KOMISJA
EUROPEJSKA

Bruksela, dnia 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji

Wkład Komisji Europejskiej w spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r.

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Ponieważ życie codzienne i gospodarki stają się coraz bardziej zależne od technologii cyfrowych, obywatele są w coraz większym stopniu narażeni na poważne cyberincydenty. Przyszłe bezpieczeństwo zależy od poprawy zdolności do ochrony Unii przed zagrożeniami dla cyberbezpieczeństwa, gdyż zarówno infrastruktura cywilna, jak i potencjał wojskowy opierają się na bezpiecznych systemach cyfrowych.

W celu sprostania rosnącym wyzwaniom Unia stale intensyfikuje swoją działalność w tym obszarze, opierając się na strategii bezpieczeństwa cybernetycznego z 2013 r.[1] oraz jej celach i zasadach służących promowaniu niezawodnego, bezpiecznego i otwartego ekosystemu cyberbezpieczeństwa. W 2016 r. Unia przyjęła pierwsze środki w dziedzinie cyberbezpieczeństwa w postaci dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[2] w sprawie bezpieczeństwa sieci i systemów informatycznych.

Wobec szybko rozwijającego się otoczenia bezpieczeństwa cyberprzestrzeni we wrześniu 2017 r. Komisja i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili wspólny komunikat[3] „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", aby w dalszym ciągu wzmacniać odporność, prewencję i reakcję Unii w kwestii cyberataków. We wspólnym komunikacie, opartym również o poprzednie inicjatywy, określono zestaw proponowanych działań, obejmujących między innymi wzmocnienie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), stworzenie dobrowolnych, ogólnounijnych ram certyfikacji cyberbezpieczeństwa mających na celu zwiększenie cyberbezpieczeństwa produktów i usług w cyfrowym świecie, jak również planu działania dotyczącego szybkiej, skoordynowanej reakcji na incydenty cybernetyczne i kryzysy cybernetyczne na dużą skalę.

We wspólnym komunikacie stwierdzono, że także w strategicznym interesie UE leży zapewnienie, aby Unia utrzymała i rozwijała podstawowe zdolności technologiczne w zakresie cyberbezpieczeństwa w celu ochrony swojego jednolitego rynku cyfrowego, a w szczególności ochrony sieci i systemów informatycznych o znaczeniu krytycznym, oraz dostarczania kluczowych usług w zakresie cyberbezpieczeństwa. Unia musi mieć możliwość zabezpieczenia swoich zasobów cyfrowych w sposób autonomiczny i konkurowania na światowym rynku cyberbezpieczeństwa.

Obecnie Unia jest importerem netto produktów i rozwiązań z w dziedzinie cyberbezpieczeństwa i w dużej mierze jest uzależniona od dostawców pozaeuropejskich[4]. Wartość globalnego rynku cyberbezpieczeństwa sięga 600 mld EUR i oczekuje się jej

---

1 WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", JOIN(2013) 1 final.

2 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

3 WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO I RADY: Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej, JOIN(2017) 450 final.

4 Projekt sprawozdania końcowego w sprawie badania rynku cyberbezpieczeństwa, 2018 r.

wzrostu w ciągu kolejnych pięciu lat średnio o 17 % pod względem sprzedaży, liczby przedsiębiorstw i zatrudnienia. Jednak w pierwszej dwudziestce państw wiodących na rynku cyberbezpieczeństwa znajduje się jedynie 6 państw członkowskich[5].

Jednocześnie w Unii istnieje bardzo wysoki poziom wiedzy eksperckiej i doświadczenia w dziedzinie cyberbezpieczeństwa – ponad 660 organizacji na terytorium całej UE zarejestrowano w trakcie prowadzonego ostatnio przez Komisję mapowania ośrodków wiedzy eksperckiej z zakresu cyberbezpieczeństwa[6]. Jeżeli tę wiedzę ekspercką przełożono by na produkty i rozwiązania przeznaczone do obrotu, Unia mogłaby uczestniczyć w całym łańcuchu wartości w dziedzinie cyberbezpieczeństwa. Jednakże wysiłki środowisk naukowych i przemysłowych są rozproszone, brakuje zbieżności działań i wspólnej misji, co stanowi przeszkodę dla konkurencyjności UE w tym obszarze, jak również dla możliwości zabezpieczenia przez Unię swoich zasobów cyfrowych. Istotne sektory cyberbezpieczeństwa (np. energetyczny, przestrzeni kosmicznej, obrony, transportu) oraz podobszary są obecnie niedostatecznie wspierane[7]. W Europie nie wykorzystuje się również w pełni synergii między sektorami cyberbezpieczeństwa cywilnego i obronnego.

Stworzenie w 2016 r. partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w Unii było znaczącym pierwszym krokiem łączącym środowiska sektora badań, przemysłu i sektora publicznego, aby ułatwić prowadzenie badań i wprowadzanie innowacji w dziedzinie cyberbezpieczeństwa, co w ramach finansowych na lata 2014–2020 powinno przynieść dobre, bardziej konkretne efekty w zakresie badań i innowacji. Umożliwiło to partnerom przemysłowym podjęcie zobowiązania dotyczącego ich indywidualnych wydatków w dziedzinach określonych w strategicznym planie badań i innowacji w ramach tego partnerstwa.

Jednakże Unia może podejmować inwestycje na dużo większą skalę i potrzebuje efektywniejszego mechanizmu, dzięki któremu można byłoby zbudować trwałe zdolności, łączyć wysiłki i kompetencje oraz stymulować rozwój innowacyjnych rozwiązań w odpowiedzi na wyzwania związane z cyberbezpieczeństwem w sektorze przemysłu w zakresie nowych technologii służących wielorakim celom (np. sztucznej inteligencji, informatyki kwantowej, łańcucha bloków i bezpiecznych tożsamości cyfrowych), jak również w sektorach o kluczowym znaczeniu (np. transportu, energetycznym, zdrowia, finansowym, administracji, telekomunikacji, produkcyjnym, obrony, przestrzeni kosmicznej).

We wspólnym komunikacie rozważono możliwość wzmocnienia zdolności Unii w zakresie cyberbezpieczeństwa za pomocą sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa na czele. Miałoby to na celu uzupełnienie istniejących wysiłków na rzecz budowania zdolności w tym obszarze na szczeblu unijnym i krajowym. We wspólnym komunikacie stwierdzono, że Komisja ma zamiar rozpocząć ocenę skutków w 2018 r., aby zbadać dostępne warianty w celu określenia struktury. Pierwszym krokiem i podstawą przyszłych rozważań była zainicjowana przez Komisję faza pilotażowa w ramach programu „Horyzont 2020”, mająca pomóc w tworzeniu sieci ośrodków krajowych; nadałoby to nowy impet rozwijaniu kompetencji i technologii w dziedzinie cyberbezpieczeństwa.

---

5 Projekt sprawozdania końcowego w sprawie badania rynku cyberbezpieczeństwa, 2018 r.

6 Sprawozdania techniczne JRC: Europejskie ośrodki wiedzy eksperckiej z zakresu cyberbezpieczeństwa, 2018 r.

7 Sprawozdanie techniczne JRC: Wyniki mapowania (szczegóły znaleźć można w załącznikach 4 i 5).

Podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. szefowie państw i rządów wezwali Unię, aby stała się „do 2025 r. światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia zaufania, pewności i ochrony naszym obywatelom, konsumentom i przedsiębiorstwom online oraz umożliwienia istnienia wolnego i podlegającego przepisom prawa internetu".

W swoich konkluzjach[8] przyjętych w listopadzie 2017 r. Rada wezwała Komisję do szybkiego dostarczenia oceny skutków dotyczącej możliwych wariantów i do zaproponowania w pierwszym półroczu 2018 r. odpowiedniego instrumentu prawnego w celu wdrożenia przedmiotowej inicjatywy.

Zaproponowany przez Komisję w czerwcu 2018 r. program „Cyfrowa Europa"[9] ma na celu zwiększenie i zmaksymalizowanie korzyści z transformacji cyfrowej dla obywateli i przedsiębiorstw Unii we wszystkich istotnych obszarach polityki UE dzięki wzmocnieniu polityk i wspieraniu ambicji związanych z jednolitym rynkiem cyfrowym. W ramach programu zaproponowano spójne i całościowe podejście do kwestii zapewnienia najlepszego wykorzystywania zaawansowanych technologii oraz właściwego połączenia zdolności i ludzkich kompetencji do celów transformacji cyfrowej – nie tylko w obszarze cyberbezpieczeństwa, lecz również w odniesieniu do inteligentnej infrastruktury danych, sztucznej inteligencji, zaawansowanych umiejętności i zastosowań w przemyśle i w dziedzinach leżących w interesie publicznym. Elementy te są współzależne, nawzajem się wzmacniające i dzięki ich jednoczesnemu promowaniu można osiągnąć skalę niezbędną, aby umożliwić rozwój gospodarki opartej na danych[10]. Do priorytetów *programu „Horyzont Europa"*[11] – kolejnego unijnego programu ramowego na rzecz badań i innowacji – należy również cyberbezpieczeństwo.

W tym kontekście w niniejszym rozporządzeniu proponuje się utworzenie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji. Ten specjalnie zaprojektowany model współpracy powinien działać w opisany poniżej sposób, aby stymulować europejski ekosystem technologiczny i przemysłowy w dziedzinie cyberbezpieczeństwa: Centrum Kompetencji będzie ułatwiać i wspierać koordynację prac sieci oraz pielęgnować środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa, stymulując realizację technologicznego planu w dziedzinie cyberbezpieczeństwa i ułatwiając dostęp do zgromadzonej w ten sposób wiedzy fachowej. Centrum Kompetencji miałoby w szczególności wdrażać odpowiednie części programów „Cyfrowa Europa" i „Horyzont Europa" poprzez przydzielanie dotacji i udzielanie zamówień. W świetle znacznych inwestycji w cyberbezpieczeństwo poczynionych w innych częściach świata, a także potrzeby koordynacji i łączenia odpowiednich zasobów w Europie, proponuje się, aby Centrum Kompetencji miało formę partnerstwa europejskiego[12], ułatwiając tym

---

8 Konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", przyjęte przez Radę do Spraw Ogólnych w dniu 20 listopada 2017 r.

9 COM(2018) 434, Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" na lata 2021–2027.

10 Zob. SWD(2018) 305.

11 COM(2018) 435, Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa" oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie.

12 Jak określono w COM(2018) 435 – Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa"

samym dokonywanie wspólnych inwestycji przez Unię, państwa członkowskie lub przemysł. W związku z tym we wniosku zobowiązuje się państwa członkowskie do wnoszenia wkładu w kwocie współmiernej do działań Centrum Kompetencji i sieci. Głównym organem decyzyjnym jest Rada Zarządzająca, w której pracach biorą udział wszystkie państwa członkowskie, lecz prawa głosu przysługują jedynie tym państwom członkowskim, które wnoszą wkład finansowy. Mechanizm głosowania w Radzie Zarządzającej uwzględnia zasadę „podwójnej większości", zgodnie z którą niezbędne jest uzyskanie poparcia reprezentacji 75 % wkładu finansowego oraz 75 % głosów. Ze względu na swoją odpowiedzialność w kwestii budżetu unijnego Komisja posiada 50 % głosów. Jeśli chodzi o udział w pracach Rady Zarządzającej, Komisja będzie korzystać, w razie potrzeby, z wiedzy fachowej Europejskiej Służby Działań Zewnętrznych. Rada Zarządzająca jest wspomagana przez Radę Konsultacyjną ds. Przemysłowych i Naukowych w celu zapewnienia regularnego dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami.

Ściśle współpracując z siecią krajowych ośrodków koordynacji i środowiskiem posiadającym kompetencje w dziedzinie cyberbezpieczeństwa (w tym dużą i zróżnicowaną grupą podmiotów zaangażowanych w rozwój technologii w dziedzinie cyberbezpieczeństwa, taką jak podmioty prowadzące badania, branże po stronie podaży, branże po stronie popytu i sektor publiczny), które powołuje się niniejszym rozporządzeniem, Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie głównym organem ds. wdrażania zajmującym się zasobami finansowymi UE przeznaczonymi na cyberbezpieczeństwo na podstawie zaproponowanego *programu „Cyfrowa Europa"* oraz *programu „Horyzont Europa"*.

Takie kompleksowe podejście pozwoliłoby na wsparcie cyberbezpieczeństwa w ramach całego łańcucha wartości, od badań po wspieranie wdrażania i absorpcji kluczowych technologii. Finansowy udział państw członkowskich powinien być współmierny do finansowego wkładu UE na rzecz tej inicjatywy i stanowi nieodłączny element pozwalający osiągnąć sukces.

Biorąc pod uwagę szczególną wiedzę ekspercką jej członków oraz szeroką i znaczącą reprezentację zainteresowanych stron, Europejska Organizacja ds. Cyberbezpieczeństwa, która stanowi odpowiednik umownego partnerstwa publiczno-prywatnego Komisji w dziedzinie cyberbezpieczeństwa w ramach programu „Horyzont 2020", powinna zostać zaproszona do wniesienia swojego wkładu w prace Centrum i sieci.

Ponadto Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych również powinno dążyć do wzmocnienia synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa. Centrum powinno wspierać państwa członkowskie i inne istotne podmioty, zapewniając doradztwo, dzieląc się wiedzą ekspercką i ułatwiając współpracę w odniesieniu do projektów i działań. Na wniosek państw członkowskich powinno także działać jako kierownik projektu, w szczególności w związku z Europejskim Funduszem Obronnym. Celem obecnej inicjatywy jest przyczynienie się do rozwiązania niżej wskazanych problemów:

---

oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie, a także jak wskazano w COM(2018) 434 – Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" na lata 2021–2027.

- **Niewystarczająca współpraca między branżami po stronie popytu i podaży w dziedzinie cyberbezpieczeństwa.** Europejskie przedsiębiorstwa stoją przed wyzwaniem pozostania bezpiecznymi oraz oferowania bezpiecznych produktów i usług klientom. Często jednak nie są w stanie odpowiednio zabezpieczyć swoich istniejących produktów, usług i aktywów lub zaprojektować bezpiecznych, innowacyjnych produktów i usług. Kluczowe aktywa w dziedzinie cyberbezpieczeństwa są zwykle zbyt kosztowne, aby opracowywały je i wprowadzały indywidualne podmioty, których główna działalność gospodarcza nie jest związana z cyberbezpieczeństwem. Jednocześnie związki między stroną popytu i podaży na rynku cyberbezpieczeństwa nie są wystarczająco dobrze rozwinięte, przez co poziom podaży europejskich produktów i rozwiązań dostosowanych do potrzeb różnych sektorów nie jest optymalny, a także niewystarczający jest poziom zaufania wśród uczestników rynku.
- **Brak skutecznego mechanizmu współpracy służącego budowaniu potencjału przemysłowego w państwach członkowskich** Obecnie nie istnieje także skuteczny mechanizm współpracy służący państwom członkowskim do wspólnego budowania niezbędnych zdolności wspierających innowacje w dziedzinie cyberbezpieczeństwa we wszystkich sektorach przemysłu i wdrażania najnowocześniejszych rozwiązań w zakresie unijnego cyberbezpieczeństwa. W ramach istniejących mechanizmów współpracy państw członkowskich w obszarze cyberbezpieczeństwa wynikających z dyrektywy (UE) 2016/1148 nie przewidziano tego rodzaju działań w mandatach udzielanych na ich podstawie.
- **Niewystarczająca współpraca w ramach środowisk naukowych i przemysłowych oraz między tymi środowiskami.** Pomimo teoretycznej zdolności Unii do objęcia całego łańcucha wartości dotyczącego cyberbezpieczeństwa istnieją istotne sektory cyberbezpieczeństwa (np. energetyczny, przestrzeni kosmicznej, obrony, transportu) oraz podobszary, które są obecnie słabo wspierane przez społeczności badawcze lub wspierane tylko w przypadku ograniczonej liczby ośrodków (np. kryptografia kwantowa i postkwantowa, zaufanie i cyberbezpieczeństwo w odniesieniu do sztucznej inteligencji). Chociaż współpraca taka oczywiście ma miejsce, jest ona bardzo często krótkofalowa i ma formę konsultacji, co nie pozwala na włączenie się w realizację długoterminowych planów badań mających na celu znalezienie rozwiązań w odpowiedzi na wyzwania związane z cyberbezpieczeństwem w sektorze przemysłu.
- **Niewystarczająca współpraca między środowiskami zajmującymi się badaniami i innowacjami w dziedzinie cyberbezpieczeństwa cywilnego i obronnego.** Problem niewystarczających poziomów współpracy dotyczy również środowisk cywilnych i zajmujących się obroną. Istniejących synergii nie wykorzystuje się w pełni ze względu na brak skutecznych mechanizmów pozwalających tym środowiskom na skuteczną współpracę i budowanie zaufania, które w jeszcze większym nawet stopniu niż w innych obszarach jest warunkiem wstępnym pomyślnej współpracy. Jest to powiązane z ograniczonymi możliwościami finansowymi unijnego rynku cyberbezpieczeństwa, w tym niewystarczającymi funduszami na wspieranie innowacji.
- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki.**

Sieć kompetencji w dziedzinie cyberbezpieczeństwa oraz Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będą zapewniały dodatkowe wsparcie na rzecz istniejących przepisów obowiązujących w obszarze polityki cyberbezpieczeństwa i podmiotów w tym obszarze. Mandat Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie miał charakter komplementarny

względem wysiłków Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), ale w jego przypadku nacisk położony będzie na inne kwestie i wymagany będzie inny zestaw umiejętności. Chociaż w ramach mandatu Agencji przewidziano rolę polegającą na doradztwie w zakresie badań i innowacji w dziedzinie cyberbezpieczeństwa w UE, proponowany mandat dotyczy przede wszystkim innych zadań, które mają decydujące znaczenie dla wzmacniania odporności w zakresie cyberbezpieczeństwa w UE. Ponadto w ramach mandatu ENISA nie przewidziano rodzajów działalności, które będą stanowić główne zadania Centrum i sieci: chodzi o pobudzanie rozwoju technologii w dziedzinie bezpieczeństwa cyberprzestrzeni i wdrażanie tej technologii oraz uzupełnianie wysiłków na rzecz budowania zdolności w tym obszarze na szczeblu unijnym i krajowym.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych (razem z siecią kompetencji w dziedzinie cyberbezpieczeństwa) będzie również działało na rzecz wspierania badań, aby ułatwić i przyspieszyć procesy standaryzacji i certyfikacji, w szczególności związane z systemami certyfikacji cyberbezpieczeństwa w znaczeniu określonym w zaproponowanym akcie w sprawie cyberbezpieczeństwa[13] [14].

Obecna inicjatywa oznacza faktycznie zwiększenie skali partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa, które stanowiło pierwszą, obejmującą całą UE próbę skupienia sektora cyberbezpieczeństwa, strony popytu (nabywców produktów i rozwiązań w dziedzinie cyberbezpieczeństwa, w tym administracji publicznej i sektorów krytycznych, takich jak np. sektory transportu, zdrowia, energetyczny, finansowy) oraz społeczności badawczej w celu zbudowania platformy zrównoważonego dialogu i stworzenia warunków do dobrowolnego przeprowadzania wspólnych inwestycji. Partnerstwo publiczno-prywatne w dziedzinie cyberbezpieczeństwa zostało utworzone w 2016 r. i przyczyniło się do zainwestowania prawie 1,8 mld EUR do 2020 r. Jednak skala inwestycji w innych częściach świata (np. w Stanach Zjednoczonych w cyberbezpieczeństwo zainwestowano 19 mld USD w samym tylko 2017 r.) pokazuje, że potrzeba większego nakładu pracy ze strony UE, aby osiągnąć masę krytyczną inwestycji i przezwyciężyć fragmentaryzację zdolności rozproszonych po całej Unii.

- **Spójność z innymi politykami Unii**

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie działać jako pojedynczy organ wdrażający różne programy unijne wpierające cyberbezpieczeństwo (programy „Cyfrowa Europa" i „Horyzont Europa") i przyczyniać się do zwiększenia spójności i synergii między tymi programami.

---

[13] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt w sprawie cyberbezpieczeństwa", COM(2017) 477 final/3).

[14] Pozostaje to bez uszczerbku dla mechanizmów certyfikacji wynikających z ogólnego rozporządzenia o ochronie danych, w ramach których organy ds. ochrony danych mają do odegrania określoną rolę, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Inicjatywa ta pozwoli także na uzupełnianie wysiłków państw członkowskich dzięki zapewnianiu odpowiednich informacji decydentom w obszarze edukacji w celu zwiększenia umiejętności z zakresu cyberbezpieczeństwa (np. dzięki opracowaniu programów z zakresu cyberbezpieczeństwa w ramach cywilnych i wojskowych systemów edukacji), aby ułatwić stworzenie wykwalifikowanej siły roboczej UE w zakresie cyberbezpieczeństwa, stanowiącej kluczowy zasób dla przedsiębiorstw z obszaru cyberbezpieczeństwa, jak również innych branż zainteresowanych cyberbezpieczeństwem. Jeśli chodzi o kształcenie i szkolenie w dziedzinie cyberobrony, przedmiotowa inicjatywa będzie spójna z trwającymi pracami platformy ds. kształcenia, szkolenia i ćwiczeń w zakresie cyberobrony ustanowionej w ramach Europejskiego Kolegium Bezpieczeństwa i Obrony.

Inicjatywa ta będzie stanowiła uzupełnienie i wsparcie wysiłków centrów innowacji cyfrowych w ramach programu „Cyfrowa Europa". Centra innowacji cyfrowych są organizacjami non-profit pomagającymi przedsiębiorstwom – w szczególności przedsiębiorstwom typu start-up, MSP oraz spółkom o średniej kapitalizacji – w zdobyciu przewagi konkurencyjnej dzięki ulepszeniu ich procesów biznesowych/produkcji, jak również produktów i usług za pomocą inteligentnych innowacji, które możliwe są dzięki technologii cyfrowej. Centra innowacji cyfrowych oferują usługi w zakresie innowacji ukierunkowane na działalność gospodarczą, takie jak badania rynkowe, doradztwo dotyczące finansowania, dostęp do odpowiedniej infrastruktury na potrzeby badań i eksperymentów, szkolenia i rozwój umiejętności, aby pomóc skutecznie wprowadzić nowe produkty i usługi na rynek lub wdrożyć lepsze procesy produkcji. Niektóre centra informacji cyfrowych posiadające szczególną wiedzę fachową z zakresu cyberbezpieczeństwa mogłyby bezpośrednio dołączyć do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa ustanowionego niniejszą inicjatywą. W większości przypadków centra informacji cyfrowych, które nie mają określonego profilu cyberbezpieczeństwa, ułatwiłyby jednak swoim członkom dostęp do wiedzy fachowej, wiedzy i zdolności z zakresu cyberbezpieczeństwa dostępnych w ramach środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa dzięki ścisłej współpracy z siecią krajowych ośrodków koordynacji oraz Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych. Centra informacji cyfrowych wsparłyby również rozwój innowacyjnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa odpowiadających potrzebom przedsiębiorstw oraz pozostałych użytkowników końcowych, którym służą. Nie mniej istotny jest fakt, że sektorowe centra informacji cyfrowych mogłyby dzielić się swoją wiedzą z zakresu rzeczywistych potrzeb sektorowych z siecią i Centrum, aby wnieść swój udział w przemyślenia na temat planu badań naukowych i innowacji odpowiadającego na wymogi przemysłu.

Poszukiwane będą synergie z właściwymi wspólnotami wiedzy i innowacji Europejskiego Instytutu Innowacji i Technologii, a w szczególności z EIT Digital.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Ze względu na jego charakter i szczególne cele Centrum Kompetencji należy ustanowić z zastosowaniem podwójnej podstawy prawnej. Art. 187 TFUE, określający struktury niezbędne do skutecznego wykonywania unijnych programów badawczych, rozwoju technologicznego i demonstracyjnych, umożliwia Centrum Kompetencji tworzenie synergii i gromadzenie zasobów, aby inwestować w niezbędne zdolności na poziomie państw członkowskich i rozwijać wspólne aktywa europejskie (np. dzięki wspólnemu pozyskiwaniu niezbędnej infrastruktury do prowadzenia badań i eksperymentów w dziedzinie

cyberbezpieczeństwa). W art. 188 akapit pierwszy przewiduje się przyjęcie takich środków. Sam art. 188 akapit pierwszy stanowiłby niemniej jednak podstawę prawną, na mocy której działania nie mogłyby wykroczyć poza sferę badań naukowych i rozwoju, co jest konieczne, aby zrealizować cele Centrum Kompetencji określone w niniejszym rozporządzeniu wspierającym wprowadzenie na rynek produktów i rozwiązań w dziedzinie cyberbezpieczeństwa pomagających europejskiej branży cyberbezpieczeństwa w zdobyciu przewagi konkurencyjnej oraz wnoszącym wartość dodatkową do wysiłków krajowych polegających na eliminowaniu niedoboru kwalifikacji w zakresie cyberbezpieczeństwa. W związku z tym, aby zrealizować te cele, niezbędne jest dodanie art. 173 ust. 3 jako podstawy prawnej, która pozwoli Unii zapewnić środki mające na celu wsparcie konkurencyjności przemysłu.

- **Uzasadnienie wniosku pod względem zasad pomocniczości i proporcjonalności**

Cyberbezpieczeństwo jest przedmiotem wspólnego zainteresowania Unii, co potwierdzono we wspomnianych powyżej konkluzjach Rady. Przykładami są skala i transgraniczny charakter incydentów, takich jak ataki za pomocą oprogramowania *WannaCry* czy *NonPetya*. Charakter i skala wyzwań technologicznych dotyczących cyberbezpieczeństwa, jak również niewystarczająca koordynacja wysiłków w ramach przemysłu, sektora publicznego i środowisk naukowych oraz pomiędzy nimi wymaga, aby UE w dalszym ciągu wpierała wysiłki koordynacyjne zarówno w celu zgromadzenia krytycznej masy zasobów, jak i zapewnienia lepszego zarządzania wiedzą i aktywami. Jest to konieczne z uwagi na wymogi w zakresie zasobów powiązane z określonymi możliwościami dotyczącymi badań naukowych, rozwoju i wdrażania cyberbezpieczeństwa; konieczność zapewnienia dostępu do interdyscyplinarnej wiedzy eksperckiej z dziedziny cyberbezpieczeństwa między różnymi dyscyplinami (często jedynie częściowo dostępnej na poziomie krajowym); globalny charakter przemysłowych łańcuchów wartości oraz światowych konkurentów działających na wielu rynkach.

Wymaga to zasobów i wiedzy fachowej w skali, którą trudno osiągnąć w wyniku indywidualnego działania któregokolwiek państwa członkowskiego. Na przykład ogólnoeuropejska komunikacyjna sieć kwantowa może wymagać ze strony UE inwestycji w wysokości około 900 mln EUR, w zależności od inwestycji państw członkowskich (które mają zostać wzajemnie połączone/uzupełnione) oraz stopnia, w jakim technologia umożliwi ponowne wykorzystanie istniejącej infrastruktury. Inicjatywa ta odegra zasadniczą rolę w łączeniu środków finansowych i umożliwieniu realizacji tego rodzaju inwestycji w Unii.

Państwa członkowskie nie mogą same w pełni zrealizować celów niniejszej inicjatywy. Jak wykazano powyżej, mogą one być lepiej realizowane na szczeblu unijnym dzięki połączeniu wysiłków i unikaniu ich niepotrzebnego powielania, pomocy w osiągnięciu krytycznej masy inwestycji oraz zapewnieniu optymalnego wykorzystania finansowania publicznego. Jednocześnie zgodnie z zasadą proporcjonalności niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do realizacji tego celu. Działanie UE ma zatem uzasadnienie na gruncie zasad pomocniczości i proporcjonalności.

Niniejszy instrument nie przewiduje żadnych nowych obowiązków regulacyjnych w odniesieniu do przedsiębiorstw. Jednocześnie przedsiębiorstwa, a zwłaszcza MŚP, prawdopodobnie ograniczą koszty związane z ich wysiłkami zmierzającymi do opracowywania innowacyjnych produktów z zakresu cyberbezpieczeństwa, ponieważ inicjatywa umożliwia gromadzenie zasobów, aby inwestować w niezbędne zdolności na szczeblu państw członkowskich lub rozwijać wspólne aktywa europejskie (np. dzięki wspólnemu zamawianiu niezbędnej infrastruktury do prowadzenia badań i eksperymentów

w dziedzinie cyberbezpieczeństwa). Aktywa te mogą zostać wykorzystane przez branże i MŚP w celu zapewnienia bezpieczeństwa ich produktów pod względem cybernetycznym i uczynienia z cyberbezpieczeństwa ich przewagi konkurencyjnej.

- **Wybór instrumentu**

Proponowany instrument ustanawia organ odpowiedzialny za wdrażanie działań dotyczących cyberbezpieczeństwa w ramach programu „Cyfrowa Europa" oraz programu „Horyzont Europa". Instrument określa mandat, zadania, jak również strukturę zarządzania. Ustanowienie takiego unijnego organu wymaga przyjęcia rozporządzenia.

3. KONSULTACJE Z ZAINTERESOWANYMI STRONAMI I OCENY SKUTKÓW

Wniosek w sprawie utworzenia sieci kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych jest nową inicjatywą. Jest to kontynuacja i poszerzenie umownego partnerstwa publiczno-prywatnego na rzecz cyberbezpieczeństwa utworzonego w 2016 r.

- **Konsultacje z zainteresowanymi stronami**

Cyberbezpieczeństwo to obszerny, międzysektorowy temat. Komisja wykorzystała różne metody konsultacji, aby zamiast określonych interesów wąskiego grona grup zainteresowanych stron zapewnić odpowiednie odzwierciedlenie ogólnego publicznego interesu unijnego w niniejszej inicjatywie. Metoda ta zapewnia przejrzystość i odpowiedzialność w ramach prac prowadzonych przez Komisję. Chociaż nie przeprowadzono otwartych konsultacji publicznych konkretnie na potrzeby niniejszej inicjatywy, biorąc po uwagę jej docelowych odbiorców (społeczność branżową i badawczą oraz państwa członkowskie), to temat był już przedmiotem szeregu innych otwartych konsultacji publicznych:

- ogólnych otwartych konsultacji publicznych przeprowadzonych w 2018 r. w sprawie inwestycji, badań i innowacji, MŚP i jednolitego rynku;
- 12-tygodniowych internetowych konsultacji publicznych rozpoczętych w 2017 r. w celu zapoznania się z opiniami szerszego grona (w przybliżeniu 90 respondentów) na temat oceny i przeglądu dotyczącego ENISA;
- 12-tygodniowych internetowych konsultacji publicznych, które przeprowadzono w 2016 r. przy okazji inauguracji umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa (w przybliżeniu 240 respondentów).

Komisja zorganizowała również ukierunkowane konsultacje w sprawie niniejszej inicjatywy, w tym warsztaty, spotkania i ukierunkowane wnioski dotyczące udzielenia informacji (przez ENISA i Europejską Agencję Obrony). Konsultacje trwały 6 miesięcy, od listopada 2017 r. do marca 2018 r. Komisja przeprowadziła również mapowanie ośrodków wiedzy fachowej, które umożliwiło zgromadzenie informacji z 665 ośrodków wiedzy fachowej z zakresu cyberbezpieczeństwa na temat ich wiedzy eksperckiej, działalności, dziedzin roboczych, współpracy międzynarodowej. Badanie rozpoczęto w styczniu, a na potrzeby analizy sprawozdania uwzględniono ankiety złożone do 8 marca 2018 r.

Zainteresowane strony należące do środowisk branżowych i naukowych stwierdziły, że Centrum Kompetencji i sieć mogą zapewnić wartość dodaną względem obecnych wysiłków na poziomie krajowym poprzez pomoc w utworzeniu ogólnoeuropejskiego ekosystemu

cyberbezpieczeństwa, umożliwiającego lepszą współpracę między społecznościami badawczymi i branżowymi. Uznały również za niezbędne, aby UE i państwa członkowskie przyjęły aktywną, długoterminową i strategiczną perspektywę w stosunku do polityki przemysłowej dotyczącej cyberbezpieczeństwa, wykraczającą poza same badania naukowe i innowacje. Zainteresowane strony wyraziły konieczność uzyskania dostępu do kluczowych zdolności, takich jak infrastruktura na potrzeby badań i eksperymentów, oraz wykazania większych ambicji w eliminowaniu niedoboru kwalifikacji w zakresie cyberbezpieczeństwa, np. za pośrednictwem dużych europejskich projektów przyciągających osoby najbardziej utalentowane. Wszystkie powyższe kwestie uznano również za niezbędne do tego, aby Unię uznano na całym świecie za lidera w dziedzinie cyberbezpieczeństwa.

W ramach działań konsultacyjnych podjętych od września ubiegłego roku[15], jak również w specjalnych konkluzjach Rady[16], państwa członkowskie z zadowoleniem przyjęły zamiar ustanowienia sieci kompetencji w dziedzinie cyberbezpieczeństwa w celu pobudzenia rozwoju i wdrażania technologii z zakresu cyberbezpieczeństwa, podkreślając konieczność sprzyjania włączeniu wszystkich państw członkowskich oraz ich istniejących centrów doskonałości i kompetencji oraz poświęcania szczególnej uwagi kwestii komplementarności. Jeśli chodzi o przyszłe Centrum Kompetencji, państwa członkowskie podkreśliły zwłaszcza znaczenie jego roli koordynacyjnej we wsparciu sieci. W szczególności w odniesieniu do krajowych działań i potrzeb w dziedzinie cyberobrony proces mapowania potrzeb państw członkowskich w zakresie cyberobrony, przeprowadzony przez Europejską Służbę Działań Zewnętrznych w marcu 2018 r., pokazał, że większość państw członkowskich dostrzega unijną wartość dodaną w obszarze szkolenia i edukacji oraz we wsparciu przemysłu poprzez badania naukowe i rozwój[17]. Inicjatywa zostałaby w rzeczywistości wdrożona wspólnie z państwami członkowskimi lub wspieranymi przez nie podmiotami. Współpraca między środowiskami branżowymi, naukowymi lub środowiskami sektora publicznego połączyłaby i wzmocniła istniejące podmioty oraz obecne wysiłki w celu uniknięcia powielania działań. Państwa członkowskie uczestniczyłyby również w określaniu konkretnych działań ukierunkowanych na sektor publiczny jako bezpośredniego użytkownika technologii i wiedzy eksperckiej z zakresu cyberbezpieczeństwa.

- **Ocena skutków**

Ocena skutków wspierająca niniejszą inicjatywę została przedłożona Radzie ds. Kontroli Regulacyjnej w dniu 11 kwietnia 2017 r. i otrzymała pozytywną opinię z zastrzeżeniami. Następnie ocenę skutków poddano przeglądowi w świetle uwag Rady. Opinia Rady oraz załącznik wyjaśniający sposób uwzględniania uwag Rady zostają opublikowane wraz z niniejszym wnioskiem.

W ocenie skutków rozważono szereg wariantów strategicznych, zarówno legislacyjnych, jak i nielegislacyjnych. Do szczegółowej oceny wybrano następujące warianty:

- Scenariusz odniesienia – wariant współpracy – zakłada kontynuację obecnego podejścia do budowania przemysłowych i technologicznych zdolności w dziedzinie cyberbezpieczeństwa w UE dzięki wspieraniu badań naukowych i innowacji oraz powiązanych mechanizmów współpracy w ramach 9PR.

[15] Np. posiedzenie okrągłego stołu wysokiego szczebla z udziałem państw członkowskich, wiceprzewodniczącego Ansip, komisarz Gabriel, 5 grudnia 2017 r.

[16] Rada do Spraw Ogólnych: Konkluzje Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego UE (20 listopada 2017 r.)

[17] ESDZ, marzec 2018 r.

- Wariant 1: sieć kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych z podwójnym mandatem do prowadzenia działań wspierających technologie przemysłowe, jak również działań w obszarze badań naukowych i innowacji.
- Wariant 2: sieć kompetencji w dziedzinie cyberbezpieczeństwa z Europejskim Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa skoncentrowanym na działaniach z zakresu badań naukowych i innowacji.

Warianty odrzucone na wczesnym etapie obejmowały: 1) wariant niepodejmowania żadnych działań, 2) wariant utworzenia jedynie sieci kompetencji w dziedzinie cyberbezpieczeństwa, 3) wariant utworzenia wyłącznie scentralizowanej struktury, jak również 4) wariant wykorzystania istniejącej agencji (Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji – (ENISA), Agencji Wykonawczej ds. Badań Naukowych (REA) lub Agencji Wykonawczej ds. Innowacyjności i Sieci (INEA).

W ramach analizy stwierdzono, że wariant 1 stanowi najlepsze rozwiązanie na potrzeby realizacji celów inicjatywy, jednocześnie zapewniając największy wpływ gospodarczy, społeczny i środowiskowy oraz zabezpieczając interesy Unii. Główne argumenty przemawiające za tym wariantem obejmowały zdolność stworzenia rzeczywistej polityki przemysłowej dotyczącej cyberbezpieczeństwa dzięki wspieraniu działań związanych nie tylko z badaniami naukowymi i rozwojem, ale również z wprowadzeniem na rynek; elastyczność umożliwiającą optymalizację wykorzystywania istniejącej wiedzy i zasobów w ramach różnych modeli współpracy z siecią centrów kompetencji; zdolność do usystematyzowania współpracy oraz wspólnych zobowiązań zainteresowanych podmiotów publicznych i prywatnych ze wszystkich właściwych sektorów, w tym sektora obrony. Nie mniej istotny jest fakt, że wariant 1 umożliwia również zwiększenie synergii i może funkcjonować jako mechanizm realizacji w przypadku dwóch różnych unijnych źródeł finansowania cyberbezpieczeństwa w ramach kolejnych wieloletnich ram finansowych (program „Cyfrowa Europa” i program „Horyzont Europa”).

- **Prawa podstawowe**

Niniejsza inicjatywa umożliwi organom publicznym i branżom w państwach członkowskich skuteczniejsze zapobieganie zagrożeniom dla cyberbezpieczeństwa i reagowanie na nie dzięki zaoferowaniu bezpieczniejszych produktów i rozwiązań oraz wyposażaniu się w nie. Jest to w szczególności istotne w przypadku ochrony dostępu do podstawowych usług (np. usług transportu, zdrowia, bankowości i finansowych).

Zwiększona zdolność Unii Europejskiej do zabezpieczenia swoich produktów i usług w sposób autonomiczny prawdopodobnie również pomoże obywatelom w korzystaniu z ich demokratycznych praw i wartości (np. lepszej ochronie ich praw dotyczących informacji przewidzianych w Karcie praw podstawowych, szczególnie prawa do ochrony danych osobowych i życia prywatnego), a wskutek tego zwiększy ich zaufanie do społeczeństwa cyfrowego i gospodarki cyfrowej.

4. WPŁYW NA BUDŻET

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, działające we współpracy z siecią kompetencji w dziedzinie cyberbezpieczeństwa, będzie głównym organem ds. wdrażania zajmującym się

zasobami finansowymi UE przeznaczonymi na cyberbezpieczeństwo na podstawie programu „Cyfrowa Europa” i programu „Horyzont Europa”.

Wpływ na budżet związany z realizacją programu „Cyfrowa Europa” określono w ocenie skutków finansowych regulacji załączonej do niniejszego wniosku. W trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo” filaru II „Globalne wyzwania i konkurencyjność przemysłowa” programu „Horyzont Europa” (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 21 ust. 1 lit. b). Wniosek będzie opierał się na wynikach procesu planowania strategicznego określonego w art. 6 ust. 6 rozporządzenia XXX [program ramowy „Horyzont Europa”].

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

W niniejszym wniosku (art. 38) przewidziano wyraźną klauzulę oceny, na podstawie której Komisja będzie przeprowadzać niezależną ocenę. Następnie Komisja będzie przedstawiać Parlamentowi Europejskiemu i Radzie sprawozdania z oceny, którym w stosownych przypadkach towarzyszyć będzie wniosek o dokonanie przeglądu w celu zmierzenia wpływu wywieranego przez instrument i wartości dodanej, którą generuje. Komisja stosować będzie metodykę oceny służącą lepszemu stanowieniu prawa.

Dyrektor wykonawczy powinien co dwa lata przedstawiać Radzie Zarządzającej ocenę ex post na temat działalności Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci, jak określono w art. 17 niniejszego wniosku. Dyrektor wykonawczy powinien również sporządzać plan działań następczych w odniesieniu do wniosków z ocen retrospektywnych i co dwa lata składać Komisji sprawozdanie z postępów. Rada Zarządzająca powinna odpowiadać za monitorowanie wdrożenia odpowiednich działań następczych w związku ze wspomnianymi wnioskami, jak określono w art. 16 niniejszego wniosku.

Domniemane przypadki niewłaściwego administrowania w ramach działań podmiotu prawnego mogą podlegać dochodzeniom prowadzonym przez Europejskiego Rzecznika Praw Obywatelskich zgodnie z przepisami art. 228 Traktatu.

2018/0328 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji

Wkład Komisji Europejskiej w spotkanie przywódców w Salzburgu w dniach 19–20 września 2018 r.

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 173 ust. 3 i art. 188 akapit pierwszy,

uwzględniając wniosek Komisji Europejskiej,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[18],

uwzględniając opinię Komitetu Regionów[19],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Nasze życie codzienne i gospodarki stają się bardziej zależne od technologii cyfrowych, dlatego obywatele w coraz większym stopniu narażeni są na poważne cyberincydenty. Przyszłe bezpieczeństwo zależy między innymi od poprawy zdolności technologicznych i przemysłowych Unii do ochrony przed zagrożeniami dla cyberbezpieczeństwa, ponieważ zarówno infrastruktura cywilna, jak i potencjał wojskowy opierają się na bezpiecznych systemach cyfrowych.

(2) Unia stale intensyfikuje swoje działania w celu rozwiązania rosnących wyzwań w zakresie cyberbezpieczeństwa, realizując strategię bezpieczeństwa cybernetycznego z 2013 r.[20] służącą promowaniu niezawodnego, bezpiecznego i otwartego ekosystemu cybernetycznego. W 2016 r. Unia przyjęła pierwsze środki w dziedzinie cyberbezpieczeństwa w postaci dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[21] w sprawie bezpieczeństwa sieci i systemów informatycznych.

---

18 Dz.U. C z, s. .

19 Dz.U. C [...] z [...], s. [...].

20 Wspólny komunikat do Parlamentu Europejskiego i Rady „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń”, JOIN(2013) 1 final.

21 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

(3) We wrześniu 2017 r. Komisja i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili wspólny komunikat[22] „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej”, aby w dalszym ciągu wzmacniać odporność, prewencję i reakcję Unii w kwestii cyberataków.

(4) Podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. szefowie państw i rządów wezwali Unię, aby stała się „do 2025 r. światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia zaufania, pewności i ochrony naszym obywatelom, konsumentom i przedsiębiorstwom online oraz umożliwienia istnienia wolnego i podlegającego przepisom prawa internetu”.

(5) Znaczne zakłócenie funkcjonowania sieci i systemów informatycznych może wpływać na poszczególne państwa członkowskie i na Unię jako całość. Bezpieczeństwo sieci i systemów informatycznych ma zatem zasadnicze znaczenie dla sprawnego funkcjonowania rynku wewnętrznego. Obecnie Unia jest uzależniona od dostawców cyberbezpieczeństwa spoza Europy. W strategicznym interesie Unii leży jednak zapewnienie, aby utrzymała i rozwijała podstawowe zdolności technologiczne w zakresie cyberbezpieczeństwa w celu ochrony swojego jednolitego rynku cyfrowego, a w szczególności ochrony sieci i systemów informatycznych o znaczeniu krytycznym, oraz dostarczania kluczowych usług w zakresie cyberbezpieczeństwa.

(6) Chociaż w Unii istnieje bardzo wysoki poziom wiedzy fachowej i doświadczenia w zakresie badań naukowych, technologii i rozwoju przemysłu w dziedzinie cyberbezpieczeństwa, to wysiłki środowisk branżowych i naukowych są rozproszone, brakuje zbieżności działań i wspólnej misji, co stanowi przeszkodę dla konkurencyjności w tej dziedzinie. Należy połączyć te wysiłki i wiedzę fachową, utworzyć sieć kontaktów i wykorzystać je w skuteczny sposób, aby wzmocnić i uzupełnić trwające badania naukowe, zdolności technologiczne i przemysłowe na szczeblu unijnym i na szczeblach krajowych.

(7) W swoich konkluzjach przyjętych w listopadzie 2017 r. Rada wezwała Komisję do szybkiego dostarczenia oceny skutków na temat możliwych wariantów stworzenia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa wraz z Europejskim Centrum Badań Naukowych i Kompetencji i do zaproponowania do połowy 2018 r. odpowiedniego instrumentu prawnego.

(8) Centrum Kompetencji powinno być głównym unijnym instrumentem służącym łączeniu inwestycji w badania naukowe w dziedzinie cyberbezpieczeństwa, technologię i rozwój przemysłowy oraz wdrażaniu odpowiednich projektów i inicjatyw razem z siecią kompetencji w dziedzinie cyberbezpieczeństwa. Centrum to powinno zapewnić wsparcie finansowe związane z cyberbezpieczeństwem z programów „Horyzont Europa” i „Cyfrowa Europa” oraz, w stosownych przypadkach, powinno być otwarte na Europejski Fundusz Rozwoju Regionalnego i inne programy. Podejście to powinno przyczynić się do tworzenia synergii i koordynacji wsparcia finansowego związanego z badaniami naukowymi, innowacjami, rozwojem technologiczno-przemysłowym w dziedzinie cyberbezpieczeństwa oraz do unikania powielania działań.

[22] Wspólny komunikat do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej”, JOIN(2017) 450 final.

(9) Biorąc pod uwagę, że cele tej inicjatywy zostaną osiągnięte w najlepszy sposób, jeżeli uczestniczyć w niej będą wszystkie państwa członkowskie lub jak najwięcej państw członkowskich, i aby zachęcić państwa członkowskie do uczestnictwa, wyłącznie państwa członkowskie, które wniosą wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji, powinny dysponować prawem głosu.

(10) Finansowy udział uczestniczących państw członkowskich powinien być współmierny do finansowego wkładu Unii na rzecz tej inicjatywy.

(11) Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy sieci kompetencji w dziedzinie cyberbezpieczeństwa („sieć"), składającej się z krajowych ośrodków koordynacji z każdego państwa członkowskiego. Krajowe ośrodki koordynacji powinny otrzymywać bezpośrednie wsparcie finansowe Unii, w tym dotacje przyznawane bez zaproszenia do składania wniosków, w celu przeprowadzania działań związanych z niniejszym rozporządzeniem.

(12) Krajowe ośrodki koordynacji powinny zostać wybrane przez państwa członkowskie. Poza niezbędnym potencjałem administracyjnym ośrodki powinny posiadać wiedzę techniczną w dziedzinie cyberbezpieczeństwa, zwłaszcza w obszarach takich jak kryptografia, usługi w zakresie bezpieczeństwa ICT, wykrywanie włamań, bezpieczeństwo systemu, bezpieczeństwo sieci, bezpieczeństwo oprogramowania i aplikacji lub ludzkie i społeczne aspekty bezpieczeństwa i prywatności, albo mieć do takiej wiedzy bezpośredni dostęp. Powinny one mieć również zdolność do skutecznego angażowania i koordynowania wysiłków przemysłu, sektora publicznego, w tym organów wyznaczonych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148[23], oraz środowiska naukowego.

(13) Jeżeli krajowym ośrodkom koordynacji zostanie zapewnione wsparcie finansowe w celu wsparcia osób trzecich na szczeblu krajowym, należy przekazać je odpowiednim zainteresowanym stronom za pośrednictwem umów o udzielenie dotacji w systemie kaskadowym.

(14) Powstające technologie, np. sztuczna inteligencja, internet rzeczy, obliczenia wielkiej skali (HPC) i informatyka kwantowa, łańcuch bloków oraz koncepcje takie jak bezpieczna tożsamość cyfrowa, jednocześnie tworzą nowe wyzwania dla cyberbezpieczeństwa i zapewniają rozwiązania. Ocena i zatwierdzenie odporności istniejących lub przyszłych systemów ICT będzie wymagać testowania rozwiązań w zakresie bezpieczeństwa pod kątem ataków na urządzenia HPC i urządzenia kwantowe. Centrum Kompetencji, sieć i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny pomagać w rozwijaniu i rozpowszechnianiu najnowszych rozwiązań w zakresie cyberbezpieczeństwa. Jednocześnie Centrum Kompetencji i sieć powinny służyć twórcom rozwiązań i operatorom w sektorach krytycznych takich jak sektor transportowy, energetyczny, zdrowia, finansowy, administracji, telekomunikacyjny, wytwórczy, obrony i przestrzeni kosmicznej, aby pomóc im w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem.

(15) Centrum Kompetencji powinno pełnić szereg kluczowych funkcji. Po pierwsze, Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy europejskiej

[23] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

sieci kompetencji w dziedzinie cyberbezpieczeństwa oraz wspierać rozwój środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Centrum powinno realizować technologiczny plan w dziedzinie cyberbezpieczeństwa i ułatwiać dostęp do wiedzy fachowej zebranej w ramach sieci i środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Po drugie, Centrum powinno wdrażać odpowiednie części programów „Cyfrowa Europa" i „Horyzont Europa" poprzez przydzielanie dotacji, zwykle na podstawie konkurencyjnych zaproszeń do składania wniosków. Po trzecie, Centrum Kompetencji powinno ułatwiać wspólne inwestycje Unii, państw członkowskich lub przemysłu.

(16) Centrum Kompetencji powinno stymulować i wspierać współpracę i koordynację działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, które obejmowałoby dużą, otwartą i zróżnicowaną grupę podmiotów zaangażowanych w technologię cyberbezpieczeństwa. Środowisko to powinno obejmować w szczególności podmioty prowadzące badania naukowe, branże po stronie podaży, branże po stronie popytu i sektor publiczny. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinno wnieść wkład w działania i plan prac Centrum Kompetencji i powinno również korzystać z działań na rzecz tworzenia środowiska prowadzonych przez Centrum Kompetencji i sieć, ale nie powinno być pod innymi względami uprzywilejowane w zakresie zaproszeń do składania wniosków lub zaproszeń do składania ofert.

(17) Aby odpowiedzieć na potrzeby zarówno branż po stronie podaży, jak i branż po stronie popytu, zadanie Centrum Kompetencji dotyczące zapewnienia wiedzy z zakresu cyberbezpieczeństwa i pomocy technicznej gałęziom przemysłu powinno odnosić się zarówno do produktów i usług ICT, jak i wszystkich innych przemysłowych i technologicznych produktów i rozwiązań, do których ma zostać włączone cyberbezpieczeństwo.

(18) Chociaż Centrum Kompetencji i sieć powinny mieć na celu osiągnięcie synergii między cyberbezpieczeństwem cywilnym i cyberbezpieczeństwem obronnym, projekty finansowane w ramach programu „Horyzont Europa" będą wdrażane zgodnie z rozporządzeniem XXX [rozporządzenie w sprawie programu „Horyzont Europa"], w którym przewidziano, że działania w zakresie badań naukowych i innowacji przeprowadzane w ramach programu „Horyzont Europa" powinny dotyczyć głównie zastosowań cywilnych.

(19) Aby zapewnić ustrukturyzowaną i zrównoważoną współpracę, relacje między Centrum Kompetencji a krajowymi ośrodkami koordynacji powinny opierać się na porozumieniu umownym.

(20) Należy stworzyć odpowiednie przepisy, aby zagwarantować odpowiedzialność i przejrzystość działania Centrum Kompetencji.

(21) W świetle wiedzy fachowej w dziedzinie cyberbezpieczeństwa, jaką posiadają odpowiednio Wspólne Centrum Badawcze Komisji oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), powinny one odgrywać aktywną rolę w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa i Radzie Konsultacyjnej ds. Przemysłowych i Naukowych.

(22) W przypadku gdy krajowy ośrodek koordynacji i podmioty wchodzące w skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa otrzymują wkład finansowy z budżetu ogólnego Unii, powinny podać do wiadomości publicznej fakt, że odpowiednie działania podejmowane są w kontekście obecnej inicjatywy.

(23) Wkład Unii na rzecz Centrum Kompetencji powinien sfinansować połowę kosztów związanych z założeniem oraz działaniami administracyjnymi i koordynacyjnymi Centrum Kompetencji. Aby uniknąć podwójnego finansowania, działania te nie powinny jednocześnie korzystać ze środków pochodzących z innych unijnych programów.

(24) Rada Zarządzająca Centrum Kompetencji, składająca się z przedstawicieli państw członkowskich i Komisji, powinna określać ogólny kierunek działalności Centrum Kompetencji oraz zapewniać wykonywanie przez nie jego zadań zgodnie z niniejszym rozporządzeniem. Rada Zarządzająca powinna posiadać uprawnienia niezbędne do uchwalania budżetu, kontroli jego wykonania, przyjmowania stosownych przepisów finansowych, ustalania przejrzystych procedur pracy w zakresie podejmowania decyzji przez Centrum Kompetencji, przyjmowania planu prac Centrum Kompetencji i wieloletniego planu strategicznego odzwierciedlającego priorytety w realizacji celów i zadań Centrum Kompetencji, uchwalania jej regulaminu wewnętrznego, powoływania dyrektora wykonawczego oraz podejmowania decyzji o przedłużeniu jego kadencji lub jej zakończeniu.

(25) Aby Centrum Kompetencji mogło prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków Rady Zarządzającej, posiadały odpowiednią zawodową wiedzę fachową i doświadczenie w obszarach funkcyjnych. Komisja i państwa członkowskie powinny również dołożyć starań, by ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej, tak aby zapewnić ciągłość jej pracy.

(26) Sprawne funkcjonowanie Centrum Kompetencji wymaga, aby dyrektor wykonawczy był mianowany na podstawie swoich osiągnięć oraz udokumentowanych kompetencji administracyjnych i zarządczych, a także odpowiednich kompetencji i doświadczenia w zakresie cyberbezpieczeństwa, oraz aby pełnił swoje obowiązki w sposób całkowicie niezależny.

(27) Centrum Kompetencji powinno posiadać organ doradczy w postaci Rady Konsultacyjnej ds. Przemysłowych i Naukowych w celu zapewnienia regularnego dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami. Rada Konsultacyjna ds. Przemysłowych i Naukowych powinna skupiać się na zagadnieniach istotnych dla zainteresowanych stron i kierować na nie uwagę Rady Zarządzającej Centrum Kompetencji. Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz przydzielone jej zadania, takie jak zasięganie jej opinii w sprawie planu prac, powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach Centrum Kompetencji.

(28) Centrum Kompetencji powinno korzystać ze szczególnej wiedzy fachowej oraz szerokiego i odpowiedniego udziału zainteresowanych stron, stworzonego w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w trakcie trwania programu „Horyzont 2020” za pośrednictwem swojej Rady Konsultacyjnej ds. Przemysłowych i Naukowych.

(29) W Centrum Kompetencji powinny obowiązywać przepisy dotyczące zapobiegania konfliktom interesów i zarządzania nimi. Centrum Kompetencji powinno również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (WE)

nr 1049/2001[24]. Przetwarzanie danych osobowych przez Centrum Kompetencji będzie podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018. Centrum Kompetencji powinno przestrzegać przepisów mających zastosowanie do instytucji Unii oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności ze szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi UE.

(30) Interesy finansowe Unii i państw członkowskich powinny być chronione w całym cyklu wydatków za pomocą proporcjonalnych środków, w tym poprzez zapobieganie nieprawidłowościom, ich wykrywanie i prowadzenie dochodzeń w sprawach nieprawidłowości, odzyskiwanie utraconych, nienależnie wypłaconych lub nieprawidłowo wykorzystanych funduszy oraz, w stosownych przypadkach, nakładanie kar administracyjnych i pieniężnych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, EURATOM) nr XXX[25] [rozporządzenie finansowe].

(31) Centrum Kompetencji powinno działać w otwarty i przejrzysty sposób pozwalający mu na czas udostępniać wszelkie stosowne informacje, jak również promować swoje działania, w tym działania informacyjne i upowszechnianie wiedzy wśród społeczeństwa. Regulamin wewnętrzny organów Centrum Kompetencji powinien być dostępny publicznie.

(32) Audytor wewnętrzny Komisji powinien mieć w stosunku do Centrum Kompetencji takie same uprawnienia jak w stosunku do Komisji.

(33) Komisja, Centrum Kompetencji, Europejski Trybunał Obrachunkowy i Europejski Urząd ds. Zwalczania Nadużyć Finansowych powinny uzyskać dostęp do wszystkich niezbędnych informacji i pomieszczeń, aby prowadzić audyty i dochodzenia dotyczące dotacji, umów i porozumień podpisanych przez Centrum Kompetencji.

(34) Ponieważ cele niniejszego rozporządzenia, a mianowicie utrzymanie i rozwijanie technologicznych i przemysłowych zdolności Unii w dziedzinie cyberbezpieczeństwa, zwiększanie konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynienia z cyberbezpieczeństwa przewagi konkurencyjnej innych gałęzi przemysłu Unii, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie z uwagi na rozproszenie istniejących, ograniczonych zasobów oraz niezbędną wielkość inwestycji, lecz ze względu na uniknięcie niepotrzebnego powielania tych wysiłków, pomoc w osiąganiu masy krytycznej inwestycji i zapewnienie, by finansowanie publiczne wykorzystywano w sposób optymalny, mogą być lepiej realizowane na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności, o której mowa w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,

---

[24] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1049/2001 z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

[25] [dodać tytuł i odniesienie do Dz.U.].

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

OGÓLNE PRZEPISY I ZASADY CENTRUM KOMPETENCJI ORAZ SIECI

Artykuł 1

Przedmiot

1. Na mocy niniejszego rozporządzenia ustanawia się Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji”) oraz sieć krajowych ośrodków koordynacji, a także określa się przepisy dotyczące nominacji krajowych ośrodków koordynacji i tworzenia środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.
2. Centrum Kompetencji wnosi wkład we wdrażanie części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa” ustanowionego rozporządzeniem nr XXX, w szczególności we wdrażanie działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”], a także we wdrażanie programu „Horyzont Europa” ustanowionego rozporządzeniem nr XXX, w szczególności filaru II pkt 2.2.6 załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa” [numer referencyjny programu szczegółowego].
3. Siedziba Centrum Kompetencji znajduje się w [Brukseli w Belgii].
4. Centrum Kompetencji posiada osobowość prawną. We wszystkich państwach członkowskich centrum ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym zgodnie z ustawodawstwem danego państwa członkowskiego. Może ono zwłaszcza nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „cyberbezpieczeństwo” oznacza ochronę sieci i systemów informatycznych, ich użytkowników i innych osób przed zagrożeniami dla cyberbezpieczeństwa;
2) „produkty i rozwiązania w dziedzinie cyberbezpieczeństwa” oznaczają produkty, usługi lub procesy ICT, których szczególnym celem jest ochrona przed zagrożeniami dla cyberbezpieczeństwa sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą;
3) „organ publiczny” oznacza jednostkę administracji rządowej lub innej administracji publicznej, w tym publiczne organy doradcze na szczeblu krajowym, regionalnym lub lokalnym, bądź osobę fizyczną lub prawną, która na mocy prawa krajowego sprawuje publiczne funkcje administracyjne, łącznie ze szczególnymi obowiązkami;

4) „uczestniczące państwo członkowskie” oznacza państwo członkowskie, które dobrowolnie wnosi wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji.

Artykuł 3

Misja Centrum i sieci

1. Centrum Kompetencji i sieć pomagają Unii:

   a) w utrzymaniu i rozwijaniu technologicznych i przemysłowych zdolności w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego;

   b) w zwiększaniu konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynieniu z cyberbezpieczeństwa przewagi konkurencyjnej innych gałęzi przemysłu Unii.

2. W stosownych przypadkach Centrum Kompetencji realizuje swoje zadania we współpracy z siecią krajowych ośrodków koordynacji i środowiskiem posiadającym kompetencje w dziedzinie cyberbezpieczeństwa.

Artykuł 4

Cele i zadania Centrum

Cele i związane z nimi zadania Centrum Kompetencji są następujące:

1. ułatwianie i pomoc w koordynacji pracy sieci krajowych ośrodków koordynacji („sieć”), o której mowa w art. 6, oraz pracy środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, o którym mowa w art. 8;

2. wnoszenie wkładu we wdrażanie części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa” ustanowionego rozporządzeniem nr XXX[26], w szczególności działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”], oraz programu „Horyzont Europa” ustanowionego rozporządzeniem nr XXX[27], w szczególności pkt 2.2.6 filaru II załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa” [numer referencyjny programu szczegółowego], oraz innych unijnych programów, jeżeli przewidziano to w aktach prawnych Unii;

3. poszerzanie możliwości, wiedzy i ulepszanie infrastruktury w zakresie cyberbezpieczeństwa z korzyścią dla gałęzi przemysłu, sektora publicznego i środowisk naukowych dzięki wykonywaniu następujących zadań:

   a) w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i związanych z nią usług – nabywanie, ulepszanie, obsługa takiej infrastruktury oraz udostępnianie jej i związanych z nią usług szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, w tym MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

[26] [dodać pełny tytuł i odniesienie do Dz.U.]
[27] [dodać pełny tytuł i odniesienie do Dz.U.]

b) w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i związanych z nią usług – zapewnianie wsparcia innym podmiotom, w tym wsparcia finansowego, jeżeli chodzi o nabywanie, ulepszanie, obsługę takiej infrastruktury oraz udostępnianie jej i związanych z nią usług szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, w tym MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej;

c) zapewnianie sektorowi przemysłu i organom publicznym wiedzy z zakresu cyberbezpieczeństwa oraz pomocy technicznej, w szczególności poprzez wspieranie działań mających na celu ułatwianie dostępu do wiedzy fachowej dostępnej w sieci i w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa;

4. wnoszenie wkładu w powszechne wdrażanie w całej gospodarce nowoczesnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań:

a) stymulowanie badań naukowych w dziedzinie cyberbezpieczeństwa, rozwoju cyberbezpieczeństwa, a także absorpcji unijnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa przez organy publiczne i branże wykorzystujące te produkty i rozwiązania;

b) wspomaganie organów publicznych, branż po stronie popytu i innych użytkowników w przyjmowaniu i wdrażaniu najnowszych rozwiązań w dziedzinie cyberbezpieczeństwa;

c) wspieranie w szczególności organów publicznych w organizacji udzielania zamówień publicznych lub przeprowadzanie zamówień na nowoczesne produkty i rozwiązania w dziedzinie cyberbezpieczeństwa w imieniu organów publicznych;

d) zapewnianie wsparcia finansowego i pomocy technicznej przedsiębiorstwom typu start-up oraz MŚP w dziedzinie cyberbezpieczeństwa w celu ich połączenia z potencjalnymi rynkami i przyciągnięcia inwestycji;

5. poprawa zrozumienia kwestii cyberbezpieczeństwa i wnoszenie wkładu w ograniczanie niedoborów kwalifikacji w zakresie cyberbezpieczeństwa w Unii dzięki realizacji następujących zadań:

a) wspieranie dalszego rozwoju umiejętności w dziedzinie cyberbezpieczeństwa, w stosownych przypadkach z udziałem odpowiednich agencji i organów UE, w tym Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji;

6. przyczynianie się do wzmacniania badań naukowych i rozwoju w dziedzinie cyberbezpieczeństwa w Unii poprzez:

a) zapewnianie wsparcia finansowego na wysiłki badawcze w dziedzinie cyberbezpieczeństwa, których podstawą jest wspólny, stale oceniany i ulepszany wieloletni program dotyczący strategii, przemysłu, technologii i badań naukowych;

b) wspieranie dużych projektów badawczych i demonstracyjnych dotyczących możliwości technologicznych nowej generacji w dziedzinie cyberbezpieczeństwa we współpracy z przemysłem i siecią;

c) wspieranie badań naukowych i innowacji w celu standaryzacji technologii cyberbezpieczeństwa;

7. zacieśnienie współpracy między kręgami cywilnymi i kręgami obronnymi w odniesieniu do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań:

   a) wspieranie państw członkowskich i zainteresowanych podmiotów naukowych i przemysłowych w zakresie badań naukowych, rozwoju i wdrażania;

   b) wnoszenie wkładu we współpracę między państwami członkowskimi dzięki wspieraniu kształcenia, szkolenia i ćwiczeń;

   c) łączenie zainteresowanych stron, aby wspierać synergie między badaniami i rynkami w zakresie cyberbezpieczeństwa w wymiarach cywilnym i obronnym;

8. zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego dzięki wykonywaniu następujących zadań:

   a) doradztwo, dzielenie się wiedzą fachową oraz ułatwianie współpracy między zainteresowanymi stronami;

   b) zarządzanie międzynarodowymi projektami w dziedzinie cyberobrony na wniosek państw członkowskich i tym samym działanie jako kierownik projektu w rozumieniu rozporządzenia XXX [rozporządzenie ustanawiające Europejski Fundusz Obronny].

Artykuł 5

Inwestowanie w infrastrukturę, możliwości, produkty lub rozwiązania oraz ich wykorzystanie

1. W przypadku gdy Centrum Kompetencji zapewnia finansowanie infrastruktury, możliwości, produktów lub rozwiązań zgodnie z art. 4 ust. 3 i 4 w formie dotacji lub nagrody, w planie prac Centrum Kompetencji mogą być określone w szczególności:

   a) zasady dotyczące funkcjonowania infrastruktury lub możliwości, w tym w stosownych przypadkach dotyczące powierzenia obsługi podmiotowi zajmującemu się hostingiem, w oparciu o kryteria, które określa Centrum Kompetencji;

   b) zasady dotyczące dostępu do infrastruktury lub możliwości oraz ich wykorzystania.

2. Centrum Kompetencji może być odpowiedzialne za ogólne wykonanie odpowiednich działań związanych ze wspólnym udzielaniem zamówień, w tym za przedkomercyjne zamówienia publiczne w imieniu członków sieci, członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa lub innych osób trzecich reprezentujących użytkowników produktów i rozwiązań w dziedzinie cyberbezpieczeństwa. W tym celu Centrum Kompetencji może być wspierane przez co najmniej jeden krajowy ośrodek koordynacji lub członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

Artykuł 6

Wyznaczenie krajowych ośrodków koordynacji

1. Do dnia [data] każde państwo członkowskie wyznacza podmiot, który będzie pełnił rolę krajowego ośrodka koordynacji do celów niniejszego rozporządzenia, i powiadamia o tym Komisję.

2. Na podstawie oceny dotyczącej spełnienia przez ten podmiot kryteriów określonych w ust. 4 Komisja w ciągu sześciu miesięcy od nominacji przekazanej przez państwo członkowskie wydaje decyzję przewidującą akredytację podmiotu jako krajowego ośrodka koordynacji lub odrzucającą nominację. Komisja publikuje wykaz krajowych ośrodków koordynacji.

3. Państwa członkowskie mogą w dowolnym momencie wyznaczyć nowy podmiot, który będzie pełnił rolę krajowego ośrodka koordynacji do celów niniejszego rozporządzenia. Ust. 1 i 2 mają zastosowanie do wyznaczenia nowego podmiotu.

4. Wyznaczony krajowy ośrodek koordynacji posiada możliwość wspierania Centrum Kompetencji oraz sieci w wypełnianiu ich misji określonej w art. 3 niniejszego rozporządzenia. Ośrodki dysponują techniczną wiedzą fachową w dziedzinie cyberbezpieczeństwa lub bezpośrednim dostępem do niej oraz mają możliwość skutecznego angażowania przemysłu, sektora publicznego i społeczności badawczej i współpracy z nimi.

5. Relacje między Centrum Kompetencji i krajowymi ośrodkami koordynacji opierają się na umowach podpisanych między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji. W umowie określa się reguły dotyczące relacji między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji oraz podziału zadań między nimi.

6. Sieć krajowych ośrodków koordynacji składa się ze wszystkich krajowych ośrodków koordynacji wyznaczonych przez państwa członkowskie.

Artykuł 7

Zadania krajowych ośrodków koordynacji

1. Cele i związane z nimi zadania krajowych ośrodków koordynacji są następujące:

   a) wspieranie Centrum Kompetencji w osiąganiu jego celów, a w szczególności w koordynowaniu działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;

   b) ułatwianie przemysłowi i innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych;

   c) udział wspólnie z Centrum Kompetencji w określaniu i eliminowaniu stojących przed przemysłem wyzwań w dziedzinie cyberbezpieczeństwa, które dotyczą konkretnych sektorów;

   d) pełnienie roli punktu kontaktowego na szczeblu krajowym na potrzeby środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji;

   e) dążenie do tworzenia synergii z odpowiednimi działaniami na szczeblu krajowym i regionalnym;

f) wdrażanie poszczególnych działań, na które Centrum Kompetencji przyznało dotacje, w tym poprzez zapewnianie wsparcia finansowego osobom trzecim zgodnie z art. 204 rozporządzenia XXX [nowe rozporządzenie finansowe] na warunkach określonych w odnośnych umowach o udzielenie dotacji;

g) promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji odpowiednich wyników prac na szczeblu krajowym i regionalnym;

h) ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa składanych przez podmioty mające siedzibę w tym samym państwie członkowskim co ośrodek koordynacji.

2. Do celów określonych w lit. f) wsparcie finansowe dla osób trzecich może być zapewniane w którejkolwiek z form określonych w art. 125 rozporządzenia XXX [nowe rozporządzenie finansowe], w tym w formie kwot ryczałtowych.

3. Krajowe ośrodki koordynacji mogą otrzymać od Unii dotacje zgodnie z art. 195 lit. d) rozporządzenia XXX [nowe rozporządzenie finansowe] w związku z wykonywaniem zadań określonych w niniejszym artykule.

4. W stosownych przypadkach krajowe ośrodki koordynacji współpracują za pośrednictwem sieci w celu realizacji zadań, o których mowa w ust. 1 lit. a), b), c), e) i g).

Artykuł 8

Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa

1. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa wnosi swój wkład w misję Centrum Kompetencji, jak określono w art. 3, oraz wzmacnia i rozpowszechnia wiedzę fachową z zakresu cyberbezpieczeństwa w całej Unii.

2. W skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa wchodzą organizacje przemysłowe, akademickie i organizacje naukowe non-profit, a także stowarzyszenia oraz podmioty publiczne i inne podmioty zajmujące się kwestiami operacyjnymi i technicznymi. Środowisko to skupia główne zainteresowane strony, jeżeli chodzi o technologiczne i przemysłowe zdolności w dziedzinie cyberbezpieczeństwa w Unii. W jego skład wchodzą krajowe ośrodki koordynacji, a także unijne instytucje i organy posiadające odpowiednią wiedzę fachową.

3. Jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa można akredytować jedynie podmioty, które mają siedzibę w Unii. Podmioty te muszą wykazać, że dysponują wiedzą fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin:

a) badania naukowe;

b) rozwój przemysłu;

c) szkolenie i kształcenie.

4. Centrum Kompetencji akredytuje podmioty ustanowione na mocy prawa krajowego jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu przez krajowy ośrodek koordynacji państwa członkowskiego, w którym ma siedzibę dany podmiot, oceny, czy podmiot ten spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale

Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli samo Centrum lub właściwy krajowy ośrodek koordynacji uzna, że podmiot nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe].

5. Centrum Kompetencji akredytuje odpowiednie organy, agencje i urzędy Unii jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu oceny, czy dany podmiot spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli uzna, że podmiot nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe].

6. W pracach prowadzonych w ramach środowiska mogą brać udział przedstawiciele Komisji.

Artykuł 9

Zadania członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa

Członkowie środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa:

1) wspierają Centrum Kompetencji w wypełnianiu misji i osiąganiu celów określonych w art. 3 i 4 oraz ściśle współpracują w tym celu z Centrum Kompetencji i właściwymi krajowymi ośrodkami koordynacji;

2) uczestniczą w działaniach promowanych przez Centrum Kompetencji i krajowe ośrodki koordynacji;

3) w stosownych przypadkach uczestniczą w grupach roboczych ustanowionych przez Radę Zarządzającą Centrum Kompetencji w celu realizacji poszczególnych działań określonych w planie prac Centrum Kompetencji;

4) w stosownych przypadkach wspierają Centrum Kompetencji i krajowe ośrodki koordynacji w promowaniu poszczególnych projektów;

5) promują i rozpowszechniają stosowne wyniki działań i projektów prowadzonych w ramach społeczności.

Artykuł 10

Współpraca Centrum Kompetencji z instytucjami, organami, urzędami i agencjami Unii

1. Centrum Kompetencji współpracuje z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, w tym z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, z zespołem reagowania na incydenty komputerowe (CERT-UE), Europejską Służbą Działań Zewnętrznych, ze Wspólnym Centrum Badawczym Komisji, Agencją Wykonawczą ds. Badań Naukowych, Agencją Wykonawczą ds. Innowacyjności i Sieci, Europejskim Centrum ds. Walki z Cyberprzestępczością w Europolu oraz z Europejską Agencją Obrony.

2. Taka współpraca ma miejsce w ramach uzgodnień roboczych. Uzgodnienia te należy uprzednio przedłożyć do zatwierdzenia przez Komisję.

ROZDZIAŁ II

ORGANIZACJA CENTRUM KOMPETENCJI

Artykuł 11

Członkostwo i struktura

1. Członkami Centrum Kompetencji są Unia reprezentowana przez Komisję i państwa członkowskie.

2. Struktura Centrum Kompetencji składa się z:

   a) Rady Zarządzającej, która wykonuje zadania określone w art. 13;

   b) dyrektora wykonawczego, który wykonuje zadania określone w art. 16;

   c) Rady Konsultacyjnej ds. Przemysłowych i Naukowych, która pełni funkcje określone w art. 20.

SEKCJA I

RADA ZARZĄDZAJĄCA

Artykuł 12

Skład Rady Zarządzającej

1. W skład Rady Zarządzającej wchodzi po jednym przedstawicielu każdego państwa członkowskiego oraz pięciu przedstawicieli Komisji w imieniu Unii.

2. Każdy z członków Rady Zarządzającej posiada zastępcę, który reprezentuje członka w przypadku jego nieobecności.

3. Członków Rady Zarządzającej i ich zastępców powołuje się, biorąc pod uwagę ich wiedzę z dziedziny technologii, a także odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem. Komisja oraz państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej w celu zapewnienia ciągłości pracy Rady. Komisja oraz państwa członkowskie mają na celu osiągnięcie zrównoważonej reprezentacji mężczyzn i kobiet w Radzie Zarządzającej.

4. Kadencja członków Rady Zarządzającej i ich zastępców trwa cztery lata. Kadencja ta jest odnawialna.

5. Członkowie Rady Zarządzającej działają w sposób niezależny i przejrzysty w interesie Centrum Kompetencji, chroniąc jego cele i misję, tożsamość, autonomię i spójność.

6. Komisja może, w stosownych przypadkach, zapraszać obserwatorów, w tym przedstawicieli odpowiednich unijnych organów, urzędów i agencji, do udziału w posiedzeniach Rady Zarządzającej.

7. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) jest stałym obserwatorem w Radzie Zarządzającej.

Artykuł 13

Zadania Rady Zarządzającej

1. Rada Zarządzająca ponosi ogólną odpowiedzialność za strategiczną orientację i operacje Centrum Kompetencji oraz nadzoruje realizację jego działalności.

2. Rada Zarządzająca uchwala swój regulamin wewnętrzny. Regulamin ten zawiera szczegółowe procedury ustalania i unikania konfliktów interesów i zapewnia poufność wszelkich informacji szczególnie chronionych.

3. Rada Zarządzająca podejmuje niezbędne decyzje strategiczne, a w szczególności:

   a) przyjmuje wieloletni plan strategiczny obejmujący zestawienie głównych priorytetów oraz planowanych inicjatyw Centrum Kompetencji, w tym oszacowanie potrzeb finansowych i źródeł finansowania;

   b) na podstawie wniosku dyrektora wykonawczego przyjmuje plan prac Centrum Kompetencji, roczne sprawozdanie finansowe i bilans oraz roczne sprawozdanie z działalności;

   c) przyjmuje szczegółowe przepisy finansowe Centrum Kompetencji zgodnie z [art. 70 RF];

   d) przyjmuje procedurę powoływania dyrektora wykonawczego;

   e) przyjmuje kryteria i procedury oceny i akredytacji podmiotów jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;

   f) powołuje, zwalnia i przedłuża kadencję dyrektora wykonawczego, udziela mu wskazówek i monitoruje jego działania oraz powołuje księgowego;

   g) przyjmuje roczny budżet Centrum Kompetencji, w tym odpowiedni plan zatrudnienia wskazujący liczbę stanowisk czasowych według grupy funkcyjnej i grupy zaszeregowania, liczbę pracowników kontraktowych i oddelegowanych ekspertów krajowych, wyrażone w ekwiwalentach pełnego czasu pracy;

   h) przyjmuje przepisy dotyczące konfliktów interesów;

   i) ustanawia grupy robocze złożone z członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa;

   j) powołuje członków Rady Konsultacyjnej ds. Przemysłowych i Naukowych;

   k) ustanawia funkcję audytu wewnętrznego zgodnie z rozporządzeniem delegowanym Komisji (UE) nr 1271/2013[28];

   l) promuje Centrum Kompetencji w skali globalnej, aby zwiększyć jego atrakcyjność i uczynić z niego światowej klasy podmiot doskonałości w dziedzinie cyberbezpieczeństwa;

   m) tworzy politykę komunikacyjną Centrum Kompetencji na podstawie zalecenia dyrektora wykonawczego;

[28] Rozporządzenie delegowane Komisji (UE) nr 1271/2013 z dnia 30 września 2013 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów, o których mowa w art. 208 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 (Dz.U. L 328 z 7.12.2013, s. 42).

n) odpowiada za monitorowanie odpowiednich działań następczych wynikających z wniosków z ocen retrospektywnych;

o) w stosownych przypadkach ustanawia przepisy wykonawcze do regulaminu pracowniczego i warunków zatrudnienia zgodnie z art. 31 ust. 3;

p) w stosownych przypadkach określa zasady dotyczące delegowania ekspertów krajowych do Centrum Kompetencji oraz wykorzystania stażystów zgodnie z art. 32 ust. 2;

q) przyjmuje przepisy bezpieczeństwa dla Centrum Kompetencji;

r) przyjmuje strategię zwalczania nadużyć finansowych, która jest proporcjonalna do istniejących w tym zakresie zagrożeń, uwzględniając analizę kosztów i korzyści w odniesieniu do środków, które mają zostać wdrożone;

s) przyjmuje metodę obliczania wkładu finansowego państw członkowskich;

t) odpowiada za każde zadanie nieprzydzielone żadnemu konkretnemu organowi Centrum Kompetencji; może przydzielać takie zadania każdemu organowi Centrum Kompetencji.

Artykuł 14

Przewodniczący i posiedzenia Rady Zarządzającej

1. Rada Zarządzająca wybiera na okres dwóch lat przewodniczącego i zastępcę przewodniczącego spośród tych członków, którzy mają prawo głosu. Kadencję przewodniczącego i zastępcy przewodniczącego można jednokrotnie przedłużyć na podstawie decyzji Rady Zarządzającej. Jeżeli jednak w dowolnym momencie swojej kadencji stracą oni status członka Rady Zarządzającej, kadencja ich kończy się automatycznie w tym samym dniu. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków. Przewodniczący bierze udział w głosowaniu.

2. Rada Zarządzająca odbywa swoje zwykłe posiedzenia co najmniej trzy razy w roku. Rada może zwoływać posiedzenia nadzwyczajne na wniosek Komisji, na wniosek co najmniej jednej trzeciej wszystkich swoich członków, na wniosek przewodniczącego lub na wniosek dyrektora wykonawczego w ramach wykonywania jego zadań.

3. Dyrektor wykonawczy ma prawo uczestniczenia w obradach, o ile Rada Zarządzająca nie postanowi inaczej, lecz bez prawa głosu. Rada Zarządzająca może zapraszać na poszczególne posiedzenia również inne osoby w charakterze obserwatorów.

4. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych mogą brać udział w posiedzeniach Rady Zarządzającej, na zaproszenie przewodniczącego, bez prawa głosu.

5. Członkowie Rady Zarządzającej i ich zastępcy mogą korzystać podczas posiedzeń z pomocy doradców lub ekspertów, z zastrzeżeniem przepisów regulaminu wewnętrznego.

6. Centrum Kompetencji zapewnia Radzie Zarządzającej obsługę sekretariatu.

Artykuł 15

Zasady głosowania Rady Zarządzającej

1. Unia posiada 50 % praw głosu. Głosy Unii są niepodzielne.

2. Każde uczestniczące państwo członkowskie posiada jeden głos.

3. Rada Zarządzająca podejmuje decyzje większością co najmniej 75 % wszystkich głosów, w tym głosów członków nieobecnych, reprezentujących co najmniej 75 % całkowitych wkładów finansowych na rzecz Centrum Kompetencji. Wkład finansowy oblicza się na podstawie zaproponowanych przez państwa członkowskie szacowanych wydatków, o których mowa w art. 17 ust. 2 lit. c), oraz na podstawie sprawozdania na temat wartości wkładów uczestniczących państw członkowskich, o którym mowa w art. 22 ust. 5.

4. Jedynie przedstawiciele Komisji i przedstawiciele uczestniczących państw członkowskich posiadają prawo głosu.

5. Przewodniczący bierze udział w głosowaniu.

SEKCJA II

DYREKTOR WYKONAWCZY

Artykuł 16

Mianowanie, zwolnienie lub przedłużenie kadencji dyrektora wykonawczego

1. Dyrektor wykonawczy musi dysponować wiedzą fachową i cieszyć się szerokim uznaniem w dziedzinach, w których Centrum Kompetencji prowadzi działalność.

2. Dyrektor wykonawczy zatrudniany jest w Centrum Kompetencji na czas określony, zgodnie z art. 2 lit. a) warunków zatrudnienia innych pracowników.

3. Rada Zarządzająca w ramach otwartej i przejrzystej procedury wyboru mianuje dyrektora wykonawczego z listy kandydatów zaproponowanych przez Komisję.

4. Do celów zawarcia umowy z dyrektorem wykonawczym Centrum Kompetencji jest reprezentowane przez przewodniczącego Rady Zarządzającej.

5. Kadencja dyrektora wykonawczego trwa cztery lata. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez dyrektora wykonawczego oraz przyszłe zadania i wyzwania Centrum Kompetencji.

6. Rada Zarządzająca, działając na wniosek Komisji, w którym uwzględniono ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jednokrotnie na okres nie dłuższy niż cztery lata.

7. Dyrektor wykonawczy, którego kadencję przedłużono, nie może brać udziału w kolejnej procedurze wyboru na to samo stanowisko.

8. Dyrektor wykonawczy zostaje odwołany ze stanowiska jedynie na mocy decyzji Rady Zarządzającej działającej na wniosek Komisji.

Artykuł 17

Zadania dyrektora wykonawczego

1. Dyrektor wykonawczy jest odpowiedzialny za działalność Centrum Kompetencji i za bieżące zarządzanie nim oraz pełni funkcję jego przedstawiciela prawnego. Dyrektor wykonawczy jest odpowiedzialny przed Radą Zarządzającą i swoje obowiązki pełni całkowicie niezależnie w zakresie przyznanych mu uprawnień.

2. W szczególności dyrektor wykonawczy realizuje w niezależny sposób następujące zadania:

a) wykonuje decyzje przyjęte przez Radę Zarządzającą;

b) wspiera działania Rady Zarządzającej, pomaga sekretariatowi w organizacji posiedzeń oraz przekazuje wszelkie informacje, które są niezbędne do wykonania jej obowiązków;

c) przygotowuje i przedkłada Radzie Zarządzającej do przyjęcia, po konsultacjach z Radą Zarządzającą i Komisją, projekt wieloletniego planu strategicznego oraz projekt rocznego planu prac Centrum Kompetencji, uwzględniając zakres zaproszeń do składania wniosków, zaproszeń do wyrażenia zainteresowania i zaproszeń do składania ofert potrzebnych do celów realizacji planu prac oraz powiązane szacunki wydatków proponowane przez państwa członkowskie i Komisję;

d) opracowuje i przedkłada Radzie Zarządzającej do przyjęcia projekt budżetu rocznego, w tym powiązanego z nim planu zatrudnienia, określającego liczbę stanowisk czasowych według grupy funkcyjnej i grupy zaszeregowania oraz liczbę pracowników kontraktowych i oddelegowanych ekspertów krajowych, wyrażone w ekwiwalentach pełnego czasu pracy;

e) realizuje plan prac i składa sprawozdania z jego realizacji Radzie Zarządzającej;

f) przygotowuje projekt rocznego sprawozdania z działalności Centrum Kompetencji, uwzględniając informacje na temat powiązanych wydatków;

g) zapewnia wdrożenie skutecznych procedur monitorowania i oceny związanych z funkcjonowaniem Centrum Kompetencji;

h) przygotowuje plan działania w następstwie wniosków z ocen retrospektywnych oraz przedkłada Komisji co dwa lata sprawozdania z postępów;

i) przygotowuje, negocjuje i zawiera umowy z krajowymi ośrodkami koordynacji;

j) jest odpowiedzialny za kwestie administracyjne, finansowe i pracownicze, w tym za wykonanie budżetu Centrum Kompetencji, należycie uwzględniając wskazówki otrzymane od komórki audytu wewnętrznego w ramach uprawnień przekazanych przez Radę Zarządzającą;

k) zatwierdza ogłaszanie zaproszeń do składania wniosków i zarządza nimi – zgodnie z planem prac – oraz zarządza umowami o udzielenie dotacji i decyzjami o udzieleniu dotacji;

l) zatwierdza wykaz działań wybranych do finansowania w oparciu o listę rankingową ustaloną przez zespół niezależnych ekspertów;

m) zatwierdza ogłaszanie zaproszeń do składania ofert i zarządza nimi – zgodnie z planem prac – oraz zarządza umowami;

n) zatwierdza oferty wybrane do finansowania;

o) przedkłada komórce audytu wewnętrznego, a następnie Radzie Zarządzającej, projekt rocznego sprawozdania finansowego oraz bilansu;

p) zapewnia przeprowadzanie oceny ryzyka oraz stosowanie środków w zakresie zarządzania ryzykiem;

q) popisuje poszczególne umowy o udzielenie dotacji, decyzje i umowy;

r) podpisuje umowy w sprawie zamówienia publicznego;

s) przygotowuje plan działania na podstawie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), oraz składa sprawozdania z postępów prac dwa razy w roku Komisji i regularnie Radzie Zarządzającej;

t) przygotowuje projekt przepisów finansowych mających zastosowanie do Centrum Kompetencji;

u) ustanawia skuteczny i efektywny system kontroli wewnętrznych i zapewnia jego funkcjonowanie oraz zgłasza Radzie Zarządzającej wszelkie istotne zmiany w tym systemie;

v) zapewnia skuteczną komunikację z instytucjami Unii;

w) podejmuje wszelkie pozostałe działania potrzebne do oceny postępów Centrum Kompetencji w realizacji jego misji i celów określonych w art. 3 i 4 niniejszego rozporządzenia;

x) wykonuje wszelkie inne zadania powierzone lub zlecone mu przez Radę Zarządzającą.

SEKCJA III

RADA KONSULTACYJNA DS. PRZEMYSŁOWYCH I NAUKOWYCH

Artykuł 18

Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych

1. Rada Konsultacyjna ds. Przemysłowych i Naukowych liczy nie więcej niż 16 członków. Członków mianuje Rada Zarządzająca spośród przedstawicieli podmiotów będących częścią środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

2. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych posiadają wiedzę fachową albo w dziedzinach badań nad cyberbezpieczeństwem, rozwoju przemysłu, zawodów regulowanych albo we wdrażaniu rozwiązań w tych obszarach. Rada Zarządzająca szczegółowo określa wymogi dotyczące takiej wiedzy fachowej.

3. Procedury dotyczące powoływania jej członków przez Radę Zarządzającą oraz funkcjonowania Rady Konsultacyjnej określa się w regulaminie wewnętrznym Centrum Kompetencji i podaje do wiadomości publicznej.

4. Kadencja członków Rady Konsultacyjnej ds. Przemysłowych i Naukowych trwa trzy lata. Kadencja ta jest odnawialna.

5. Przedstawiciele Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji mogą brać udział w pracach Rady Konsultacyjnej ds. Przemysłowych i Naukowych i zapewniać im wsparcie.

Artykuł 19

Funkcjonowanie Rady Konsultacyjnej ds. Przemysłowych i Naukowych

1. Posiedzenia Rady Konsultacyjnej ds. Przemysłowych i Naukowych odbywają się co najmniej dwa razy w roku.

2. Rada Konsultacyjna ds. Przemysłowych i Naukowych może doradzać Radzie Zarządzającej w sprawie tworzenia, w razie potrzeby, grup roboczych ds. konkretnych kwestii istotnych dla pracy Centrum Kompetencji koordynowanych całościowo przez co najmniej jednego członka Rady Konsultacyjnej ds. Przemysłowych i Naukowych.

3. Rada Konsultacyjna ds. Przemysłowych i Naukowych wybiera swojego przewodniczącego.

4. Rada Konsultacyjna ds. Przemysłowych i Naukowych przyjmuje swój regulamin wewnętrzny, obejmujący powołanie przedstawicieli, którzy w stosownych przypadkach reprezentują Radę Konsultacyjną, oraz określający okres, na jaki zostali powołani.

Artykuł 20

Zadania Rady Konsultacyjnej ds. Przemysłowych i Naukowych

Rada Konsultacyjna ds. Przemysłowych i Naukowych doradza Centrum Kompetencji w kwestiach dotyczących prowadzenia jego działalności i wykonuje następujące zadania:

1) zapewnia dyrektorowi wykonawczemu i Radzie Zarządzającej doradztwo strategiczne i uwagi dotyczące przygotowywania planu prac i wieloletniego planu strategicznego w terminach ustalonych przez Radę Zarządzającą;

2) organizuje konsultacje publiczne otwarte dla wszystkich zainteresowanych stron z sektora publicznego i prywatnego, dla których cyberbezpieczeństwo stanowi przedmiot zainteresowania, aby zebrać informacje na potrzeby strategicznego doradztwa, o którym mowa w ust. 1;

3) promuje przesyłanie informacji zwrotnych na temat planu prac i wieloletniego planu strategicznego Centrum Kompetencji oraz je gromadzi.

ROZDZIAŁ III

PRZEPISY FINANSOWE

Artykuł 21

Wkład finansowy Unii

1. Wkład Unii na pokrycie administracyjnych i operacyjnych kosztów Centrum Kompetencji obejmuje następujące kwoty:

   a) 1 981 668 000 EUR z programu „Cyfrowa Europa”, w tym do wysokości 23 746 000 EUR na pokrycie kosztów administracyjnych;

   b) kwotę pochodzącą z programu „Horyzont Europa”, w tym na pokrycie kosztów administracyjnych, która zostanie określona z uwzględnieniem procesu planowania strategicznego, który zostanie przeprowadzony na podstawie art. 6 ust. 6 rozporządzenia XXX [rozporządzenie w sprawie programu „Horyzont Europa”].

2. Maksymalny wkład Unii wypłaca się ze środków w budżecie ogólnym Unii przeznaczonych na [program „Cyfrowa Europa”] i na program szczegółowy służący realizacji programu „Horyzont Europa”, ustanowiony decyzją XXX.

3. Centrum Kompetencji realizuje działania dotyczące cyberbezpieczeństwa w ramach [programu „Cyfrowa Europa”] oraz [programu „Horyzont Europa”] zgodnie z art. 62 lit. c) ppkt (iv) rozporządzenia (UE, Euratom) XXX[29] [rozporządzenie finansowe].

4. Wkład finansowy Unii nie pokrywa zadań, o których mowa w art. 4 ust. 8 lit. b).

Artykuł 22

Wkład uczestniczących państw członkowskich

1. Uczestniczące państwa członkowskie wnoszą łączny wkład na poczet kosztów operacyjnych i administracyjnych Centrum Kompetencji co najmniej w kwotach, o których mowa w art. 21 ust. 1 niniejszego rozporządzenia.

2. Na potrzeby oszacowania wkładów, o których mowa w art. 23 ust. 1 oraz ust. 3 lit. b) ppkt (ii), koszty ustala się zgodnie z praktykami księgowymi zwyczajowo stosowanymi przez dane państwa członkowskie przy obliczaniu kosztów, standardami rachunkowości obowiązującymi w danym państwie członkowskim, a także obowiązującymi międzynarodowymi standardami rachunkowości oraz międzynarodowymi standardami sprawozdawczości finansowej. Koszty poświadcza niezależny audytor zewnętrzny powołany przez dane państwo członkowskie. Jeżeli poświadczenie budzi jakiekolwiek wątpliwości, Centrum Kompetencji może zweryfikować metodę wyceny.

3. W przypadku gdy uczestniczące państwo członkowskie nie wykonuje swoich zobowiązań dotyczących uzgodnionego wkładu finansowego, dyrektor wykonawczy sporządza pismo w tej sprawie i ustala w nim rozsądny termin, w którym takie niewykonanie zobowiązania ma zostać naprawione. W przypadku gdy niewykonanie zobowiązania nie zostanie naprawione we wskazanym terminie, dyrektor wykonawczy zwołuje posiedzenie Rady Zarządzającej, która podejmuje decyzję, czy uczestniczącemu państwu członkowskiemu, które nie wywiązuje się ze swoich zobowiązań, należy odebrać prawo głosu, bądź czy należy zastosować inne środki do czasu wywiązania się przez nie z zobowiązania. Prawo głosu uczestniczącego państwa członkowskiego, które nie wywiązuje się ze swoich zobowiązań, zawiesza się do czasu wywiązania się z nich.

4. Komisja może zakończyć, w proporcjonalnym stopniu ograniczyć lub zawiesić wypłacanie wkładu finansowego Unii na rzecz Centrum Kompetencji, jeżeli uczestniczące państwa członkowskie nie wnoszą swojego wkładu, o którym mowa w ust. 1, wnoszą go jedynie częściowo lub spóźniają się z jego wniesieniem.

5. Do dnia 31 stycznia każdego roku uczestniczące państwa członkowskie składają Radzie Zarządzającej sprawozdanie na temat wartości wkładów, o których mowa w ust. 1 i które zostały wniesione w każdym poprzednim roku budżetowym.

Artykuł 23

Koszty i zasoby Centrum Kompetencji

[29] [dodać pełny tytuł i odniesienie do Dz.U.]

1. Centrum Kompetencji jest wspólnie finansowane przez Unię i państwa członkowskie za pomocą wkładów finansowych wypłacanych w transzach i wkładów obejmujących koszty poniesione przez krajowe ośrodki koordynacji oraz beneficjentów w związku z realizacją działań, których koszty nie są zwracane przez Centrum Kompetencji.

2. Koszty administracyjne Centrum Kompetencji nie przekraczają [kwota] EUR i są pokrywane z wkładów finansowych podzielonych równo w skali rocznej między Unię i uczestniczące państwa członkowskie. Ewentualna niewykorzystana część wkładu na pokrycie kosztów administracyjnych może zostać przeznaczona na pokrycie kosztów operacyjnych Centrum Kompetencji.

3. Koszty operacyjne Centrum Kompetencji są pokrywane ze środków pochodzących z:

   a) wkładu finansowego Unii;

   b) wkładów uczestniczących państw członkowskich w postaci:

      (i) wkładów finansowych; oraz

      (ii) w stosownych przypadkach wkładów rzeczowych uczestniczących państw członkowskich na pokrycie kosztów poniesionych przez krajowe ośrodki koordynacji oraz beneficjentów w związku z realizacją działań po odliczeniu wkładu Centrum Kompetencji i wszelkich innych wkładów Unii przeznaczonych na pokrycie tych kosztów;

4. Na zasoby uwzględnione w budżecie Centrum Kompetencji składają się następujące wkłady:

   a) wkłady finansowe uczestniczących państw członkowskich na pokrycie kosztów administracyjnych;

   b) wkłady finansowe uczestniczących państw członkowskich na pokrycie kosztów operacyjnych;

   c) wszelkie przychody osiągane przez Centrum Kompetencji;

   d) wszelkie inne wkłady finansowe, zasoby i przychody.

5. Wszelkie odsetki uzyskane z wkładów wypłaconych na rzecz Centrum Kompetencji przez uczestniczące państwa członkowskie uznaje się za jego przychód.

6. Wszystkie zasoby Centrum Kompetencji i jego działania służą osiągnięciu celów określonych w art. 4.

7. Wszystkie aktywa wytworzone przez Centrum Kompetencji lub przekazane mu na potrzeby realizacji jego celów stanowią własność Centrum Kompetencji.

8. Poza przypadkiem likwidacji Centrum Kompetencji na rzecz uczestniczących członków Centrum Kompetencji nie dokonuje się żadnych wypłat ewentualnej nadwyżki przychodów nad wydatkami.

Artykuł 24

Zobowiązania finansowe

Zobowiązania finansowe Centrum Kompetencji nie przekraczają kwoty zasobów finansowych dostępnych w jego budżecie lub zadeklarowanych na rzecz tego budżetu przez jego członków.

Artykuł 25

Rok budżetowy

Rok budżetowy trwa od dnia 1 stycznia do dnia 31 grudnia.

Artykuł 26

Ustanowienie budżetu

1. Każdego roku dyrektor wykonawczy sporządza projekt preliminarza dochodów i wydatków Centrum Kompetencji na następny rok budżetowy oraz przekazuje ten projekt Radzie Zarządzającej wraz z projektem planu zatrudnienia. Dochody i wydatki muszą się równoważyć. Wydatki Centrum Kompetencji obejmują wydatki na personel, administrację, infrastrukturę i działania operacyjne. Wydatki administracyjne utrzymywane są na jak najniższym poziomie.
2. Każdego roku Rada Zarządzająca opracowuje na podstawie projektu preliminarza dochodów i wydatków, o którym mowa w ust. 1, preliminarz dochodów i wydatków Centrum Kompetencji w następnym roku budżetowym.
3. Do dnia 31 stycznia każdego roku Rada Zarządzająca przesyła Komisji preliminarz, o którym mowa w ust. 2, stanowiący część projektu jednolitego dokumentu programowego.
4. Na podstawie tego preliminarza Komisja wprowadza do projektu budżetu Unii przewidywane kwoty, które uważa za niezbędne w związku z planem zatrudnienia, oraz kwotę wkładu, który ma zostać wniesiony z budżetu ogólnego, oraz przedkłada ten projekt Parlamentowi Europejskiemu i Radzie zgodnie z art. 313 i 314 TFUE.
5. Parlament Europejski i Rada zatwierdzają środki przewidziane na wkład na rzecz Centrum Kompetencji.
6. Parlament Europejski i Rada przyjmują plan zatrudnienia Centrum Kompetencji.
7. Rada Zarządzająca przyjmuje budżet Centrum wraz z planem prac. Budżet staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W stosownych przypadkach Rada Zarządzająca dostosowuje budżet i plan prac Centrum Kompetencji zgodnie z budżetem ogólnym Unii.

Artykuł 27

Przedstawienie sprawozdania finansowego Centrum Kompetencji i udzielenie absolutorium

Przedstawienie wstępnego i ostatecznego sprawozdania finansowego Centrum Kompetencji oraz udzielenie absolutorium przebiegają zgodnie z zasadami i terminarzem wynikającymi z rozporządzenia finansowego oraz jego przepisów finansowych przyjętych zgodnie z art. 29.

Artykuł 28

Sprawozdawczość operacyjna i finansowa

1. Dyrektor wykonawczy co roku przekazuje Radzie Zarządzającej sprawozdanie z wykonania swoich obowiązków zgodnie z przepisami finansowymi Centrum Kompetencji.

2. W ciągu dwóch miesięcy od zakończenia każdego roku budżetowego dyrektor wykonawczy przedkłada Radzie Zarządzającej do zatwierdzenia roczne sprawozdanie z działalności dotyczące postępów poczynionych przez Centrum Kompetencji w poprzednim roku kalendarzowym, w szczególności w odniesieniu do planu prac na dany rok. Sprawozdanie to zawiera m.in. informacje dotyczące następujących kwestii:

   a) przeprowadzonych działań operacyjnych i powiązanych wydatków;

   b) proponowanych działań, w tym w podziale na rodzaje uczestników, w tym MŚP, i na państwa członkowskie;

   c) działań wybranych do finansowania, w tym w podziale na rodzaje uczestników, w tym MŚP, i na państwa członkowskie, ze wskazaniem wkładu Centrum Kompetencji na rzecz poszczególnych uczestników i działań;

   d) postępów w kierunku realizacji celów określonych w art. 4 i propozycji dalszych działań niezbędnych do zrealizowania tych celów.

3. Po zatwierdzeniu przez Radę Zarządzającą roczne sprawozdanie z działalności jest podawane do wiadomości publicznej.

Artykuł 29

Przepisy finansowe

Centrum Kompetencji przyjmuje swoje szczegółowe przepisy finansowe zgodnie z art. 70 rozporządzenia XXX [nowe rozporządzenie finansowe].

Artykuł 30

Ochrona interesów finansowych

1. W trakcie realizacji działań finansowanych na podstawie niniejszego rozporządzenia Centrum Kompetencji stosuje odpowiednie środki w celu zapewnienia ochrony interesów finansowych Unii przeciw nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, w drodze skutecznych kontroli oraz, w razie wykrycia nieprawidłowości, w drodze odzyskiwania kwot nienależnie wypłaconych, a także, w stosownych przypadkach, skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych.

2. Centrum Kompetencji zapewnia pracownikom Komisji i innym upoważnionym przez Komisję osobom, a także Trybunałowi Obrachunkowemu, dostęp do swoich obiektów i pomieszczeń oraz do wszelkich informacji, włącznie z informacjami w formacie elektronicznym, niezbędnych do przeprowadzenia ich audytów.

3. Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) może przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu Rady (Euratom, WE) nr 2185/96[30] oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom)

[30] Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2).

nr 883/2013[31], aby ustalić, czy miały miejsce nadużycia finansowe, korupcja lub jakakolwiek inna nielegalna działalność na szkodę interesów finansowych Unii w związku z finansowaniem umowy o udzielenie dotacji lub zamówienia – bezpośrednio lub pośrednio – zgodnie z niniejszym rozporządzeniem.

4. Nie naruszając przepisów ust. 1, 2 i 3 niniejszego artykułu, w zamówieniach i umowach o udzielenie dotacji wynikających z wykonania niniejszego rozporządzenia zamieszcza się postanowienia wyraźnie upoważniające Komisję, Centrum Kompetencji, Trybunał Obrachunkowy i OLAF do prowadzenia takich audytów i dochodzeń zgodnie z ich odpowiednimi uprawnieniami. W przypadku gdy realizację działania zlecono na zewnątrz lub przekazano do podwykonawstwa w całości lub w części lub gdy realizacja działania wymaga udzielenia zamówienia publicznego lub udzielenia wsparcia finansowego osobie trzeciej, w umowie o udzielenie dotacji określa się zobowiązanie wykonawcy lub beneficjenta do uzyskania od każdej zaangażowanej osoby trzeciej wyraźnej akceptacji tych uprawnień Komisji, Centrum Kompetencji, Trybunału Obrachunkowego i OLAF-u.

ROZDZIAŁ IV

PERSONEL CENTRUM KOMPETENCJI

Artykuł 31

Personel

1. Do pracowników Centrum Kompetencji mają zastosowanie: regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Unii Europejskiej określone w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68[32] („regulamin pracowniczy urzędników” i „warunki zatrudnienia”) oraz przepisy przyjęte wspólnie przez instytucje Unii do celów stosowania regulaminu pracowniczego urzędników i warunków zatrudnienia.

2. W odniesieniu do personelu Centrum Kompetencji Rada Zarządzająca korzysta z uprawnień powierzonych organowi powołującemu na podstawie regulaminu pracowniczego oraz z uprawnień powierzonych organowi właściwemu do zawierania umów o pracę na podstawie warunków zatrudnienia („uprawnień organu powołującego”).

3. Zgodnie z art. 110 regulaminu pracowniczego Rada Zarządzająca przyjmuje na podstawie art. 2 ust. 1 regulaminu pracowniczego i art. 6 warunków zatrudnienia decyzję przekazującą odpowiednie uprawnienia organu powołującego dyrektorowi wykonawczemu i określającą warunki, na jakich można zawiesić przekazanie tych uprawnień. Dyrektor wykonawczy jest uprawniony do dalszego przekazywania tych uprawnień.

---

31 Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

32 Rozporządzenie Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiające regulamin pracowniczy urzędników Wspólnot Europejskich i warunki zatrudnienia innych pracowników Wspólnot oraz ustanawiające specjalne środki stosowane tymczasowo wobec urzędników Komisji (Dz.U. L 56 z 4.3.1968, s. 1).

4. Jeżeli wymagają tego szczególne okoliczności, Rada Zarządzająca może w drodze decyzji tymczasowo zawiesić przekazanie uprawnień organu powołującego dyrektorowi wykonawczemu i każde dalsze przekazanie przez niego tych uprawnień. W takich przypadkach Rada Zarządzająca samodzielnie wykonuje uprawnienia organu powołującego lub przekazuje je jednemu ze swoich członków lub też członkowi personelu Centrum Kompetencji innemu niż dyrektor wykonawczy.

5. Rada Zarządzająca przyjmuje odpowiednie przepisy wykonawcze dotyczące regulaminu pracowniczego i warunków zatrudnienia zgodnie z art. 110 regulaminu pracowniczego.

6. Zasoby kadrowe określa się w planie zatrudnienia Centrum Kompetencji, w którym wskazuje się liczbę stanowisk czasowych w podziale na grupy funkcyjne i grupy zaszeregowania oraz liczbę pracowników kontraktowych w przeliczeniu na ekwiwalenty pełnego czasu pracy, zgodnie z rocznym budżetem Centrum Kompetencji.

7. Personel Centrum Kompetencji składa się z personelu zatrudnionego na czas określony i personelu kontraktowego.

8. Centrum Kompetencji ponosi wszystkie koszty związane z pracownikami.

Artykuł 32

Oddelegowani eksperci krajowi i inni pracownicy

1. Centrum Kompetencji może korzystać z pomocy oddelegowanych ekspertów krajowych lub innych pracowników niezatrudnionych przez Centrum Kompetencji.

2. Rada Zarządzająca przyjmuje decyzję określającą zasady oddelegowania ekspertów krajowych do Centrum Kompetencji w porozumieniu z Komisją.

Artykuł 33

Przywileje i immunitety

Do Centrum Kompetencji i jego pracowników zastosowanie ma Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej.

ROZDZIAŁ V
WSPÓLNE PRZEPISY

Artykuł 34

Przepisy bezpieczeństwa

1. Do uczestnictwa we wszystkich działaniach finansowanych przez Centrum Kompetencji ma zastosowanie art. 12 ust. 7 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”].

2. Do działań finansowanych w ramach programu „Horyzont Europa” zastosowanie mają następujące szczególne przepisy bezpieczeństwa:

   a) do celów określonych w art. 34 ust. 1 [Własność i ochrona] rozporządzenia (UE) nr XXX [„Horyzont Europa”], jeżeli przewidziano to w planie prac,

udzielanie licencji niewyłącznych może zostać ograniczone do osób trzecich mających siedzibę lub uznanych za mające siedzibę w państwie członkowskim i znajdujących się pod kontrolą państw członkowskich lub obywateli państw członkowskich;

b) do celów określonych w art. 36 ust. 4 lit. b) [Przeniesienie własności i udzielanie licencji] rozporządzenia (UE) nr XXX [„Horyzont Europa”] przeniesienie własności lub udzielenie licencji na rzecz podmiotu prawnego z siedzibą w państwie stowarzyszonym lub w Unii, ale kontrolowanego z państw trzecich, również stanowi podstawę do zgłoszenia sprzeciwu wobec przeniesienia prawa własności rezultatów lub wobec udzielenia wyłącznej licencji w odniesieniu do rezultatów;

c) do celów określonych w art. 37 ust. 3 lit. a) [Prawa dostępu] rozporządzenia (UE) nr XXX [„Horyzont Europa”], jeżeli przewidziano to w planie prac, udzielanie dostępu do rezultatów i posiadanej istniejącej wiedzy może zostać ograniczone jedynie do podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwie członkowskim i znajdujących się pod kontrolą państw członkowskich lub obywateli państw członkowskich.

Artykuł 35

Przejrzystość

1. Centrum Kompetencji wykonuje swoje działania przy zachowaniu wysokiego stopnia przejrzystości.

2. Centrum Kompetencji zapewnia, aby społeczeństwo i wszelkie inne zainteresowane strony otrzymywały odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników jej pracy. Centrum Kompetencji podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 41.

3. Rada Zarządzająca, działając na wniosek dyrektora wykonawczego, może upoważnić zainteresowane strony do obserwowania przebiegu niektórych działań Centrum Kompetencji.

4. Centrum Kompetencji określa w regulaminie wewnętrznym praktyczne ustalenia w zakresie wdrażania zasad przejrzystości, o których mowa w ust. 1 i 2. W przypadku działań finansowanych w ramach programu „Horyzont Europa” w tym względzie zostaną należycie wzięte pod uwagę przepisy zawarte w załączniku III do rozporządzenia w sprawie programu „Horyzont Europa”.

Artykuł 36

Przepisy bezpieczeństwa w zakresie ochrony informacji niejawnych i szczególnie chronionych informacji jawnych

1. Nie naruszając przepisów art. 35, Centrum Kompetencji nie ujawnia osobom trzecim przetwarzanych lub otrzymywanych przez siebie informacji, w odniesieniu do których w całości lub w części zgłoszono uzasadniony wniosek o zachowanie poufności.

2. Członkowie Rady Zarządzającej, dyrektor wykonawczy, członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych, eksperci zewnętrzni uczestniczący w pracach grup roboczych *ad hoc* oraz członkowie personelu Centrum podlegają

wymogom dotyczącym poufności określonym w art. 339 Traktatu o funkcjonowaniu Unii Europejskiej, nawet po zakończeniu pełnienia swoich obowiązków.

3. Rada Zarządzająca Centrum Kompetencji przyjmuje po zatwierdzeniu przez Komisję przepisy bezpieczeństwa Centrum Kompetencji oparte na zasadach i przepisach zawartych w przepisach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych UE (EUCI) oraz szczególnie chronionych informacji jawnych, w tym między innymi przepisy dotyczące przetwarzania i przechowywania takich informacji określone w decyzjach Komisji (UE, Euratom) 2015/443[33] i 2015/444[34].

4. Centrum Kompetencji może podjąć wszelkie niezbędne środki w celu ułatwienia mającej istotne znaczenie dla jego zadań wymiany informacji z Komisją i państwami członkowskimi oraz, w stosownych przypadkach, z właściwymi agencjami i organami Unii. Wszelkie ustalenia administracyjne poczynione w tym celu w sprawie udostępniania EUCI lub, jeżeli nie ma takiego porozumienia, jakiekolwiek nadzwyczajne doraźne udostępnienie EUCI muszą zostać uprzednio zatwierdzone przez Komisję.

Artykuł 37

Dostęp do dokumentów

1. Do dokumentów będących w posiadaniu Centrum Kompetencji ma zastosowanie rozporządzenie (WE) nr 1049/2001.

2. Rada Zarządzająca przyjmuje ustalenia dotyczące wykonania rozporządzenia (WE) nr 1049/2001 w ciągu sześciu miesięcy od ustanowienia Centrum Kompetencji.

3. Decyzje podjęte przez Centrum Kompetencji na podstawie art. 8 rozporządzenia (WE) nr 1049/2001 mogą być przedmiotem skarg składanych do Europejskiego Rzecznika Praw Obywatelskich na podstawie art. 228 Traktatu o funkcjonowaniu Unii Europejskiej lub skarg wnoszonych do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 Traktatu o funkcjonowaniu Unii Europejskiej.

Artykuł 38

Monitorowanie, ocena i przegląd

1. Centrum Kompetencji zapewnia, aby jego działania, w tym działania zarządzane za pośrednictwem krajowych ośrodków koordynacji i sieci, podlegały stałemu i systematycznemu monitorowaniu i okresowej ocenie. Centrum Kompetencji zapewnia, aby dane dotyczące monitorowania wdrażania i rezultatów programów gromadzono efektywnie, skutecznie i terminowo, a na odbiorców środków unijnych i państwa członkowskie nakłada się proporcjonalne wymogi sprawozdawcze. Wyniki oceny podaje się do publicznej wiadomości.

2. Komisja przeprowadza śródokresową ocenę Centrum Kompetencji po uzyskaniu wystarczających informacji na temat wdrażania niniejszego rozporządzenia, jednak nie później niż w ciągu trzech i pół roku od rozpoczęcia wdrażania niniejszego rozporządzenia. Komisja przygotowuje sprawozdanie z tej oceny i przedkłada to

[33] Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41).

[34] Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

sprawozdanie Parlamentowi Europejskiemu i Radzie do dnia 31 grudnia 2024 r. Centrum Kompetencji i państwa członkowskie dostarczają Komisji informacje niezbędne do przygotowania przedmiotowego sprawozdania.

3. Ocena, o której mowa w ust. 2, obejmuje ocenę rezultatów osiągniętych przez Centrum Kompetencji z uwzględnieniem jego celów, mandatu i zadań. Jeżeli Komisja uzna, że kontynuacja prac Centrum Kompetencji jest uzasadniona pod względem jego założonych celów, mandatu i zadań, może zaproponować przedłużenie mandatu Centrum Kompetencji określonego w art. 46.

4. Na podstawie wniosków z oceny śródokresowej, o której mowa w ust. 2, Komisja może postąpić zgodnie z [art. 22 ust. 5] lub podjąć dowolne inne właściwe działania.

5. Monitorowanie, ocena, stopniowe wycofywanie i odnawianie wkładu finansowego z programu „Horyzont Europa" przebiega zgodnie z przepisami zawartymi w art. 8, 45 i 47 oraz w załączniku III do rozporządzenia w sprawie programu „Horyzont Europa" oraz z uzgodnionym trybem realizacji.

6. Monitorowanie i ocena wkładu z programu „Cyfrowa Europa" oraz sprawozdawczość w tym zakresie podlegają przepisom zawartym w art. 24 i 25 programu „Cyfrowa Europa".

7. W przypadku likwidacji Centrum Kompetencji Komisja przeprowadza ocenę końcową Centrum Kompetencji w ciągu sześciu miesięcy od likwidacji Centrum Kompetencji, ale nie później niż po upływie dwóch lat od uruchomienia procedury likwidacji, o której mowa w art. 46 niniejszego rozporządzenia. Wnioski z tej oceny końcowej przedstawia się Parlamentowi Europejskiemu i Radzie.

Artykuł 39

Odpowiedzialność Centrum Kompetencji

1. Odpowiedzialność umowną Centrum Kompetencji reguluje prawo właściwe dla danej umowy, decyzji lub danego zamówienia.

2. W zakresie odpowiedzialności pozaumownej Centrum Kompetencji naprawia szkody wyrządzone przez swoich pracowników podczas wykonywania przez nich obowiązków służbowych, zgodnie z ogólnymi zasadami wspólnymi dla systemów prawnych państw członkowskich.

3. Wszelkie wypłaty dokonywane przez Centrum Kompetencji z tytułu odpowiedzialności, o której mowa w ust. 1 i 2, a także poniesione w związku z tym koszty i wydatki, uznaje się za wydatki Centrum Kompetencji i pokrywa się z jego środków.

4. Centrum Kompetencji ponosi wyłączną odpowiedzialność za swoje zobowiązania.

Artykuł 40

Właściwość Trybunału Sprawiedliwości Unii Europejskiej i prawo właściwe

1. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy:

   1) na podstawie wszelkich klauzul arbitrażowych zamieszczonych w umowach lub kontraktach zawieranych przez Centrum Kompetencji lub decyzjach przez nie podejmowanych;

2) w sporach dotyczących odszkodowań za szkody wyrządzone przez pracowników Centrum Kompetencji podczas wykonywania przez nich obowiązków służbowych;

3) w sporach między Centrum Kompetencji a członkami jego personelu w granicach i przy zachowaniu warunków określonych w regulaminie pracowniczym.

2. W odniesieniu do wszelkich kwestii nieobjętych przepisami niniejszego rozporządzenia lub innymi aktami prawnymi Unii zastosowanie ma prawo państwa członkowskiego, w którym znajduje się siedziba Centrum Kompetencji.

Artykuł 41

Odpowiedzialność członków i ubezpieczenie

1. Odpowiedzialność finansowa członków za długi Centrum Kompetencji jest ograniczona do kwoty już wniesionych przez nich wkładów na poczet kosztów administracyjnych.

2. Centrum Kompetencji zawiera i podtrzymuje odpowiednie umowy ubezpieczeniowe.

Artykuł 42

Konflikty interesów

Rada Zarządzająca Centrum Kompetencji przyjmuje zasady, których celem jest zapobieganie konfliktom interesów i zarządzanie nimi w odniesieniu do członków, organów i personelu Centrum Kompetencji. Zasady te zawierają przepisy służące unikaniu konfliktów interesów przez przedstawicieli członków pełniących obowiązki w Radzie Zarządzającej oraz w Radzie Konsultacyjnej ds. Przemysłowych i Naukowych zgodnie z rozporządzeniem XXX [nowe rozporządzenie finansowe].

Artykuł 43

Ochrona danych osobowych

1. Przetwarzanie danych osobowych przez Centrum Kompetencji podlega przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018.

2. Rada Zarządzająca przyjmuje środki wykonawcze, o których mowa w art. xx ust. 3 rozporządzenia (UE) nr XXX/2018. Rada Zarządzająca może przyjąć dodatkowe środki niezbędne do stosowania przez Centrum Kompetencji rozporządzenia (UE) nr XXX/2018.

Artykuł 44

Wsparcie ze strony przyjmującego państwa członkowskiego

Centrum Kompetencji i państwo członkowskie [Belgia], w którym znajduje się jego siedziba, mogą dokonać ustaleń administracyjnych w sprawie przywilejów i immunitetów oraz innego wsparcia udzielanego Centrum Kompetencji przez to państwo członkowskie.

ROZDZIAŁ VII

PRZEPISY KOŃCOWE

Artykuł 45

Początek funkcjonowania

1. Komisja odpowiada za ustanowienie Centrum Kompetencji i jego początkowe funkcjonowanie do momentu osiągnięcia przez nie zdolności operacyjnej do wykonywania własnego budżetu. Zgodnie z prawem Unii Komisja przeprowadza wszystkie niezbędne działania przy pomocy właściwych organów Centrum Kompetencji.

2. Do celów określonych w ust. 1, do czasu objęcia obowiązków przez dyrektora wykonawczego w wyniku mianowania go przez Radę Zarządzającą zgodnie z art. 16, Komisja może wyznaczyć tymczasowego dyrektora wykonawczego i wykonywać obowiązki powierzone dyrektorowi wykonawczemu, któremu może pomagać ograniczona liczba urzędników Komisji. Komisja może tymczasowo wyznaczyć ograniczoną liczbę swoich urzędników.

3. Tymczasowy dyrektor wykonawczy może zatwierdzać wszelkie płatności w ramach środków przydzielonych w rocznym budżecie Centrum Kompetencji po zatwierdzeniu przez Radę Zarządzającą oraz może podejmować decyzje, udzielać zamówień i zawierać umowy, w tym umowy o pracę po przyjęciu planu zatrudnienia Centrum Kompetencji.

4. Tymczasowy dyrektor wykonawczy — w porozumieniu z dyrektorem wykonawczym Centrum Kompetencji i za zgodą Rady Zarządzającej — określa datę uzyskania przez Centrum Kompetencji zdolności do wykonywania własnego budżetu. Począwszy od tej daty, Komisja przestaje podejmować zobowiązania i dokonywać płatności z tytułu działań Centrum Kompetencji.

Artykuł 46

Czas trwania

1. Centrum Kompetencji ustanawia się na okres od dnia 1 stycznia 2021 r. do dnia 31 grudnia 2029 r.

2. Pod koniec tego okresu, o ile w drodze przeglądu niniejszego rozporządzenia nie postanowiono inaczej, wszczyna się procedurę likwidacji. Procedurę likwidacji wszczyna się automatycznie, jeśli Unia lub wszystkie uczestniczące państwa członkowskie wystąpią z Centrum Kompetencji.

3. Do celów przeprowadzenia postępowania mającego na celu likwidację Centrum Kompetencji, Rada Zarządzająca wyznacza co najmniej jednego likwidatora, który działa zgodnie z jej decyzjami.

4. W ramach likwidacji Centrum Kompetencji jego aktywa wykorzystuje się do pokrycia jego zobowiązań oraz wydatków związanych z jego likwidacją. Wszelką nadwyżkę rozdziela się między Unię oraz uczestniczące państwa członkowskie proporcjonalnie do ich wkładu finansowego na rzecz Centrum Kompetencji. Każda taka nadwyżka przydzielona Unii jest zwracana do budżetu Unii.

Artykuł 47

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cel(e)

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Okres trwania wniosku/inicjatywy i wpływ finansowy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Rozporządzenie ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[35]

Badania naukowe i innowacje

Europejskie inwestycje strategiczne

1.3. Charakter wniosku/inicjatywy

☒Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[36]

☐ Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cel(e)

1.4.1. Wieloletnie cele strategiczne Komisji wskazane we wniosku/inicjatywie

1. Połączony jednolity rynek cyfrowy

2. Pobudzenie zatrudnienia, wzrostu i inwestycji

1.4.2. Cele szczegółowe, których dotyczy wniosek/inicjatywa

Cele szczegółowe

1.3 Gospodarka cyfrowa może osiągnąć swój pełny potencjał opierający się na inicjatywach umożliwiających pełen rozwój technologii cyfrowych i technologii dotyczących danych.

2.1 Europa utrzymuje swoją pozycję światowego lidera gospodarki cyfrowej, dzięki której europejskie przedsiębiorstwa mogą rozwijać się na skalę ogólnoświatową, opierając się na silnej przedsiębiorczości cyfrowej i prowadzących działalność przedsiębiorstwach typu start-up, i dzięki której przemysł i usługi publiczne opanowują transformację cyfrową.

2.2. Europejskie środowiska naukowe dostrzegają możliwości inwestycyjne w odniesieniu do potencjalnych technologicznych przełomów i inicjatyw przewodnich, w szczególności programu „Horyzont 2020”/„Horyzont Europa” oraz wykorzystywania partnerstw publiczno-prywatnych.

---

[35] ABM: *activity-based management:* zarządzanie kosztami działań; ABB: *activity-based budgeting:* budżet zadaniowy.

[36] O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Centrum Kompetencji wraz z siecią i środowiskiem posiadającym kompetencje w dziedzinie cyberbezpieczeństwa będzie dążyć do realizacji następujących celów:

1) wnoszenie wkładu we wdrażanie części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa" ustanowionego rozporządzeniem nr XXX, w szczególności działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa"], oraz programu „Horyzont Europa" ustanowionego rozporządzeniem nr XXX, w szczególności z pkt 2.2.6 załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa", oraz innych unijnych programów, jeżeli przewidziano to w aktach prawnych Unii;

2) poszerzanie możliwości i wiedzy oraz ulepszanie infrastruktury w zakresie cyberbezpieczeństwa z korzyścią dla gałęzi przemysłu, sektora publicznego i środowisk naukowych;

3) wnoszenie wkładu w powszechne wdrażanie w całej gospodarce najnowocześniejszych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa;

4) lepsze zrozumienie kwestii cyberbezpieczeństwa i przyczynienie się do ograniczania niedoborów kwalifikacji w dziedzinie cyberbezpieczeństwa w Unii;

5) przyczynianie się do wzmacniania badań naukowych i rozwoju w dziedzinie cyberbezpieczeństwa w Unii;

6) zacieśnienie współpracy między kręgami cywilnym i obronnym w odniesieniu do technologii i aplikacji podwójnego zastosowania;

7) zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa;

8) pomoc w zakresie koordynacji i ułatwienia pracy sieci krajowych ośrodków koordynacji („sieć"), o której mowa w art. 10, oraz środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, o którym mowa w art. 12.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

· Liczba infrastruktur/narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień.

· Zapewnienie europejskim naukowcom i europejskiemu przemysłowi czasu na prowadzenie badań i eksperymentów w całej sieci oraz w ramach Centrum. W przypadku istniejącej infrastruktury zwiększenie liczby godzin dostępnej dla tych środowisk w stosunku do liczby godzin dostępnej obecnie.

· Wzrost liczby obsłużonych społeczności użytkowników oraz liczby naukowców, którzy uzyskali dostęp do europejskiej infrastruktury z zakresu cyberbezpieczeństwa, w stosunku do liczby tych społeczności i naukowców, którzy muszą szukać takich zasobów poza Europą.

· Początek wzrostu konkurencyjności europejskich dostawców mierzonej w kategoriach udziału w rynku światowym (docelowy udział w rynku do 2027 r. to 25 %) oraz w kategoriach wielkości udziału wyników europejskich badań naukowych i innowacji wykorzystanych przez przemysł.

· Wniesienie wkładu w rozwój nowych technologii z zakresu cyberbezpieczeństwa, mierzonego w kategoriach praw autorskich, patentów, publikacji naukowych i produktów komercyjnych.

· Liczba ocenionych i ujednoliconych programów nauczania umiejętności z zakresu cyberbezpieczeństwa, liczba ocenionych programów profesjonalnej certyfikacji w dziedzinie cyberbezpieczeństwa.

· Liczba wyszkolonych naukowców, studentów, użytkowników (z sektora przemysłu i administracji publicznej).

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej

Osiągnięcie masy krytycznej inwestycji w technologiczny i przemysłowy rozwój cyberbezpieczeństwa oraz przezwyciężenie fragmentacji istotnych zdolności rozproszonych w całej UE.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

Cyberbezpieczeństwo jest przedmiotem wspólnego zainteresowania Unii, co potwierdzono we wspomnianych powyżej konkluzjach Rady. Przykładami są skala i transgraniczny charakter incydentów, takich jak ataki za pomocą oprogramowania WannaCry lub NonPetya. Charakter i skala wyzwań technologicznych dotyczących cyberbezpieczeństwa, jak również niewystarczająca koordynacja wysiłków w ramach przemysłu, sektora publicznego i środowisk naukowych oraz pomiędzy nimi wymaga, aby UE w dalszym ciągu wpierała wysiłki koordynacyjne zarówno w celu zgromadzenia krytycznej masy zasobów, jak i zapewnienia lepszego zarządzania wiedzą i aktywami. Jest to konieczne z uwagi na wymogi w zakresie zasobów powiązane z określonymi możliwościami dotyczącymi badań naukowych, rozwoju i wdrażania cyberbezpieczeństwa; konieczność zapewnienia dostępu do interdyscyplinarnej wiedzy eksperckiej z dziedziny cyberbezpieczeństwa między różnymi dyscyplinami (często jedynie częściowo dostępnej na poziomie krajowym); globalny charakter przemysłowych łańcuchów wartości oraz światowych konkurentów działających na wielu rynkach.

Wymaga to zasobów i wiedzy fachowej w skali, którą trudno osiągnąć w wyniku indywidualnego działania któregokolwiek państwa członkowskiego. Na przykład ogólnoeuropejska komunikacyjna sieć kwantowa może wymagać ze strony UE inwestycji w wysokości około 900 mln EUR, w zależności od inwestycji państw członkowskich (które mają zostać wzajemnie połączone/uzupełnione) oraz stopnia, w jakim technologia umożliwi ponowne wykorzystanie istniejącej infrastruktury.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Ocena okresowa programu „Horyzont 2020” potwierdziła m.in., że wsparcie ze strony UE na rzecz badań naukowych i rozwoju oraz wyzwań społecznych jest nadal istotne (wśród tych wyzwań znajdują się „bezpieczne społeczeństwa”, w ramach których wspiera się badania naukowe i rozwój w obszarze cyberbezpieczeństwa). Jednocześnie wyniki oceny potwierdzają, że wzmocnienie wiodącej pozycji w przemyśle pozostaje wyzwaniem, oraz że nadal istnieje luka innowacyjna, a UE pozostaje w tyle pod względem przełomowych innowacji tworzących rynki.

Wydaje się, że ocena śródokresowa instrumentu „Łącząc Europę” potwierdza wartość dodaną interwencji UE wykraczającej poza badania naukowe i rozwój,

aczkolwiek w przypadku cyberbezpieczeństwa w ramach instrumentu „Łącząc Europę” nacisk kładziono na nieco inną kwestię (bezpieczeństwo operacyjne sieci) i logika interwencji była nieco inna. Jednocześnie większość odbiorców dotacji dotyczących cyberbezpieczeństwa w ramach instrumentu „Łącząc Europę” – środowisko krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego – wyraziła życzenie, aby w ramach kolejnych WRF powstał odpowiednio dostosowany program wsparcia.

Stworzenie w 2016 r. partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w Unii było znaczącym pierwszym krokiem w kierunku skupienia środowisk naukowych, przemysłu i sektora publicznego, aby ułatwić prowadzenie badań i wprowadzanie innowacji w dziedzinie cyberbezpieczeństwa, co w ramach finansowych na lata 2014–2020 powinno przynieść dobre, bardziej konkretne efekty w zakresie badań i innowacji. Umożliwiło to partnerom przemysłowym podjęcie zobowiązania dotyczącego ich indywidualnych wydatków w dziedzinach określonych w strategicznym planie badań i innowacji w ramach tego partnerstwa.

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia

Sieć kompetencji w dziedzinie cyberbezpieczeństwa oraz Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będą zapewniały dodatkowe wsparcie na rzecz istniejących przepisów obowiązujących w obszarze polityki cyberbezpieczeństwa i podmiotów w tym obszarze. Mandat Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie miał charakter komplementarny względem wysiłków Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), ale w jego przypadku nacisk położony będzie na inne kwestie i wymagany będzie inny zestaw umiejętności. Chociaż Agencja ma do odegrania rolę polegającą na doradztwie w zakresie badań i innowacji w dziedzinie cyberbezpieczeństwa w UE, proponowany mandat dotyczy przede wszystkim innych zadań, które mają decydujące znaczenie dla wzmacniania odporności UE w zakresie cyberbezpieczeństwa. Centrum powinno pobudzać rozwój technologii w dziedzinie cyberbezpieczeństwa i jej wdrażanie oraz uzupełniać budowanie zdolności w tym obszarze na szczeblu unijnym i krajowym.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią kompetencji w dziedzinie cyberbezpieczeństwa będzie również działało na rzecz wspierania badań, aby ułatwić i przyspieszyć procesy standaryzacji i certyfikacji, w szczególności związane z systemami certyfikacji cyberbezpieczeństwa w rozumieniu aktu w sprawie cyberbezpieczeństwa.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie działać jako jednolity mechanizm wdrażający dwa europejskie programy wpierające cyberbezpieczeństwo (programy „Cyfrowa Europa” i „Horyzont Europa”) i przyczyniać się do zwiększenia spójności i synergii między tymi programami.

Inicjatywa ta umożliwia uzupełnienie wysiłków państw członkowskich dzięki zapewnianiu odpowiednich informacji decydentom w obszarze edukacji w celu poprawy edukacji w zakresie cyberbezpieczeństwa (np. dzięki opracowaniu programów z zakresu cyberbezpieczeństwa w ramach cywilnych i wojskowych systemów edukacji, a także informacji na potrzeby podstawowej edukacji w zakresie

cyberbezpieczeństwa). Inicjatywa umożliwiłaby również wsparcie ujednolicenia i stałej oceny profesjonalnych programów certyfikacji w dziedzinie cyberbezpieczeństwa – wszystkich niezbędnych działań mających na celu łatwiejsze wyeliminowanie niedoboru kwalifikacji w zakresie cyberbezpieczeństwa oraz ułatwienie dostępu gałęziom przemysłu i pozostałym środowiskom do ekspertów z dziedziny cyberbezpieczeństwa. Ujednolicenie edukacji i umiejętności ułatwi wykształcenie w UE wykwalifikowanej siły roboczej w zakresie cyberbezpieczeństwa, stanowiącej kluczowy zasób dla przedsiębiorstw z obszaru cyberbezpieczeństwa, a także innych branż zainteresowanych cyberbezpieczeństwem.

1.6. Okres trwania wniosku/inicjatywy i wpływ finansowy

☒ Wniosek/inicjatywa o **ograniczonym okresie trwania**

– ☒ Okres trwania wniosku/inicjatywy: od 1.01.2021 r. do 31.12.2029 r.

– ☒ Okres trwania wpływu finansowego: od 2021 r. do 2027 r. w odniesieniu do środków na zobowiązania oraz od 2021 r. do 2031 r. w odniesieniu do środków na płatności.

☐ Wniosek/inicjatywa o **nieograniczonym okresie trwania**

– Wprowadzenie w życie z okresem rozruchu od RRRR r. do RRRR r.,

– po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[37]

☐ **Bezpośrednie zarządzanie** przez Komisję

– ☐ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze;

☐ **Zarządzanie dzielone** z państwami członkowskimi

☒

Zarządzanie pośrednie poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☒ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

[37] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Szczegółowe przepisy dotyczące nadzoru i sprawozdawczości określono w art. 28.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Abu ograniczyć ryzyko związane z funkcjonowaniem Centrum Kompetencji po jego ustanowieniu oraz opóźnienia, Komisja będzie wspierać Centrum Kompetencji na tym etapie, aby zapewnić szybkie zatrudnienie podstawowego personelu oraz opracowanie skutecznego wewnętrznego systemu kontroli i prawidłowych procedur.

2.2.2. Informacje dotyczące struktury wewnętrznego systemu kontroli

Dyrektor wykonawczy jest odpowiedzialny za działalność Centrum Kompetencji i za bieżące zarządzanie nim oraz pełni funkcję jego przedstawiciela prawnego. Dyrektor jest odpowiedzialny przed Radą Zarządzającą, której na bieżąco przekazuje informacje o działalności Centrum Kompetencji. Rada Zarządzająca ponosi ogólną odpowiedzialność za strategiczną orientację i operacje Centrum Kompetencji oraz nadzoruje realizację jego działalności. Przepisy finansowe mające zastosowanie do Centrum Kompetencji są przyjmowane przez Radę Zarządzającą po konsultacji z Komisją. Przepisy te nie mogą odbiegać od przepisów rozporządzenia (UE) nr 1271/2013, chyba że takie różnice są szczególnie wymagane w przypadku funkcjonowania Centrum Kompetencji, a Komisja wydała na nie uprzednią zgodę. Audytor wewnętrzny Komisji wykonuje w stosunku do Centrum Kompetencji te same uprawnienia co w stosunku do Komisji. Trybunał Obrachunkowy jest uprawniony do kontroli, na podstawie dokumentacji i na miejscu, wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymują od Centrum Kompetencji środki unijne.

2.2.3. Oszacowanie kosztów i korzyści wynikających z kontroli i ocena prawdopodobnego ryzyka błędu

Koszty i korzyści wynikające z kontroli Koszty kontroli w przypadku Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych dzielą się na koszt nadzoru na poziomie Komisji oraz koszt kontroli operacyjnej na poziomie organu wdrażającego. Koszt kontroli na poziomie Centrum Kompetencji szacuje się na około 1,19 % operacyjnych środków na płatności realizowanych na poziomie Centrum Kompetencji. Koszt nadzoru na poziomie Komisji szacuje się na około 1,20 % operacyjnych środków na płatności realizowanych na poziomie Centrum Kompetencji. Zakładając, że działania byłyby w pełni zarządzane przez Komisję bez wsparcia ze strony organu wdrażającego, koszt kontroli byłby znacznie wyższy i mógłby wynieść około 7,7 % środków na płatności.

Przewidziane kontrole mają na celu zapewnienie sprawnego i skutecznego nadzoru Komisji nad podmiotami realizującymi program oraz zapewnienie niezbędnego poziomu pewności na poziomie Komisji.

Korzyści wynikające z kontroli są następujące:

- niedopuszczenie do wyboru słabszych lub nieodpowiednich wniosków,
- optymalizacja planowania i wykorzystania unijnych środków w celu utrzymania unijnej wartości dodanej,
- zapewnienie jakości umów o udzielenie dotacji, uniknięcie błędów przy określaniu podmiotów prawnych, zapewnienie prawidłowego obliczania wkładu UE i pozyskanie koniecznych gwarancji dla prawidłowego funkcjonowania dotacji,
- wykrywanie kosztów niekwalifikowalnych na etapie płatności,
- wykrywanie błędów mających wpływ na legalność i prawidłowość działań na etapie audytu.

Szacowany poziom błędu

Celem jest utrzymanie poziomu błędu resztowego poniżej progu wynoszącego 2 % dla całego programu, przy jednoczesnym ograniczeniu obciążenia beneficjentów kontrolami w celu osiągnięcia właściwej równowagi między celem w zakresie legalności i prawidłowości a innymi celami, takimi jak atrakcyjność programu, w szczególności dla MŚP, oraz kosztami kontroli.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

OLAF może przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu Parlamentu Europejskiego i Rady nr 883/2013 oraz w rozporządzeniu Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Unii przed nadużyciami finansowymi i innymi nieprawidłowościami, aby ustalić, czy miały miejsce nadużycia finansowe, korupcja lub jakakolwiek inna nielegalna działalność na szkodę interesów finansowych Unii w związku z dokonywanym przez Centrum Kompetencji finansowaniem dotacji lub umowy.

Umowy, decyzje i zamówienia wynikające z wdrożenia niniejszego rozporządzenia zawierają postanowienia wyraźnie upoważniające Komisję, Centrum Kompetencji, Trybunał Obrachunkowy oraz OLAF do przeprowadzania audytów i dochodzeń, zgodnie z przysługującymi im kompetencjami.

Centrum Kompetencji zapewnia należytą ochronę interesów finansowych swoich członków, prowadząc lub zlecając odpowiednie kontrole wewnętrzne i zewnętrzne.

Centrum Kompetencji przystępuje do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich, dotyczącego dochodzeń wewnętrznych

prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF). Centrum Kompetencji przyjmuje środki niezbędne do ułatwienia prowadzenia dochodzeń wewnętrznych przez OLAF.

Centrum Kompetencji przyjmie strategię zwalczania nadużyć finansowych w oparciu o analizę ryzyka nadużyć finansowych i stosunek kosztów do korzyści. Centrum Kompetencji chroni interesy finansowe Unii poprzez stosowanie środków zapobiegających nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, za pomocą skutecznych kontroli, a w przypadku wykrycia nieprawidłowości – poprzez odzyskanie nienależnie wypłaconych kwot, oraz w stosownych przypadkach poprzez skuteczne, proporcjonalne i odstraszające kary administracyjne i finansowe;

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział wieloletnich ram finansowych i proponowane nowe linie budżetowe po stronie wydatków

- Nowe linie budżetowe, o których utworzenie się wnioskuje

  Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj wydatków	Wkład			
	Numer	Zróżn. / niezróżn.[38]	państw EFTA[39]	państw kandydujących[40]	państw trzecich	w rozumieniu art. [21 ust. 2 lit. b)] rozporządzenia finansowego
Dział 1: Jednolity rynek, innowacje i gospodarka cyfrowa	01 02 XX XX „Horyzont Europa”: Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych – wydatki na wsparcie 01 02 XX XX „Horyzont Europa”: Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych 02 06 01 XX Program „Cyfrowa Europa”: Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych – wydatki na wsparcie 02 06 01 XX Program „Cyfrowa Europa”: Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań	Zróżn.	TAK	TAK (jeżeli określono w rocznym programie prac)	TAK (ograniczony do pewnych części programu)	NIE

[38] Zróżn. = środki zróżnicowane / niezróżn. = środki niezróżnicowane.

[39] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

[40] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

	Naukowych					

- Wkład do tych linii budżetowych ma pochodzić z następujących działów:

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa	Rok 2021	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**Ogółem**
01 01 01 01 Wydatki związane z urzędnikami, pracownikami zatrudnionymi na czas określony, zajmujących się dziedziną badań naukowych – „Horyzont Europa”	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Personel zewnętrzny wdrażający programy badawcze – „Horyzont Europa”	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Inne wydatki na zarządzanie w zakresie badań naukowych – „Horyzont Europa”	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globalne wyzwania i konkurencyjność przemysłowa	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Wsparcie administracyjne – program „Cyfrowa Europa”	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cyberbezpieczeństwo – program „Cyfrowa Europa”	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Wydatki ogółem	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

W trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo” filaru II „Globalne wyzwania i konkurencyjność przemysłowa” programu „Horyzont Europa” (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 21 ust. 1 lit. b). Wniosek będzie opierał się

na wynikach procesu planowania strategicznego określonego w art. 6 ust. 6 rozporządzenia XXX [program ramowy „Horyzont Europa”].

Powyższe kwoty nie obejmują wkładu państw członkowskich w operacyjne i administracyjne koszty Centrum Kompetencji współmiernego do wkładu finansowego Unii.

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	**1**	Jednolity rynek, innowacje i gospodarka cyfrowa

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po 2027***	**OGÓŁEM**
Tytuł 1 (Wydatki na personel)	Środki na zobowiązania = środki na płatności	1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Tytuł 2 (Infrastruktura i wydatki operacyjne)	Środki na zobowiązania = środki na płatności	2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Tytuł 3 (Wydatki operacyjne)	Środki na zobowiązania	3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Środki na płatności	4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
OGÓŁEM środki przydzielone na	Środki na	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] Środki na personel są wyliczone jedynie w odniesieniu do połowy roku w 2021 r.

programy[42]	zobowiązania										
	Środki na płatności	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] Całkowite określone środki dotyczą jedynie środków finansowych UE przeznaczonych na cyberbezpieczeństwo w ramach programu „Cyfrowa Europa". W trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo" filaru II „Globalne wyzwania i konkurencyjność przemysłowa" programu „Horyzont Europa" (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 5 ust. 1 lit. b). Wniosek będzie opierał się na wynikach procesu planowania strategicznego określonego w art. 6 ust. 6 rozporządzenia XXX [program ramowy „Horyzont Europa"].

Dział wieloletnich ram finansowych	7	„Wydatki administracyjne”

w mln EUR (do trzech miejsc po przecinku)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po 2027***	**OGÓŁEM**
Zasoby ludzkie		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Pozostałe wydatki administracyjne		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

w mln EUR (do trzech miejsc po przecinku)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po 2027***	**OGÓŁEM**
OGÓŁEM środki z wszystkich DZIAŁÓW wieloletnich ram finansowych	Środki na zobowiązania	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Środki na płatności	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 [2]061,715**	**2 005,637**

3.2.2. Podsumowanie szacunkowego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☒ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

Rok	2021	2022	2023	2024	2025	2026	2027	OGÓŁEM
DZIAŁ 7 wieloletnich ram finansowych								
Zasoby ludzkie	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Pozostałe wydatki administracyjne	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

poza DZIAŁEM 7[43] wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki administracyjne	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

OGÓŁEM	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Powyższe środki potrzebne na pokrycie wydatków na zasoby ludzkie i innych wydatków administracyjnych nieujętych w Dziale 7 odpowiadają kwotom pokrytym w ramach wkładu finansowego Unii z programu „Cyfrowa Europa".

Środki potrzebne na pokrycie wydatków na zasoby ludzkie i innych wydatków administracyjnych nieujętych w Dziale 7 zostaną zwiększone o kwoty pokryte z wkładu finansowego Unii z programu „Horyzont Europa", kiedy Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo" filaru II „Globalne wyzwania i konkurencyjność przemysłowa" programu „Horyzont Europa" (całkowita pula to 2 800 000 000 EUR), o którym

[43] Pomoc techniczna lub administracyjna oraz wydatki na wsparcie w zakresie wdrażania programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

mowa w art. 21 ust. 1 lit. b), podczas procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego.

Powyższe kwoty środków na pokrycie wydatków na zasoby ludzkie i innych wydatków administracyjnych nieujętych w Dziale 7 nie obejmują wkładu państw członkowskich w koszty administracyjne Centrum Kompetencji współmiernego do wkładu finansowego Unii.

3.2.2.1. Szacowane zapotrzebowanie na zasoby ludzkie w Komisji

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

– ■ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

Rok		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
W centrali i w biurach przedstawicielstw Komisji		20	21	21	21	21	21	22
W delegaturach								
Badania naukowe								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC) – CA, LA, SNE, INT i JED [44] Dział 7								
Finansowanie z DZIAŁU 7 wieloletnich ram finansowych	– w centrali	3	3	3	3	3	3	3
	– w delegaturach							
Finansowanie ze środków przydzielonych na program [45]	– w centrali							
	– w delegaturach							
Badania naukowe								
Inne (wyszczególnić)								
OGÓŁEM		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Koordynacja zadań powierzonych Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, ich monitorowanie i kierowanie nimi, w tym koszty wsparcia i koordynacji. Rozwój i koordynacja polityki w dziedzinie cyberbezpieczeństwa w związku z zadaniami powierzonymi Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, np. w odniesieniu do określania priorytetów dotyczących polityki w zakresie badań naukowych i przemysłu, ogólnej współpracy między państwami członkowskimi i podmiotami gospodarczymi, spójności z przyszłymi unijnymi ramami certyfikacji w dziedzinie cyberbezpieczeństwa, pracy nad odpowiedzialnością i należytą starannością lub koordynacji z politykami dotyczącymi HPC, sztucznej inteligencji i umiejętności cyfrowych. .

[44] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

[45] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

Personel zewnętrzny	Koordynacja zadań powierzonych Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, ich monitorowanie i kierowanie nimi, w tym koszty wsparcia i koordynacji. Rozwój i koordynacja polityki w dziedzinie cyberbezpieczeństwa w związku z zadaniami powierzonymi Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, np. w odniesieniu do określania priorytetów dotyczących polityki w zakresie badań naukowych i przemysłu, ogólnej współpracy między państwami członkowskimi i podmiotami gospodarczymi, spójności z przyszłymi unijnymi ramami certyfikacji w dziedzinie cyberbezpieczeństwa, pracy nad odpowiedzialnością i należytą starannością lub koordynacji z politykami dotyczącymi HPC, sztucznej inteligencji i umiejętności cyfrowych. .

3.2.2.2. Szacowane zapotrzebowanie na zasoby ludzkie w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych

	2021	2022	2023	2024	2025	2026	2027
Urzędnicy Komisji							
z czego grupa funkcyjna AD							
z czego grupa funkcyjna AST							
z czego grupa funkcyjna AST-SC							
Personel zatrudniony na czas określony							
z czego grupa funkcyjna AD	10	11	13	13	13	13	13
z czego grupa funkcyjna AST							
z czego grupa funkcyjna AST-SC							
Personel kontraktowy	26	32	39	39	39	39	39
Oddelegowani eksperci krajowi (SNE)	1	1	1	1	1	1	1
Ogółem	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Operacyjna realizacja zadań powierzonych Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych zgodnie z art. 4 niniejszego rozporządzenia, w tym koszty wsparcia i koordynacji.
Personel zewnętrzny	Operacyjna realizacja zadań powierzonych Europejskiemu Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych zgodnie z art. 4 niniejszego rozporządzenia, w tym koszty wsparcia i koordynacji.

Powyższe szacowane zapotrzebowanie na zasoby ludzkie w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych odpowiada szacowanemu zapotrzebowaniu na wdrażanie wsparcia finansowego Unii w ramach programu „Cyfrowa Europa”.

Powyższe szacowane zapotrzebowanie na zasoby ludzkie w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych zostanie podniesione o szacowane zapotrzebowanie na wdrażanie

wsparcia finansowego Unii w ramach programu „Horyzont Europa”, kiedy w trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo” filaru II „Globalne wyzwania i konkurencyjność przemysłowa” programu „Horyzont Europa” (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 21 ust. 1 lit. b).

3.2.2.3. Plan zatrudnienia Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych

Grupa funkcyjna i grupa zaszeregowania	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Ogółem AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							

AST 1							
Ogółem AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Ogółem AST/SC							
SUMA CAŁKOWITA	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Szacunkowy wpływ personelu (dodatkowego) – personel zewnętrzny Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych

Personel kontraktowy	2021	2022	2023	2024	2025	2026	2027
Grupa funkcyjna IV	20	22	29	29	29	29	29
Grupa funkcyjna III	2	4	4	4	4	4	4
Grupa funkcyjna II	4	6	6	6	6	6	6
Grupa funkcyjna I							
Ogółem	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Aby zapewnić stabilną liczbę osób zatrudnionych, liczba dodatkowego personelu w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych zostanie częściowo zrównoważona ograniczeniem liczby urzędników i personelu zewnętrznego (tj. obecny plan zatrudnienia i personel zewnętrzny) w odpowiednich służbach Komisji.

Liczba pracowników Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych w pkt 3.2.2.2–4 zostanie skompensowana w następujący sposób[46]:

OGÓŁEM	2021	2022	2023	2024	2025	2026	2027

[46] Z zastrzeżeniem ostatecznej kwoty budżetu, którego wykonanie zostanie powierzone Centrum Kompetencji.

Urzędnicy Komisji	5	5	6	6	6	6	6
Personel zatrudniony na czas określony							
Personel kontraktowy	14	17	20	20	20	20	20
Oddelegowani eksperci krajowi (SNE)							
Ogółem ekwiwalenty pełnego czasu pracy	19	22	26	26	26	26	26
Liczba osób zatrudnionych	19	22	26	26	26	26	26

Kompensacja zasobów ludzkich w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych będzie współmierna do udziału wsparcia finansowego Unii, tj. 50 %.

Powyższa kompensacja odnosi się do szacowanego zapotrzebowania na zasoby ludzkie w Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych, jeżeli chodzi o wdrażanie wsparcia finansowego Unii w ramach programu „Cyfrowa Europa”.

Powyższa kompensacja zostanie zwiększona o szacowane zapotrzebowanie na wdrażanie wsparcia finansowego Unii w ramach programu „Horyzont Europa”, kiedy w trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo” filaru II „Globalne wyzwania i konkurencyjność przemysłowa” programu „Horyzont Europa” (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 21 ust. 1 lit. b).

3.2.3. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– ☐ nie przewiduje współfinansowania ze strony osób trzecich.

– ☒ przewiduje współfinansowanie ze strony osób trzecich[47] szacowane zgodnie z poniższymi szacunkami:

Środki w mln EUR (do trzech miejsc po przecinku)

Rok	2021	2022	2023	2024	2025	2026	2027	OGÓŁEM
Państwa członkowskie – wkład w wydatki na personel	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Państwa członkowskie – wkład w wydatki na infrastrukturę i wydatki administracyjne	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Państwa członkowskie – wkład w wydatki operacyjne	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
OGÓŁEM środki objęte współfinansowaniem	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Powyższy wkład osób trzecich dotyczy jedynie współfinansowania współmiernego do zasobów finansowych UE przeznaczonych na cyberbezpieczeństwo w ramach programu „Cyfrowa Europa". Powyższy wkład osób trzecich zostanie zwiększony, kiedy w trakcie procesu legislacyjnego, a w każdym razie przed osiągnięciem porozumienia politycznego, Komisja zaproponuje wkład z puli środków finansowych klastra „Integracyjne i bezpieczne społeczeństwo" filaru II „Globalne wyzwania i konkurencyjność przemysłowa" programu „Horyzont Europa" (całkowita pula to 2 800 000 000 EUR), o którym mowa w art. 21 ust. 1 lit. b). Wniosek będzie opierał się na wynikach procesu planowania strategicznego określonego w art. 6 ust. 6 rozporządzenia XXX [program ramowy „Horyzont Europa"].

3.3. Szacunkowy wpływ na dochody

– ☒ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

☐ wpływ na zasoby własne

☐ wpływ na dochody inne

Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków ☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po	Wpływ wniosku/inicjatywy[48]

[47] Szacowany wkład rzeczowy ze strony państw członkowskich

[48] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.

stronie dochodów:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artykuł …							

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).