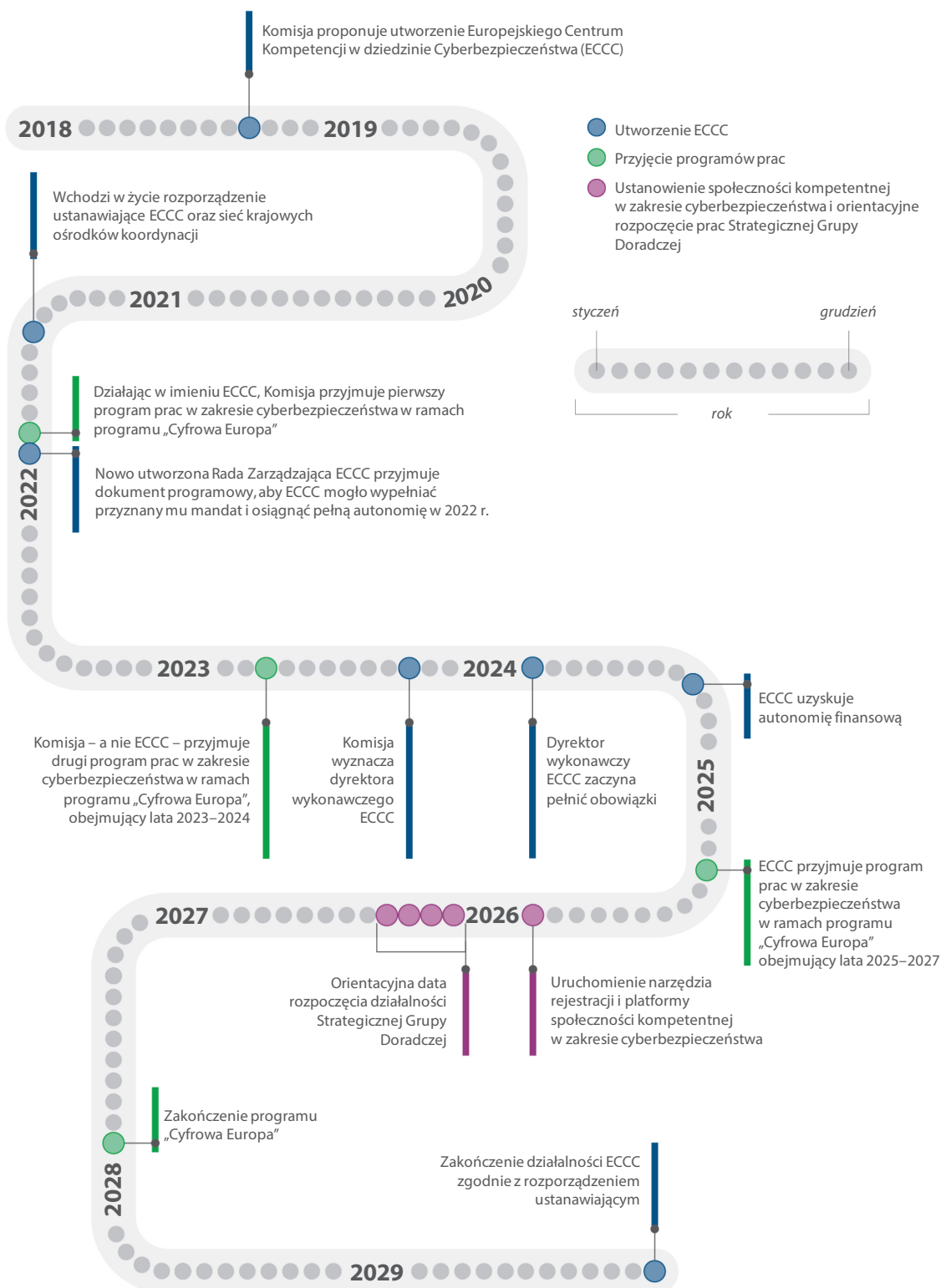
Niektóre projekty finansowane przez UE w ramach programu „Cyfrowa Europa” mają na celu wzmocnienie cyberbezpieczeństwa, ale kontrolerzy odnotowali problemy, jeśli chodzi o wdrożenie i sprawozdawczość

Opóźnienia w ustanowieniu społeczności kompetentnej w zakresie cyberbezpieczeństwa uniemożliwiły jej wzięcie udziału w ukształtowaniu programu „Cyfrowa Europa”, tak aby uwzględnił jej potrzeby

- 75** W 2018 r. Komisja zaproponowała utworzenie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), które miało zarządzać komponentem programu „Cyfrowa Europa” dotyczącym cyberbezpieczeństwa. W rozporządzeniu w sprawie ECCC przewidziano, że ECCC będzie wspierane przez sieć 29 krajowych ośrodków koordynacji, po jednym z każdego państwa członkowskiego oraz po jednym z Islandii i Norwegii. W rozporządzeniu wezwano również do utworzenia społeczności kompetentnej w zakresie cyberbezpieczeństwa (zwanej dalej „społecznością”), składającej się z przedstawicieli branży, organizacji akademickich i badawczych, a także innych odpowiednich stowarzyszeń społeczeństwa obywatelskiego.

- 76** Spośród członków społeczności maksymalnie 20 miało zostać powołanych na członków Strategicznej Grupy Doradczej (SAG), która jest jednym z trzech elementów struktury ECCC. Jednym z kluczowych zadań SAG jest organizowanie konsultacji publicznych, których wyniki mają być wykorzystywane przy opracowywaniu programów prac ECCC i programu „Cyfrowa Europa”.
- 77** Trybunał ocenił, czy program „Cyfrowa Europa” i powiązane z nim programy prac zostały przyjęte na podstawie rzetelnej analizy potrzeb, a także w jaki sposób ECCC, sieć krajowych ośrodków koordynacji, społeczność i SAG były w stanie wnieść wkład we wspomniane programy prac. W praktyce ECCC, sieć krajowych ośrodków koordynacji, społeczność i SAG powstawały stopniowo przez kilka lat (zob. [rys. 7](#)).

Rys. 7 | Kalendarium utworzenia Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa, sieci krajowych ośrodków koordynacji, społeczności i Strategicznej Grupy Doradczej



Źródło: Europejski Trybunał Obrachunkowy.

- 78** Ponieważ ECCC rozpoczęło w pełni działalność operacyjną dopiero we wrześniu 2024 r., programy prac na lata 2021–2022 i 2023–2024 przyjęła w imieniu ECCC Komisja. W przypadku tych dwóch programów prac przyjętych przez Komisję nie było możliwości skorzystania z wkładu społeczności.
- 79** Jednocześnie państwa członkowskie zaczęły ustanawiać krajowe ośrodki koordynacji, które pełnią funkcję krajowych punktów kontaktowych dla społeczności. Ustanowienie i funkcjonowanie tych ośrodków było współfinansowane ze środków programu „Cyfrowa Europa”, przy czym do czasu przeprowadzenia kontroli przyznano na ten cel finansowanie unijne w wysokości ponad 90 mln euro. Około 44 mln euro z tej kwoty ma zostać następnie rozdzielone w ramach wsparcia finansowego na rzecz osób trzecich. Na wsparcie krajowych ośrodków koordynacji przeznaczono dodatkowe 38 mln euro w okresie do 2027 r.
- 80** Trybunał stwierdził, że w grudniu 2025 r. – cztery lata po ustanowieniu ECCC i sieci krajowych ośrodków koordynacji – społeczność nie została jeszcze ustanowiona, a SAG nie została jeszcze powołana. 14 marca 2025 r. ECCC przyjęło najnowszy program prac w zakresie cyberbezpieczeństwa w ramach programu „Cyfrowa Europa” obejmujący lata 2025–2027. Choć ECCC przygotowało i przyjęło program prac po szeroko zakrojonych konsultacjach z państwami członkowskimi i siecią krajowych ośrodków koordynacji, nie mogło skorzystać z wkładu i doradztwa ze strony społeczności ani SAG. Jest to sprzeczne z przepisami rozporządzenia ustanawiającego. Kontrolerzy uznają to za straconą szansę.
- 81** Program „Cyfrowa Europa” wygaśnie w 2027 r. i jeśli nie zostanie on przedłużony, oczekuje się, że ECCC zakończy działalność w 2029 r. W związku z tym wsparcie ze strony sieci krajowych ośrodków koordynacji, społeczności i SAG po ich uruchomieniu może być dostępne jedynie przez krótki okres.

Projekty finansowane przez UE służą realizacji odpowiednich celów, ale w przypadku wielu z nich występują trudności operacyjne

82 Trybunał dobrał próbę 11 projektów związanych z wykrywaniem cyberincydentów i reagowaniem na nie, sfinansowanych w ramach programu „Cyfrowa Europa” w latach 2022–2025 (zob. [rys. 5](#) w [załączniku I](#) i [załączniku III](#)). Kontrolerzy ocenili, czy:

- cele projektów były zgodne z oczekiwanymi wynikami wyrażonymi w naborach wniosków oraz ogólnie z celami programu „Cyfrowa Europa”;
- w ramach projektów udało się do tej pory wypracować planowane produkty i rezultaty;
- produkty zaplanowane w ramach projektów zostały wypracowane w terminie.

Wynik przeprowadzonej przez kontrolerów oceny przedstawiono w [załączniku IV](#).

W niektórych projektach udało się wypracować pierwsze rezultaty, ale w wielu występują trudności operacyjne i opóźnienia

83 Trybunał stwierdził, że zgodnie z zamierzeniami wszystkie projekty przyczyniają się do realizowania celów programu „Cyfrowa Europa” w zakresie cyberbezpieczeństwa¹⁴. W projektach uwzględniono też większość celów ujętych w zaproszeniach do składania wniosków¹⁵.

84 Spośród 11 projektów objętych próbą Trybunału dwa znajdowały się na wczesnym etapie realizacji, w związku z czym kontrolerzy nie byli w stanie sformułować wniosków na temat wyników wypracowanych w tych projektach. Spośród pozostałych projektów cztery Trybunał ocenił jako zadowalające, jeśli chodzi o osiągnięcie planowanych produktów i rezultatów. W dwóch projektach wystąpiły pewne uchybienia, a trzy projekty kontrolerzy ocenili jako niezadowalające (zob. [załącznik IV](#)).

¹⁴ Art. 6 [rozporządzenia \(UE\) 2021/694](#) ustanawiającego program „Cyfrowa Europa”.

¹⁵ Nabory wniosków pod następującymi nazwami: „Capacity building of security operation centres”; „Deploying the network of national coordination centres with member states”; „Preparedness support and mutual assistance”; „Novel applications of AI and other enabling technologies for security operation centres”.

- 85** W programie „Cyfrowa Europa” wyraźnie wskazano jako cel podniesienie poziomu cyberbezpieczeństwa małych i średnich przedsiębiorstw (MŚP), w związku z czym szereg realizowanych projektów ma zapewnić konkretne rozwiązania dla MŚP (zob. [ramka 2](#)).

Ramka 2

Przykłady projektów przynoszących wymierne rezultaty dla MŚP

Projekt [GR-SME-SOC](#) (projekt nr 6 w [załączniku III](#)) ma zapewnić narzędzia i usługi w zakresie cyberbezpieczeństwa MŚP działającym w Grecji przez ustanowienie centrum monitorowania bezpieczeństwa, które będzie dostosowane do potrzeb tych przedsiębiorstw. Projekt rozpoczął się w styczniu 2024 r. i jest realizowany przez konsorcjum pięciu greckich organizacji. Planuje się oferowanie bezpłatnych usług w zakresie cyberbezpieczeństwa 120 MŚP przez okres jednego roku, po czym usługi te zostaną udostępnione na zasadach rynkowych. Projekt oferuje MŚP zaawansowane usługi, takie jak monitorowanie w czasie rzeczywistym, wykrywanie zagrożeń oparte na sztucznej inteligencji i elastyczne reagowanie na incydenty.

W ramach projektu [NCC-IE](#) (projekt nr 3 w [załączniku III](#)) koordynator projektu przekazał około 1,8 mln euro w formie dotacji ponad 50 irlandzkim MŚP w celu poprawy cyberbezpieczeństwa tych przedsiębiorstw. Program dotacji przyniósł korzyści przedsiębiorstwom zatrudniającym od 2 do około 200 pracowników, w tym przedsiębiorstwom rodzinnym, przedsiębiorstwom typu start-up i światowym eksporterom działającym w różnych sektorach. Dotacje były przeznaczone wyłącznie dla przedsiębiorstw, które wcześniej przeszły przegląd w zakresie cyberbezpieczeństwa przeprowadzany przez agencję rządową Enterprise Ireland. Z dotacji można było pokryć 80% kosztów (do 60 000 euro) związanych z wdrożeniem zaleceń wynikających z przeglądu.

Źródło: Europejski Trybunał Obrachunkowy.

- 86** W wielu projektach objętych próbą Trybunału występują trudności z dotrzymaniem terminów lub trudności operacyjne (zob. [załącznik IV](#)). Kontrolerzy odnotowali znaczne opóźnienia w przypadku czterech projektów. Dotyczy to również projektów odnoszących się do centrów ENSOC i ATHENA, jak opisano w pkt [65–70](#). Przykłady takich sytuacji omówiono w [ramce 3](#).

Ramka 3

Przykłady projektów borykających się z trudnościami operacyjnymi i opóźnieniami

W Irlandii jedynym beneficjentem dotacji na projekt **ILG-SOC** (projekt nr 8 w **załączniku III**) jest samorządowa instytucja zarządzająca (LGMA). Celem projektu jest utworzenie centralnego centrum monitorowania bezpieczeństwa dla 31 organów władz lokalnych, aby mogły one korzystać z zaawansowanych narzędzi wykrywania zagrożeń i reagowania na nie. Projekt rozpoczął się w październiku 2023 r. i miał potrwać trzy lata. W wyniku przeglądu śródkresowego odrzucono wszystkie wypracowane do tamtej pory produkty. Kilka postępowań o udzielenie zamówienia w ramach projektu zakończyło się niepowodzeniem lub wystąpiły w nich opóźnienia. Okres realizacji projektu zostanie przedłużony (bez dodatkowego finansowania), co może dać beneficjentowi wystarczająco dużo czasu na wypracowanie rezultatów.

Realizowany w Grecji projekt **EL-SOC** (projekt nr 5 w **załączniku III**) ma na celu utworzenie skonsolidowanego centrum monitorowania bezpieczeństwa na szczeblu krajowym, które gromadziłoby informacje z podobnych centrów sektorowych. Centrum ma zapewnić kompleksowy przegląd sytuacji w zakresie cyberbezpieczeństwa w czasie rzeczywistym. Realizacja projektu ma potrwać od stycznia 2024 r. do grudnia 2026 r. Planowane zamówienie na sprzęt i usługi opóźniło się ze względu na problemy z ukończeniem i opublikowaniem specyfikacji technicznych w ramach zaproszenia do składania ofert. Jako przyczyny opóźnienia koordynator projektu wskazał również trudności związane z zapewnieniem współfinansowania krajowego i ograniczoną dostępnością personelu zajmującego się zamówieniami publicznymi.

Źródło: Europejski Trybunał Obrachunkowy.

- 87** W przypadku dwóch innych projektów objętych próbą Trybunału wystąpiły umiarkowane opóźnienia. W ramach trzech projektów produkty udało się wypracować w terminie. Ponadto dwa projekty znajdują się na wczesnym etapie realizacji, w związku z czym kontrolerzy nie są w stanie dokonać odpowiedniej oceny.

Ograniczenia związane z bezpieczeństwem skutkowały powstaniem trudności operacyjnych, a fakt, że kontrole przeprowadzają sami beneficjenci, wiąże się ze znacznym ryzykiem

- 88** Rozporządzenie w sprawie programu „Cyfrowa Europa” stanowi, że ze względów bezpieczeństwa przyznawanie finansowania na rzecz cyberbezpieczeństwa może zostać ograniczone do podmiotów mających siedzibę w UE i kontrolowanych przez państwa członkowskie lub obywateli UE. Ograniczenie to ma na celu zmniejszenie ryzyka ingerencji bądź wpływu ze strony państw spoza UE oraz zapobieganie sytuacji, w której organy władz spoza UE zyskałyby dostęp do szczególnie chronionych informacji dotyczących bezpieczeństwa.
- 89** Unijny wymóg dotyczący struktury własności i kontroli ma zastosowanie nie tylko do beneficjentów dotacji, ale również do podwykonawców i wszelkich odbiorców wsparcia finansowego przyznawanego osobom trzecim. Z wyjątkiem tej ostatniej kategorii (zob. pkt [92–96](#)) stosowną ocenę przeprowadza Centralny Dział ds. Zatwierdzeń Europejskiej Agencji Wykonawczej ds. Badań Naukowych. Ostateczna decyzja co do kwalifikowalności danych podmiotów do udziału w ograniczonych naborach wniosków pozostaje jednak w gestii organu przyznającego dotację, tj. DG CONNECT lub ECCC.
- 90** W trakcie prac kontrolnych Trybunału beneficjenci, z którymi kontrolerzy przeprowadzili wywiady, wielokrotnie wspominali o praktycznych trudnościach związanych z ocenami struktury własności i kontroli. Ocena struktury własności i kontroli unijnych przedsiębiorstw może być złożonym i długotrwałym procesem. Wymaga ona przeanalizowania pełnej struktury własności i łańcucha kontroli każdej organizacji, w tym wszystkich poziomów struktury własnościowej aż do ostatecznych właścicieli. Centralny Dział ds. Zatwierdzeń wymaga, aby każdy podmiot przedstawił obszerne [dowody w postaci dokumentów](#) potwierdzających strukturę własności i określone uprawnienia, strukturę korporacyjną oraz wszelkie powiązania handlowe, finansowe lub inne zapewniające kontrolę nad danym podmiotem.
- 91** W trzech projektach sfinansowanych przez UE objętych próbą Trybunału co najmniej jeden beneficjent uczestniczący w konsorcjum został później wykluczony, ponieważ uznano, że jest własnością podmiotów spoza UE lub jest przez nie kontrolowany. Wykluczenie członka konsorcjum pokazuje, że unijne pojęcie struktury własności i kontroli nie jest w pełni rozumiane przez wszystkich uczestników programu „Cyfrowa Europa”. Ogólnie rzecz biorąc, z danych Centralnego Działu ds. Zatwierdzeń wynika, że w latach 2022–2025 7% wszystkich wnioskodawców lub podwykonawców ubiegających się o dotacje w dziedzinie cyberbezpieczeństwa w ramach programu „Cyfrowa Europa” nie przeszło przedmiotowej oceny. Składanie wniosków przez niekwalifikujących się uczestników powoduje opóźnienia w naborach wniosków, jak przedstawiono w [ramce 4](#).

Ramka 4

Przykłady sytuacji, gdy beneficjenci zostali wykluczeni po niepomyślnym wyniku kontroli w zakresie bezpieczeństwa

Dwóch członków konsorcjum w ramach projektu **NG-SOC** (projekt nr 7 w **załączniku III**) nie przeszło pomyślnie oceny struktury własności i kontroli. Wynik ogłoszono na około miesiąc przed terminem podpisania umowy o udzielenie dotacji. Koordynator projektu musiał wyrazić zgodę na przejęcie prac przydzielonych dwóm wykluczonym członkom, ponieważ nie było czasu na znalezienie nowego partnera. Jeden z wykluczonych członków należał do konkretnej branży, w której miał być prowadzony pilotaż opracowanego rozwiązania. W związku z tym znaczna część projektu, która dotyczyła testowania rozwiązań w praktyce, nie mogła zostać zrealizowana zgodnie z założeniami. Sytuacji tej udało się później zaradzić, zmieniając umowę o dofinansowanie w celu włączenia do konsorcjum nowych członków.

Źródło: Europejski Trybunał Obrachunkowy.

- 92** W ramach dwóch spośród projektów skontrolowanych przez Trybunał (NCC-IE i CYberSynchrony) zapewniono wsparcie finansowe osobom trzecim. Ten mechanizm finansowania umożliwia beneficjentom dotacji wykorzystanie części finansowania z dotacji do finansowania innych podmiotów w drodze otwartych naborów wniosków. Mechanizm ten może ułatwić dostęp do finansowania unijnego. W takim przypadku wyłączną odpowiedzialność za przeprowadzenie oceny struktury własności i kontroli ponoszą beneficjenci, a Centralny Dział ds. Zatwierdzeń nie angażuje się w te działania.
- 93** W 2021 r. Komisja opublikowała ogólnodostępne wytyczne dla beneficjentów biorących udział w ograniczonych naborach wniosków. Zostały one zaktualizowane w 2026 r. Wprawdzie mechanizm wsparcia finansowego na rzecz osób trzecich funkcjonuje w naborach wniosków w ramach programu „Cyfrowa Europa” już od 2021 r., lecz ani Komisja, ani ECCC nie przedstawiły beneficjentom szczegółowej metodyki dotyczącej tego, jak mieliby oceniać strukturę własności i kontroli osób trzecich, którym udzielają wsparcia finansowego. W lipcu 2025 r. ECCC udostępniło niewiążące wytyczne w tym zakresie, przedstawiając sieci krajowych ośrodków koordynacji ustrukturyzowane podejście do oceny struktury własności i kontroli. Wytyczne wskazują ogólne zasady i czynności, jakie można podjąć. Nie określono w nich jednak, w jaki sposób należy przeprowadzać kontrole, pozostawiając beneficjentom odpowiedzialność za opracowanie własnego podejścia.

- 94** Trybunał stwierdził, że ECCC nie zatwierdza metodyki przyjętej przez beneficjentów ani nie przeprowadza kontroli wrywkowych w celu sprawdzenia, czy metodyka ta jest wystarczająco solidna, a także czy wybrani odbiorcy wsparcia finansowego faktycznie są własnością podmiotów z UE i są kontrolowani przez takie podmioty.
- 95** Ponadto w [sprawozdaniu rocznym za 2024 r.](#) Trybunał stwierdził, że beneficjenci, którym Komisja powierzyła zarządzanie wsparciem finansowym przekazywanym osobom trzecim (w obszarze badań naukowych), nie byli zobowiązani do wykazania, że stosują skuteczne kontrole gwarantujące prawidłowe wydatkowanie środków unijnych. ECCC nie ocenia również zdolności administracyjnych i technicznych beneficjentów w zakresie właściwego przeprowadzania oceny struktury własności i kontroli. Jak pokazano w pkt [90](#), ocena ta może być złożonym przedsięwzięciem i jest przeprowadzana na szczeblu UE przez specjalną służbę dysponującą specjalistyczną wiedzą fachową.
- 96** W związku z powyższym Trybunał uważa, że istnieje znaczne ryzyko, iż beneficjenci, którzy są odpowiedzialni za przeprowadzanie oceny struktury własności i kontroli, nie mają do tego odpowiednich zdolności. Biorąc pod uwagę charakter finansowanych działań, niedociągnięcie to może sprawić, że narażone na szwank będą infrastruktura wrażliwa, dane operacyjne i technologie o kluczowym znaczeniu dla bezpieczeństwa.

W przypadku większości projektów finansowanych przez UE przyjęte ramy wykonania są nieodpowiednie, a dane dotyczące wyników programu „Cyfrowa Europa” związanych z cyberbezpieczeństwem nie są poprawne

W przypadku większości projektów finansowanych przez UE przyjęte ramy wykonania są nieodpowiednie

- 97** Beneficjenci zarządzający projektami finansowanymi przez UE muszą składać ECCC sprawozdania z osiągniętych postępów i wypracowanych rezultatów. Opierają się przy tym na ustalonych kamieniach milowych, produktach i wskaźnikach (zob. [rys. 8](#)). Trybunał ocenił, czy kamienie milowe i produkty określone dla każdego projektu umożliwiają odpowiednie monitorowanie projektów. Kontrolerzy ocenili również, czy wskaźniki wykonania są odpowiednie i wymierne oraz czy określono dla nich poziomy wyjściowe i docelowe.

Rys. 8 | Cele pośrednie, oczekiwane produkty i wskaźniki wykonania w projektach realizowanych w programie „Cyfrowa Europa”

	 Kamienie milowe	 Zaplanowane produkty	 Wskaźniki wykonania
Czym są?	punkty kontrolne w trakcie realizacji projektu, pomagające w mierzeniu postępów	produkty wypracowane w ramach projektu zgłaszane w celu wykazania postępów	są wykorzystywane do pomiaru wyników
Jak powinny zostać zdefiniowane?	powiązane wyłącznie z najważniejszymi (nielicznymi) produktami	tylko najważniejsze produkty (maksymalnie 10–15 na projekt)	skonkretyzowane, mierzalne, osiągalne, realne, określone w czasie
Przykłady	„uruchomienie platformy w fazie pilotażowej”	„opracowanie podręcznika dla użytkowników platformy”	„skrócenie czasu reakcji na incydent o 30%”
	Ustrukturyzowane podejście, część internetowego systemu zarządzania dotacjami		Podejście nieustrukturyzowane

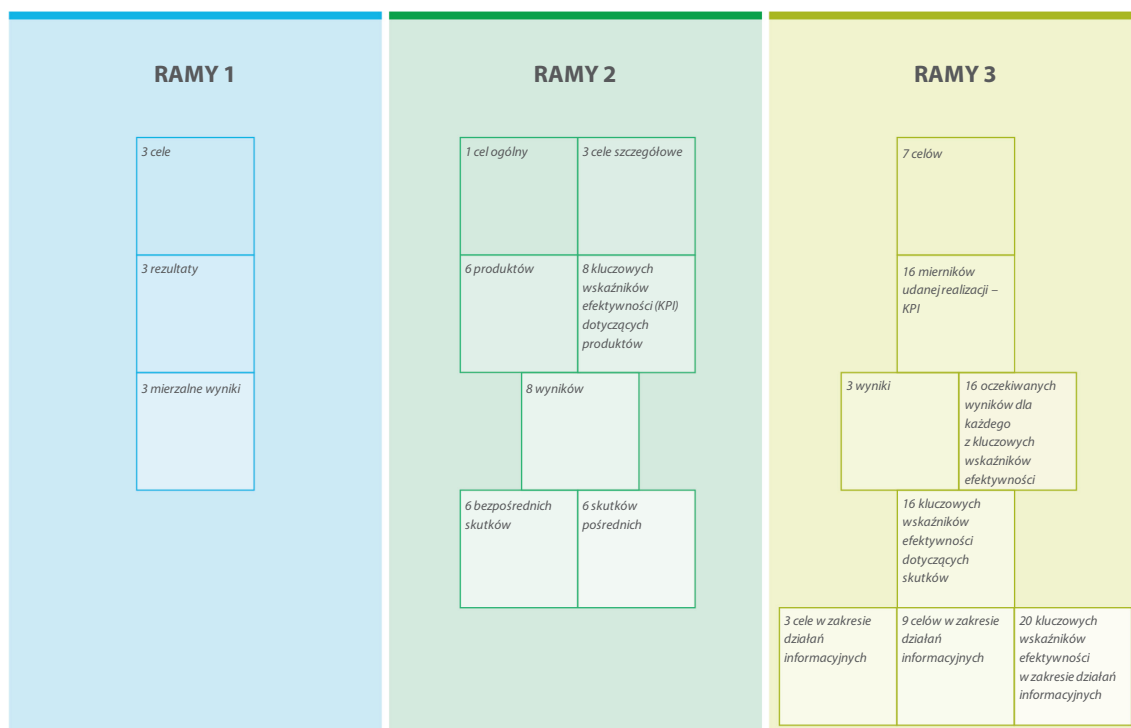
Źródło: Europejski Trybunał Obrachunkowy na podstawie formularza wniosku o przyznanie dotacji.

98 We wniosku beneficjenci muszą określić szereg kamieni milowych i produktów zgodnie z ustrukturyzowanym podejściem określonym w instrukcjach dla wnioskodawców. Wszystkie kamienie milowe i produkty są rejestrowane w internetowym systemie zarządzania dotacjami, aby ułatwić późniejsze monitorowanie. ECCC zazwyczaj dokonuje przeglądu każdego projektu dwukrotnie: w połowie realizacji projektu i po jego zakończeniu. Podczas tych przeglądów eksperci zewnętrznymi weryfikują, czy kamienie milowe zostały osiągnięte, a produkty wypracowane. Następnie ECCC zatwierdza te wyniki. W związku z tym kamienie milowe i produkty mają kluczowe znaczenie dla monitorowania projektów i powinny zostać odpowiednio określone.

99 Trybunał stwierdził, że niemal żaden z projektów objętych próbą nie był opracowany zgodnie z instrukcjami dotyczącymi liczby kamieni milowych i produktów: liczba kamieni milowych na projekt waha się od ośmiu do 39, a liczba produktów, które mają zostać wypracowane – od ośmiu do 45. Wiele kamieni milowych i produktów określono niezgodnie z instrukcjami dotyczącymi tego, jak powinny one być formułowane, i w związku z tym nie są one przydatne do monitorowania postępów (np. „spotkanie w celu rozpoczęcia sporządzania projektu zaproszenia do składania wniosków badawczych” lub „protokół z formalnego posiedzenia zespołu projektowego”). W przypadku trzech projektów komisja oceniająca zidentyfikowała te problemy jeszcze przed podpisaniem umowy o udzielenie dotacji. W dwóch przypadkach beneficjenci zaproponowali jedynie niewielkie zmiany (np. w odniesieniu do terminów), nie odnosząc się do podstawowych kwestii, natomiast w trzecim przypadku nie wprowadzono żadnych zmian. W przypadku sześciu innych projektów objętych próbą przeprowadzona przez Trybunał analiza wykazała, że kamienie milowe lub produkty nie są zgodne z instrukcjami i nie zawsze są odpowiednie. Trybunał uważa, że źle określone produkty lub kamienie milowe – bądź zbyt duża ich liczba – utrudniają śledzenie postępów.

100 W przeciwieństwie do kamieni milowych i założonych produktów wskaźniki wykonania nie musiały być formułowane zgodnie z ustrukturyzowanym podejściem i nie są skonsolidowane w tabeli w systemie zarządzania dotacjami, lecz można je znaleźć w różnych sekcjach składanych wniosków. W konsekwencji beneficjenci zaproponowali bardzo różnorodne ramy wykonania. Podczas gdy część beneficjentów wyznaczyła jedynie cele projektów powiązane ze wskaźnikami wykonania, inni ustanowili znacznie bardziej złożone ramy wykonania. Przykładowe rozwiązania przedstawiono na [rys. 9](#) poniżej.

Rys. 9 | Przykład zróżnicowania ram wykonania opracowanych dla poszczególnych projektów



Źródło: Europejski Trybunał Obrachunkowy.

101 Jak wynika z analizy przeprowadzonej przez kontrolerów Trybunału, wiele wskaźników wykonania stosowanych w ramach projektów jest nieadekwatnych bądź niemierzalnych. Nie określono też poziomów wyjściowych ani docelowych (zob. [ramka 5](#)). W siedmiu projektach określono co najmniej 20 wskaźników, przy czym dla jednego projektu przewidziano 52 wskaźniki. Wynik przeprowadzonej przez kontrolerów oceny przedstawiono w [załączniku IV](#).

Ramka 5

Przykłady nieodpowiednich wskaźników wykonania

Niemierzalne wskaźniki

- „Oznaki naruszenia integralności systemu i inne świadczone usługi zwiększają zdolności MŚP w zakresie cyberbezpieczeństwa”
- „Dostarczanie narzędzi i metod reagowania na incydenty umożliwiających integrację z kanałami komunikacji EU-CyCLONe”

Nie podano poziomu wyjściowego lub docelowego

- „Wzrost poziomu gotowości personelu o $\geq 20\%$ ”
- „Ograniczenie o $\geq 20\%$ wysiłków niezbędnych do dostosowania się do odpowiednich inicjatyw UE w zakresie cyberbezpieczeństwa i do zapewnienia zgodności z tymi inicjatywami”

Wskaźniki niezwiązane z wynikami

- „Sprawozdanie końcowe z realizacji projektu na koniec etapu finansowania”
- „Liczba stażystów, którzy wezmą udział we wszystkich sesjach szkoleniowych”

Źródło: Europejski Trybunał Obrachunkowy na podstawie dokumentacji projektowej.

102 Ogólnie rzecz biorąc, Trybunał uważa, że duże zróżnicowanie ram wykonania, niedopracowana struktura wskaźników i ich nadmierna liczba znacznie komplikują monitorowanie wyników. W konsekwencji właściwa ocena wyników projektów nie jest możliwa. Sytuację dodatkowo komplikuje fakt, że formularz sprawozdawczy nie zawiera specjalnej sekcji dotyczącej wskaźników wykonania obowiązujących w projektach, w związku z czym w większości projektów objętych próbą Trybunału nie przedstawiono informacji na ten temat.

Dane na temat wyników uzyskanych w komponencie programu „Cyfrowa Europa” dotyczącym cyberbezpieczeństwa nie są poprawne

- 103** Aby monitorować osiągnięcia programu „Cyfrowa Europa”, w rozporządzeniu określono wskaźniki programu, które muszą być uwzględniane w sprawozdawczości we wszystkich projektach (jak wyszczególniono w [ramce 6](#)).

Ramka 6

Wskaźniki dotyczące cyberbezpieczeństwa w ramach programu „Cyfrowa Europa”

- 1a. Liczba infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień, w tym w kontekście europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa
- 1b. Liczba zastosowanych infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa
- 2. Liczba użytkowników i społeczności użytkowników uzyskujących dostęp do europejskiej infrastruktury z zakresu cyberbezpieczeństwa
- 3. Liczba działań wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w ramach mechanizmu cyberkryzysowego

Źródło: załącznik II do [rozporządzenia \(UE\) 2021/694 ustanawiającego program „Cyfrowa Europa”](#); ramy monitorowania i oceny programu „Cyfrowa Europa” (SWD(2024) 37).

- 104** Trybunał ocenił, czy w projektach objętych próbą przedstawiono informacje na temat tych wskaźników, i zbadał, w jaki sposób ECCC gromadzi i weryfikuje te dane.
- 105** Beneficjenci wszystkich projektów mają obowiązek przekazywania informacji sprawozdawczych na temat wskaźników programu „Cyfrowa Europa” w systemie zarządzania dotacjami przed dokonaniem śródkresowego i końcowego przeglądu. Trybunał stwierdził, że spośród siedmiu projektów, których realizacja w momencie przeprowadzania kontroli osiągnęła już półmetek i które w związku z tym powinny były przedstawić informacje na temat tych wskaźników, tylko w przypadku trzech z nich takie informacje przekazano. Jeśli chodzi o wspomniane trzy projekty, w przypadku dwóch przekazane informacje nie były poprawne: w jednym przekazano informacje na temat niewłaściwego wskaźnika, w drugim natomiast podano wartości docelowe, a nie informacje na temat wypracowanych rezultatów.

106 Co roku Komisja przedstawia informacje na temat tych wskaźników w [zestawieniach wyników programów](#). Umożliwia to zainteresowanym stronom ocenę, czy w ramach programu osiągnięte są założone cele. Zgodnie z zestawieniami wyników programów za 2024 r. wskaźniki programu „Cyfrowa Europa” dotyczące cyberbezpieczeństwa są na dobrej drodze do osiągnięcia założonych poziomów docelowych. ECCC wyjaśniło kontrolerom Trybunału, że przy zestawianiu tych wskaźników nie opierało się na systemie zarządzania dotacjami, tylko wykorzystało szereg ankiet rozesłanych do beneficjentów projektów. Trybunał dokonał przeglądu zdezagregowanych danych przekazanych przez ECCC i wykrył liczne problemy dotyczące sposobu gromadzenia danych i ich ogólnej jakości. Kontrolerzy stwierdzili, że zgromadzone dane nie odpowiadają wartościom przedstawionym w zestawieniu wyników programów, w związku z czym nie jest jasne, w jaki sposób obliczono podane wartości. Kontrolerzy nie znaleźli dowodów na to, że ECCC zweryfikowało poprawność zgłoszonych danych. Na podstawie kontroli projektów objętych próbą Trybunał stwierdził, że zgłoszone dane nie odzwierciedlają odpowiednio osiągniętych rezultatów, ponieważ brakuje większości wartości lub są one niepoprawne.

Niniejsze sprawozdanie zostało przyjęte przez Izbę III, której przewodniczy George Marius Hyzler, członek Trybunału Obrachunkowego, na posiedzeniu w Luksemburgu w dniu 16 czerwca 2026 r.

W imieniu Trybunału Obrachunkowego

Tony Murphy
Prezes

Załączniki

Załącznik I – O kontroli

- 01** Cyberbezpieczeństwo definiuje się jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”¹. Cyberzagrożenie oznacza z kolei „wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób”². Cyberbezpieczeństwo wymaga przyjęcia całościowego podejścia obejmującego szereg powiązanych ze sobą działań mających na celu zapobieganie cyberzagrożeniom, wykrywanie ich, reagowanie na nie i usuwanie ich skutków, jak pokazano na [rys. 1](#) poniżej.

¹ Rozporządzenie (UE) 2019/881 ([akt o cyberbezpieczeństwie](#)).

² Art. 2 [aktu o cyberbezpieczeństwie](#).

Rys. 1 | Przykłady działań w zakresie cyberbezpieczeństwa

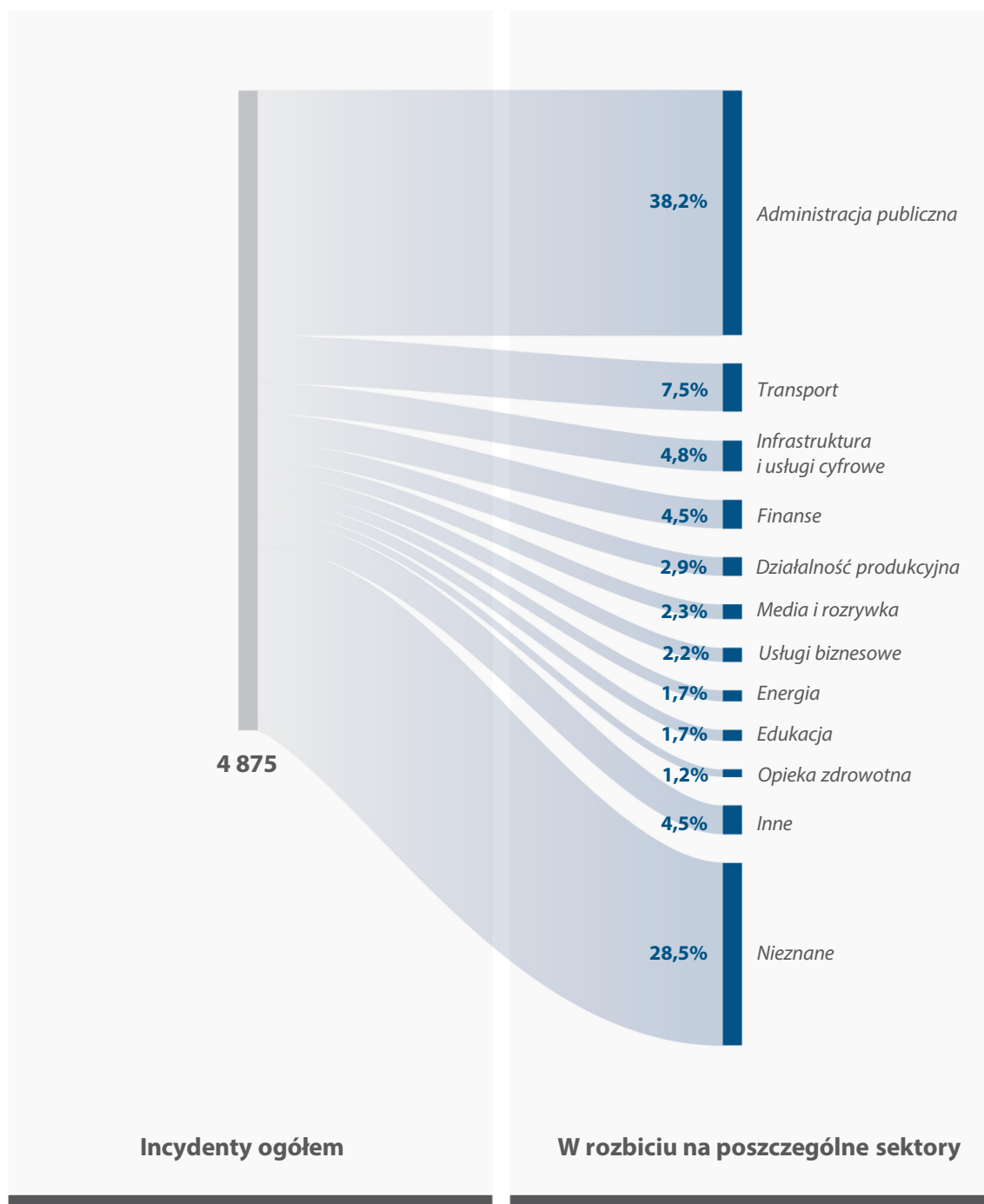
Zapobieganie 	Zmniejszenie ryzyka wystąpienia cyberincydentów i zminimalizowanie potencjalnych skutków <i>Przykłady: oprogramowanie antywirusowe, zapory sieciowe, szyfrowanie, uwierzytelnianie dwuskładnikowe, zarządzanie aktualizacjami oprogramowania, szkolenia dla pracowników uczulające na kwestie związane z bezpieczeństwem</i>
Wykrywanie 	Odkrycie złośliwego działania <i>Przykłady: monitorowanie sieci, orientacja sytuacyjna</i>
Reagowanie 	Zarządzanie cyberincydentem i łagodzenie jego skutków przez ograniczanie rozprzestrzeniania się zagrożenia i zapobieganie dalszym szkodom <i>Przykłady: usuwanie zagrożeń, ograniczanie rozprzestrzeniania się przez izolowanie serwerów, blokowanie uszkodzonych kont i resetowanie haseł</i>
Odtwarzanie awaryjne 	Przywrócenie systemów, danych i usług, których dotyczył incydent, do bezpiecznego i funkcjonalnego stanu <i>Przykłady: ponowne zainstalowanie systemów operacyjnych na oddzielnych serwerach, przywrócenie danych z kopii zapasowych, wyciągnięcie wniosków, aktualizacja obowiązujących zasad</i>

Źródło: Europejski Trybunał Obrachunkowy na podstawie motywu 78 dyrektywy (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (dyrektywy NIS 2).

02 Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) uważa, że poziom zagrożeń w dziedzinie cyberbezpieczeństwa jest znaczny. Zauważa jednocześnie, że środowisko zagrożeń dla cyberbezpieczeństwa stało się znacznie bardziej złożone, a złożoność ta wciąż rośnie³. Konstatacja ta zwraca uwagę na kluczowe znaczenie cyberbezpieczeństwa w gospodarkach i społeczeństwach, w których rola technologii cyfrowych rośnie. W [sprawozdaniu dotyczącym zagrożeń](#) z 2025 r. ENISA wskazała oprogramowanie szantażujące jako najpoważniejsze zagrożenie w UE. Na [rys. 2](#) przedstawiono najważniejsze sektory, na które ukierunkowane są cyberataki.

³ Sprawozdanie ENISA z 2024 r. o stanie cyberbezpieczeństwa w Unii.

Rys. 2 | Sektory, na które ukierunkowane są cyberataki



Źródło: Europejski Trybunał Obrachunkowy na podstawie informacji przekazanych przez ENISA.

Poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę

- 03** Incydenty w cyberbezpieczeństwie, które obejmują cyberzagrożenia i niezamierzone zdarzenia (takie jak te wymienione na [rys. 3](#) i w pkt [40](#)), „mogą utrudniać świadczenie usług publicznych [...] oraz utrudniać prowadzenie działalności gospodarczej, [...] powodować znaczne straty finansowe, podważać zaufanie użytkowników, powodować poważne szkody dla gospodarki i systemów demokratycznych Unii, a nawet mieć konsekwencje zagrażające zdrowiu lub życiu”⁴. Cyberincydent uznaje się za⁵:
- **poważny**, jeśli spowodował lub może spowodować znaczne zakłócenia operacyjne w świadczeniu usług lub straty finansowe dla danego podmiotu, lub jeśli dotknął lub może dotknąć inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe;
 - **na dużą skalę**, jeśli spowodował zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania lub wywiera znaczące skutki w co najmniej dwóch państwach członkowskich.
- 04** Incydent na dużą skalę może przerodzić się w rozległy **kryzys cyberbezpieczeństwa w UE**, jeśli uniemożliwi prawidłowe funkcjonowanie rynku wewnętrznego lub będzie stanowić poważne zagrożenie dla bezpieczeństwa publicznego i ryzyko dla bezpieczeństwa podmiotów lub obywateli w kilku państwach członkowskich lub w całej Unii⁶.

⁴ Motyw 2 rozporządzenia (UE) 2025/38 ([akt w sprawie cybersolidarności](#)).

⁵ Art. 6 i 23 [dyrektywy NIS 2](#), doprecyzowane w [rozporządzeniu wykonawczym Komisji \(UE\) 2024/2690](#) w odniesieniu do szeregu dostawców w sektorze infrastruktury cyfrowej.

⁶ Motyw 69 [dyrektywy NIS 2](#).

Ramy polityczne UE

- 05** Unijne cyberśrodowisko jest złożone i wielowarstwowe. Obejmuje cały wachlarz obszarów polityki wewnętrznej, takich jak wymiar sprawiedliwości i sprawy wewnętrzne, jednolity rynek cyfrowy i strategie dotyczące badań naukowych⁷. W polityce zewnętrznej kwestie dotyczące cyberbezpieczeństwa pojawiają się w dyplomacji i w coraz większym stopniu stanowią element kształtującej się unijnej polityki w dziedzinie obronności⁸.
- 06** W ostatnich latach UE wzmocniła własne ramy regulacyjne w dziedzinie cyberbezpieczeństwa. Na [rys. 3](#) poniżej przedstawiono najistotniejsze akty prawne i instrumenty polityki na szczeblu UE. Zgodnie z zakresem kontroli (zob. pkt [13–14](#)) Trybunał skoncentrował się na instrumentach służących wykrywaniu poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę oraz reagowaniu na nie.

⁷ Dokument analityczny Europejskiego Trybunału Obrachunkowego pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją”, s. 12.

⁸ Na przykład konkluzje Rady w sprawie rozwijania pozycji Unii Europejskiej w kwestiach cyberprzestrzeni (2022 r.), wytyczne dotyczące ram skoordynowanej reakcji UE na kampanie hybrydowe (2022 r.), polityka UE w zakresie cyberobrony (2023 r.) oraz zmieniony zestaw narzędzi dla dyplomacji cyfrowej (2023 r.).

Rys. 3 | Odpowiednie przepisy i instrumenty polityki UE

- Przyjmowanie aktów prawnych i instrumentów polityki
- Tworzenie sieci i struktur



Źródło: Europejski Trybunał Obrachunkowy.

Role i obowiązki

- 07** W UE w kwestię cyberbezpieczeństwa są zaangażowane liczne cywilne podmioty publiczne i prywatne na szczeblu regionalnym, krajowym i unijnym (w tym organy ścigania). Cyberbezpieczeństwo jest ponadto kluczowym elementem bezpieczeństwa narodowego i obrony narodowej⁹. W [załączniku II](#) przedstawiono obecną sytuację w UE w tej dziedzinie.
- 08** Odpowiedzialność za zapobieganie incyidentom i sytuacjom kryzysowym związanym z cyberbezpieczeństwem oraz przygotowywanie się i reagowanie na nie ponoszą przede wszystkim państwa członkowskie, których dany incydent bądź sytuacja kryzysowa dotyczy. Zgodnie z art. 4 ust. 2 [Traktatu o Unii Europejskiej](#) bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego. Ponieważ cyberincydenty mogą prowadzić do zakłóceń i uszkodzenia krytycznej infrastruktury informatycznej, która jest z kolei niezbędna do sprawnego funkcjonowania rynku wewnętrznego, również UE ma do odegrania ważną rolę w przypadku wystąpienia poważnego incydentu lub kryzysu¹⁰. Główne podmioty na szczeblu UE zajmujące się cyberbezpieczeństwem opisano na [rys. 4](#) poniżej.

⁹ [Opinia 02/2023](#) w sprawie proponowanego aktu w sprawie cybersolidarności.

¹⁰ [Plan działania UE na rzecz zarządzania cyberkryzysami](#).

Rys. 4 | Podmioty na szczeblu UE odgrywające kluczową rolę w dziedzinie cyberbezpieczeństwa



Źródło: Europejski Trybunał Obrachunkowy.

Finansowanie unijne

- 09** W bieżących wieloletnich ramach finansowych na lata 2021–2027 głównym źródłem finansowania w dziedzinie cyberbezpieczeństwa jest [program „Cyfrowa Europa”](#). Jest on pierwszym programem UE, którego celem jest pobudzenie transformacji cyfrowej UE. Całkowity budżet programu, uruchomionego w 2021 r., wynosi 8,1 mld euro¹¹.
- 10** W ramach celu szczegółowego nr 3 programu „Cyfrowa Europa” – „Cyberbezpieczeństwo i zaufanie” – finansowane są działania w zakresie cyberbezpieczeństwa. Jeśli chodzi o szczegółowy rozkład środków, 1,4 mld euro przeznaczono na:
- usprawnienie koordynacji w zakresie cyberbezpieczeństwa między narzędziami państw członkowskich a infrastrukturą danych;
 - wspieranie szerokiego wdrożenia najnowszych rozwiązań z zakresu cyberbezpieczeństwa w całej gospodarce.
- 11** Większość finansowania z programu „Cyfrowa Europa” na rzecz cyberbezpieczeństwa jest udostępniana za pośrednictwem naborów wniosków, przy czym w okresie od listopada 2021 r. do grudnia 2025 r. ogłoszono 12 takich naborów. Kwota finansowania unijnego udostępnionego w ramach tych naborów wyniosła 825 mln euro. Na lata 2026 i 2027 planowane są nowe nabory wniosków w celu przyznania kolejnych 212 mln euro w formie dotacji.
- 12** Kolejnym ważnym programem UE wspierającym cyberbezpieczeństwo jest [program „Horyzont Europa”](#). Projekty w zakresie cyberbezpieczeństwa są finansowane głównie w ramach [klastra 3](#) – „Bezpieczeństwo cywilne na rzecz społeczeństwa” – i zazwyczaj znajdują się na wczesnym etapie zaawansowania ze względu na ukierunkowanie programu „Horyzont Europa” głównie na badania naukowe i innowacje. Również ze środków [Instrumentu na rzecz Odbudowy i Zwiększania Odporności](#) zapewniane jest finansowanie na rzecz cyberbezpieczeństwa.

¹¹ Program „Cyfrowa Europa”.

Zakres kontroli i podejście kontrolne

13 Rosnące cyberzagrożenia i ich potencjalne skutki zwróciły uwagę na konieczność wzmocnienia wspólnej cyberodporności UE. Celem kontroli Trybunału była ocena, na ile skutecznie działania UE ułatwiają wykrywanie poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, a także reagowanie na nie. W szczególności Trybunał przeanalizował sytuację w odniesieniu do:

- sieci i mechanizmów na szczeblu UE (tj. sieci CSIRT, EU-CyCLONe, europejskiego systemu cyberostrzeżeń, centrum ds. orientacji sytuacyjnej oraz rezerwy cyberbezpieczeństwa UE);
- działań sfinansowanych w ramach programu „Cyfrowa Europa”.

Trybunał nie objął zakresem kontroli współpracy organów ścigania na szczeblu UE ani działań w zakresie cyberprewencji podejmowanych na szczeblu UE za pomocą środków dyplomatycznych lub działań obronnych.

14 Przeprowadzona kontrola objęła lata 2022–2025. Ustalenia sformułowano na podstawie przeglądu dokumentacji i analizy odpowiednich dokumentów, wizyt kontrolnych w trzech państwach członkowskich (w Irlandii, Grecji i we Włoszech) oraz na podstawie pisemnych kwestionariuszy i wywiadów z odpowiednimi zainteresowanymi stronami. Na [rys. 5](#) przedstawiono, w jaki sposób Trybunał uzyskał dowody, które stały się podstawą sformułowanych uwag.

Rys. 5 | Przeprowadzone prace kontrolne

Trybunał zbadał:

- **ramy prawne** mające zastosowanie do wykrywania poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę oraz reagowania na nie
- **role i obowiązki** sieci i struktur utworzonych na szczeblu UE

Trybunał przeanalizował:

- dokumenty dotyczące funkcjonowania **sieci CSIRT i EU-CyCLONe**
 - dokumentację dotyczącą **ram programowania i monitorowania realizacji celów w ramach programu „Cyfrowa Europa”**
 - dokumentację dotyczącą **13 wybranych działań finansowanych przez UE** (11 dotacji i 2 umowy – zob. szczegółowy wykaz w załączniku III)
- * Trybunał wybrał działania finansowane przez UE w trzech państwach (Irlandia, Grecja i Włochy), w których kwoty przedmiotowego finansowania z programu „Cyfrowa Europa” były największe. 11 dotacji dobrano z wykazu 137 projektów finansowanych przez UE istotnych z punktu widzenia wykrywania zagrożeń i reagowania na nie. Kontrolerzy starali się dobrać do próby zróżnicowany zestaw projektów.

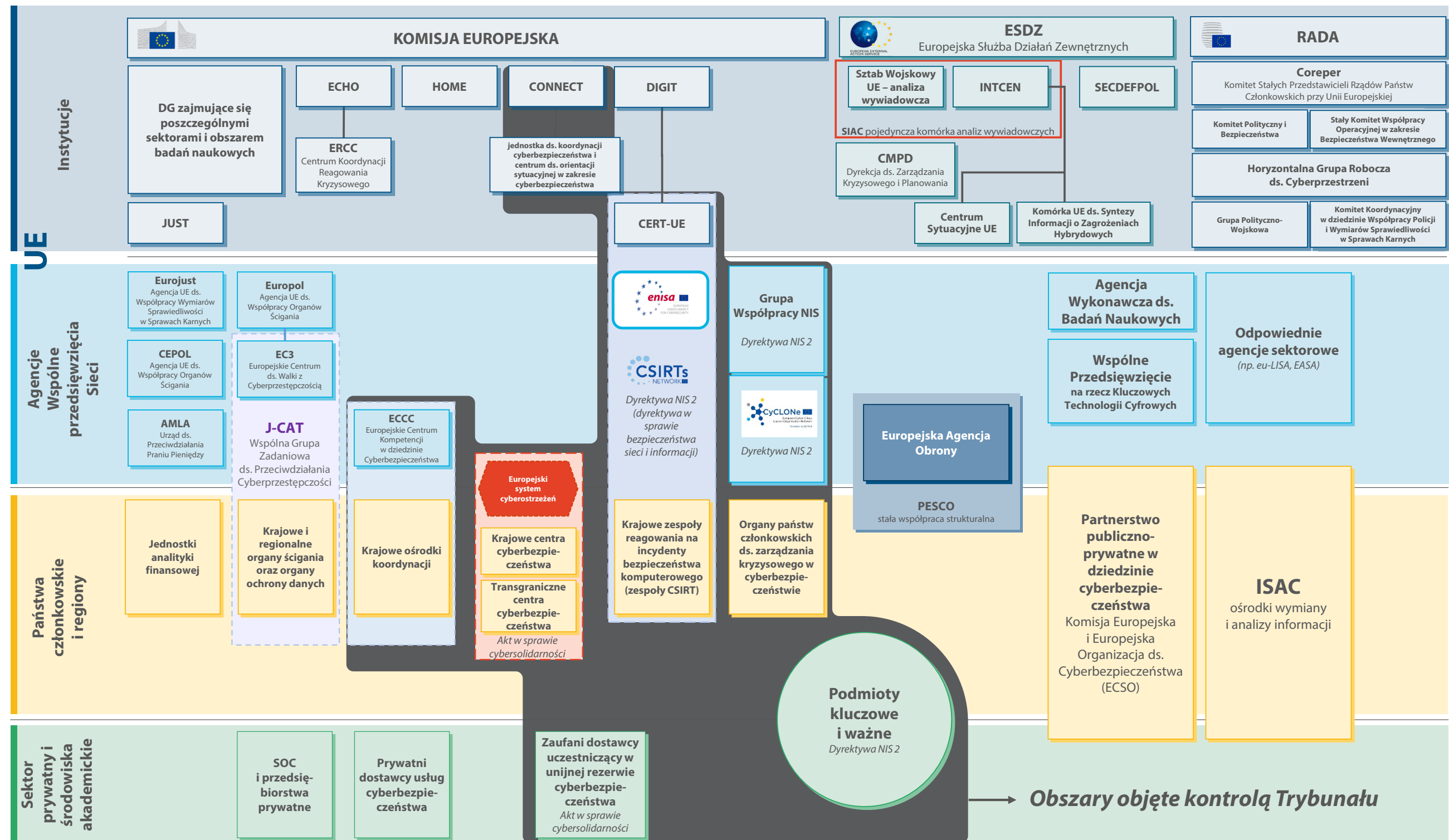
Trybunał przeprowadził wywiady z:

- beneficjentami **11 objętych próbą dotacji finansowanych przez UE**
- przedstawicielami krajowych organów odpowiedzialnych za cyberbezpieczeństwo w **trzech państwach członkowskich** (Irlandia, Grecja i Włochy)
- przedstawicielami Komisji Europejskiej (**DG CONNECT**), **ENISA** i **ECCC**

Źródło: Europejski Trybunał Obrachunkowy.

- 15** W zamierzeniu Trybunału sformułowane ustalenia przyczynią się do poprawy skuteczności i efektywności unijnego wykrywania poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę oraz reagowania na nie, a także do poprawy sposobu wyboru i monitorowania działań finansowanych przez UE. [Metodyka kontroli](#) stosowana przez Trybunał jest zgodna z międzynarodowymi standardami rewizji finansowej ustanowionymi przez [Międzynarodową Organizację Najwyższych Organów Kontroli \(INTOSAI\)](#).

Załącznik II – Środowisko UE w dziedzinie cyberbezpieczeństwa



DG CONNECT – Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii
DG ECHO – Dyrekcja Generalna ds. Prowadzonych przez UE Operacji Ochrony Ludności i Pomocy Humanitarnej

DG HOME – Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych
DG JUST – Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów
DG DIGIT – Dyrekcja Generalna ds. Usług Cyfrowych
EASA – Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego

EU-CyCLONe – europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa
eu-LISA – Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości

INTCEN – Centrum Analiz Wywiadowczych Unii Europejskiej
SECDEFPOL – Dyrekcja ds. Polityki Bezpieczeństwa i Obrony
SOC – centrum monitorowania bezpieczeństwa

Załącznik III – Wybrane działania w zakresie cyberbezpieczeństwa

Nr identyfikacyjny	Nazwa	Państwa	Data rozpoczęcia	Data zakończenia	Łączny koszt (w mln euro) i wkład UE (w %)	Link do unijnego portalu Funding & Tenders
Dotacje na rzecz transgranicznych centrów cyberbezpieczeństwa, które są częścią europejskiego systemu cyberostrzeżeń						
1	Ustanowienie transgranicznych centrów monitorowania bezpieczeństwa (ATHENA)	Bułgaria, Grecja, Cypr, Malta	1.1.2024	31.3.2028	4,7 (50%)	
2	Platforma transgraniczna ENSOC (ENSOC)	Hiszpania, Włochy, Luksemburg, Niderlandy, Austria, Portugalia, Rumunia	1.1.2024	30.6.2028	10,4 (50%)	
Dotacje na rzecz uruchomienia sieci krajowych ośrodków koordynacji w państwach członkowskich						
3	Opracowanie koncepcji i ustanowienie Krajowego Centrum Koordynacji i Rozwoju w dziedzinie Cyberbezpieczeństwa w Irlandii (NCC-IE)	Irlandia	2.10.2023	1.10.2026	4,2 (47%)	
4	Włoski krajowy ośrodek koordynacji (NCC-IT)	Włochy	1.11.2023	31.10.2025	2,0 (50%)	

Nr identyfikacyjny	Nazwa	Państwa	Data rozpoczęcia	Data zakończenia	Łączny koszt (w mln euro) i wkład UE (w %)	Link do unijnego portalu Funding & Tenders
Dotacje na budowanie zdolności centrów monitorowania bezpieczeństwa, promowanie nowatorskich zastosowań sztucznej inteligencji i innych technologii użytecznych dla funkcjonowania centrów monitorowania bezpieczeństwa oraz udzielanie wsparcia w zakresie zapewniania gotowości i wzajemnej pomocy						
5	Zwiększenie zdolności greckiego głównego centrum monitorowania bezpieczeństwa (EL-SOC)	Grecja, Cypr	1.1.2024	31.12.2026	9,7 (50%)	
6	Greckie Centrum Monitorowania Bezpieczeństwa dla Małych i Średnich Przedsiębiorstw (GR-SME-SOC)	Grecja	1.1.2024	31.12.2026	12,1 (50%)	
7	Centra monitorowania bezpieczeństwa nowej generacji (NG-SOC)	Grecja, Hiszpania, Cypr, Luksemburg, Słowenia, Norwegia	1.1.2024	31.12.2026	4,8 (50%)	
8	Centrum monitorowania bezpieczeństwa dla irlandzkiego samorządu (ILG-SOC)	Irlandia	1.10.2023	30.9.2026	8,3 (50%)	
9	Wzajemnie połączony system sieci koordynacji i reagowania w zakresie cyberbezpieczeństwa (Cyber-CORE-Network)	Irlandia	1.1.2024	31.12.2026	3,6 (50%)	
10	Harmonizacja zaangażowanych osób, procesów i technologii na rzecz wzmocnienia cyberbezpieczeństwa (CYberSynchrony)	Belgia, Grecja, Włochy, Cypr, Niderlandy	1.6.2024	31.5.2027	7,0 (100%)	
11	Zaawansowane wspólne centra monitorowania bezpieczeństwa (ACSOC)	Grecja, Włochy, Rumunia	1.1.2025	31.12.2027	3,0 (50%)	

Nr identyfikacyjny	Nazwa	Państwa	Data rozpoczęcia	Data zakończenia	Łączny koszt (w mln euro) i wkład UE (w %)	Link do unijnego portalu Funding & Tenders
Umowa ramowa dotycząca działania ENISA na rzecz wsparcia cyberbezpieczeństwa						
12	Pomoc ENISA w świadczeniu usług w ramach działania na rzecz wsparcia cyberbezpieczeństwa (28 części)	27 części dotyczących poszczególnych państw członkowskich 1 część ogólnoeuropejska	1.12.2022 ¹	31.12.2025	28,3 (100%)	
Umowa o świadczenie usług dla centrum DG CONNECT ds. orientacji sytuacyjnej						
13	Specjalna służba wspierająca centrum Komisji Europejskiej ds. orientacji sytuacyjnej i analiz w zakresie cyberbezpieczeństwa	–	30.12.2022	30.12.2026	18,0 (100%)	

Źródło: Europejski Trybunał Obrachunkowy.

¹ W grudniu 2022 r. podpisano wiele umów w ramach zamówienia.

Załącznik IV – Przeprowadzona przez Trybunał ocena projektów w dziedzinie cyberbezpieczeństwa sfinansowanych ze środków UE

Nr identyfikacyjny	Projekt	Wynik zadowalający Wynik niezadowalający Występują pewne uchybienia Nie można sformułować wniosków (projekt na zbyt wczesnym etapie)				Projekt odpowiada na większość potrzeb określonych w zaproszeniu do składania wniosków	W ramach projektu udało się do tej pory wypracować planowane produkty i rezultaty	Produkty wypracowane w ramach projektu zostały dostarczone w wymaganym terminie	Wskaźniki wykonania są odpowiednie i wymierne oraz określono dla nich poziomy wyjściowe i docelowe
1	Ustanowienie transgranicznych centrów monitorowania bezpieczeństwa (ATHENA)								
2	Platforma transgraniczna ENSOC (ENSOC)								
3	Opracowanie koncepcji i ustanowienie Krajowego Centrum Koordynacji i Rozwoju w dziedzinie Cyberbezpieczeństwa w Irlandii (NCC-IE)								
4	Włoski krajowy ośrodek koordynacji (NCC-IT)								
5	Zwiększenie zdolności greckiego głównego centrum monitorowania bezpieczeństwa (EL-SOC)								
6	Greckie Centrum Monitorowania Bezpieczeństwa dla Małych i Średnich Przedsiębiorstw (GR-SME-SOC)								
7	Centra monitorowania bezpieczeństwa nowej generacji (NG-SOC)								
8	Centrum monitorowania bezpieczeństwa dla irlandzkiego samorządu (ILG-SOC)								
9	Wzajemnie połączony system sieci koordynacji i reagowania w zakresie cyberbezpieczeństwa (Cyber-CORE-Network)								
10	Harmonizacja zaangażowanych osób, procesów i technologii na rzecz wzmocnienia cyberbezpieczeństwa (CYberSynchrony)								
11	Zaawansowane wspólne centra monitorowania bezpieczeństwa (ACSOC)								

Akronimy

Akronim	Definicja / wyjaśnienie
CSIRT	zespół reagowania na incydenty bezpieczeństwa komputerowego
DG CONNECT	Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii
ECCC	Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa
ENISA	Agencja Unii Europejskiej ds. Cyberbezpieczeństwa
EU-CyCLONe	europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa
MŚP	małe i średnie przedsiębiorstwa
NIS	bezpieczeństwo sieci i informacji
SAG	Strategiczna Grupa Doradcza
SOC	centrum monitorowania bezpieczeństwa

Glosariusz

Termin	Definicja / wyjaśnienie
Centrum ds. cyberprzestrzeni	Centralna platforma skupiająca różne służby, narzędzia i specjalistów IT w celu poprawy monitorowania, wykrywania i analizy cyberzagrożeń, zapobiegania cyberincydentom i wspierania analizowania cyberzagrożeń.
Centrum monitorowania bezpieczeństwa	Jednostka organizacyjna zajmująca się zapobieganiem cyberzagrożeniom i cyberincydentom oraz gromadzeniem powiązanych informacji.
Cyberincydent; incydent cyberbezpieczeństwa; incydent w cyberbezpieczeństwie	Wydarzenie naruszające dostępność, autentyczność, integralność lub poufność danych bądź systemów informatycznych.
Cyberzagrożenie	Potencjalne wykorzystanie cyberprzestrzeni w taki sposób, by naruszyć dostępność, autentyczność, integralność lub poufność danych bądź systemów informatycznych.
Incydent w cyberbezpieczeństwie na dużą skalę	Incydent w cyberbezpieczeństwie, który powoduje zbyt poważne zakłócenia, aby państwo członkowskie było w stanie poradzić sobie z nimi samodzielnie lub który wywiera znaczące skutki w co najmniej dwóch państwach członkowskich.
Oprogramowanie szantażujące (ransomware)	Złośliwe oprogramowanie, które pozbawia ofiarę dostępu do systemu komputerowego lub szyfruje pliki, uniemożliwiając dostęp do nich i zazwyczaj zmuszając ofiarę do zapłacenia okupu w celu przywrócenia dostępu.
Podmiot stwarzający zagrożenie	Osoba lub grupa osób celowo wyrządzająca szkodę, zakłócająca świadczenie usług lub dopuszczająca się kradzieży danych przez wykorzystanie luk w zabezpieczeniach systemów, sieci i urządzeń informatycznych.
Poważny incydent w cyberbezpieczeństwie	Incydent w cyberbezpieczeństwie, który spowodował lub może spowodować dotkliwe zakłócenia lub straty finansowe dla danej organizacji bądź wyrządzić znaczne szkody innym podmiotom lub osobom.
Systematyka	W kontekście cyberbezpieczeństwa oznacza system klasyfikacji wykorzystywany do organizowania, kategoryzacji i strukturyzowania wiedzy na temat kluczowych pojęć, takich jak zagrożenia i incydenty.

Odpowiedzi Komisji

<https://www.eca.europa.eu/pl/publications/SR-2026-19>

Odpowiedzi Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC)

<https://www.eca.europa.eu/pl/publications/SR-2026-19>

Odpowiedzi Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)

<https://www.eca.europa.eu/pl/publications/SR-2026-19>

Kalendarium

<https://www.eca.europa.eu/pl/publications/SR-2026-19>

Zespół kontrolny

W sprawozdaniach specjalnych Trybunału przedstawiane są wyniki kontroli dotyczących obszarów polityki i programów UE bądź kwestii związanych z zarządzaniem w wybranych obszarach budżetowych. Trybunał wybiera i opracowuje zadania kontrolne tak, aby osiągnąć jak największe oddziaływanie, biorąc przy tym pod uwagę kryteria takie jak zagrożenia dla realizacji celów lub zgodności, poziom dochodów lub wydatków w danym obszarze, nadchodzące zmiany oraz interes polityczny i społeczny.

Niniejsza kontrola wykonania zadań została przeprowadzona przez Izbę III – której przewodniczy członek Trybunału George-Marius Hyzler – zajmującą się obszarami wydatków dotyczącymi działań zewnętrznych, bezpieczeństwa i wymiaru sprawiedliwości. Kontrolą kierował członek Trybunału George-Marius Hyzler, a w prace kontrolne zaangażowani byli: Romuald Kayibanda, szef gabinetu; Annette Farrugia, attaché; Cyril Messein, kierownik; Frédéric Soblet, koordynator zadania, a także kontrolerzy: Jurgen Manjé i Flavia Di Marco. Wsparcia językowego udzieliła Zoe Amador Martínez, a wsparcia w opracowaniu materiałów graficznych – Dunja Weibel.



Od lewej: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

PRAWA AUTORSKIE

© Unia Europejska, 2026.

Polityka Europejskiego Trybunału Obrachunkowego w zakresie ponownego wykorzystywania dokumentów została określona w [decyzji Trybunału nr 6-2019](#) w sprawie polityki otwartych danych oraz ponownego wykorzystywania dokumentów.

O ile nie wskazano inaczej (np. nie zamieszczono szczegółowych adnotacji o prawach autorskich), treści Europejskiego Trybunału Obrachunkowego będące własnością UE objęte są licencją [Creative Commons Uznanie autorstwa 4.0 Międzynarodowe \(CC BY 4.0\)](#).

Oznacza to, że co do zasady ponowne wykorzystanie jest dozwolone, pod warunkiem że treści zostaną odpowiednio oznaczone i zostaną wskazane dokonane w nich zmiany. W przypadku ponownego wykorzystania treści Trybunału niedozwolone jest zmienianie ich oryginalnego znaczenia albo przesłania. Trybunał nie ponosi odpowiedzialności za jakiegokolwiek konsekwencje ponownego wykorzystywania.

Jeżeli konkretna treść wskazuje na możliwą do zidentyfikowania osobę fizyczną – tak jak w przypadku zdjęć, na których widoczni są pracownicy Trybunału – lub zawiera prace stron trzecich, wymagane jest uzyskanie dodatkowego zezwolenia.

W takim przypadku uzyskane dodatkowe zezwolenie na ponowne wykorzystanie określonej treści unieważnia i zastępuje wspomniane wcześniej zezwolenie ogólne. Powinny być w nim wyraźnie wskazane wszelkie ograniczenia dotyczące wykorzystania treści.

W celu wykorzystania lub powielenia treści niebędącej własnością UE konieczne może być wystąpienie o zgodę bezpośrednio do właścicieli praw autorskich.

Zdjęcie na stronie tytułowej: © 4AXY – stock.adobe.com.

Ikony na rys. 6 i 8: materiały zostały opracowane z wykorzystaniem zasobów ze strony [Flaticon.com](#). © Freepik Company S.L. Wszelkie prawa zastrzeżone.

Mapy na rys. 5: [Eurostat](#).

Oprogramowanie lub dokumenty objęte prawem własności przemysłowej, takie jak patenty, znaki towarowe, wzory użytkowe, znaki graficzne i nazwy, nie są objęte polityką Europejskiego Trybunału Obrachunkowego w zakresie ponownego wykorzystywania.

Na stronach internetowych instytucji Unii Europejskiej dostępnych w domenie europa.eu zamieszczane są linki do stron zewnętrznych. Trybunał nie ma kontroli nad ich zawartością i w związku z tym zachęca użytkowników, aby we własnym zakresie zapoznali się z polityką ochrony prywatności i polityką w zakresie praw autorskich obowiązującymi na tych stronach.

Wykorzystywanie znaku graficznego Europejskiego Trybunału Obrachunkowego

Znak graficzny Europejskiego Trybunału Obrachunkowego nie może być wykorzystywany bez uprzedniej zgody Trybunału.

HTML	ISBN 978-92-849-7885-4	ISSN 1977-5768	doi:10.2865/1372942	QJ-01-26-032-PL-Q
PDF	ISBN 978-92-849-7886-1	ISSN 1977-5768	doi:10.2865/1418163	QJ-01-26-032-PL-N

CYTOWANIE

Europejski Trybunał Obrachunkowy, [sprawozdanie specjalne 19/2026](#) pt. „Wykrywanie cyberincydentów i reagowanie na nie – budowa unijnych ram współpracy postępuje, ale są one tylko częściowo skuteczne ze względu na opóźnienia we wdrażaniu i niewielką wymianę informacji”, Urząd Publikacji Unii Europejskiej, 2026.

W ostatnich latach UE udoskonaliła ramy regulacyjne w zakresie cyberbezpieczeństwa oraz ustanowiła odpowiednie sieci i mechanizmy służące radzeniu sobie z cyberincydentami. Ponadto Unia finansuje projekty dotyczące cyberbezpieczeństwa w ramach programu „Cyfrowa Europa”.

Trybunał stwierdził, że działania UE jedynie częściowo ułatwiają wykrywanie poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, a także reagowanie na nie. Choć budowanie ram współpracy stopniowo postępuje, to prace nad stworzeniem pełnej struktury cyberbezpieczeństwa nie są jeszcze zakończone. Niewielki zakres wymiany informacji, uchybienia w zakresie sprawozdawczości i znaczne opóźnienia we wdrażaniu uniemożliwiają pełne wykorzystanie potencjału unijnych sieci i mechanizmów. Finansowane projekty służą realizacji zamierzonych celów, ale w przypadku szeregu z nich Trybunał odnotował problemy operacyjne i opóźnienia. Ponadto kontrolerzy wykryli uchybienia w ogólnych ramach monitorowania wyników. Trybunał sformułował zalecenia służące wyeliminowaniu tych niedociągnięć.

Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego przedstawiono na podstawie art. 287 ust. 4 akapit drugi TFUE.



EUROPEJSKI
TRYBUNAŁ
OBRACHUNKOWY



Urząd Publikacji
Unii Europejskiej

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
12, rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Formularz kontaktowy: eca.europa.eu/pl/contact
Strona internetowa: eca.europa.eu
Media społecznościowe: @EUauditors