**OPIS PRZEDMIOTU ZAMÓWIENIA**

**na opracowanie**

**„****Strategii budowania krajowej Społeczności kompetentnej w obszarze cyberbezpieczeństwa”   
w ramach projektu NATIONAL COORDINATION CENTRE – POLAND (NCC-PL) współfinansowanego ze środków Programu Cyfrowa Europa**

1. **Uzasadnienie**

Budowanie krajowej Społeczności kompetentnej w obszarze cyberbezpieczeństwa i wzmacnianie jej potencjału stanowi jeden z zasadniczych obszarów merytorycznych projektu „National Coordination Centre – Poland (NCC-PL)”, współfinasowanego ze środków Programu Cyfrowa Europa.

Program Cyfrowa Europa jest to unijny program finansowania, skoncentrowany na wdrażaniu rozwiązań w zakresie technologii cyfrowych przedsiębiorstw, obywateli i administracji publicznej. Program zapewnia strategiczne finansowanie w odpowiedzi na wyzwania technologiczne, wspierając projekty m.in. z obszaru cyberbezpieczeństwa. Program wspiera również przemysł, małe i średnie przedsiębiorstwa (MŚP) oraz administrację publiczną w ich transformacji cyfrowej m.in. za pomocą sieci europejskich centrów innowacji cyfrowych (EDIH).

Projekt „National Coordination Centre – Poland (NCC-PL)” jest realizowany przez Krajowe Centrum Kompetencji Cyberbezpieczeństwa, działające w strukturach Ministerstwa Cyfryzacji, powołane na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiającego Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (dalej: Rozporządzenie). Celem projektu jest ustanowienie i rozwój polskiego krajowego ośrodka koordynacji, który posiada zasoby i kompetencje do wykonywania zadań mu powierzonych, a także wspieranie krajowych zdolności w obszarze cyberbezpieczeństwa.

Jednym z zadań powierzonych NCC-PL, tak jak i pozostałym krajowym ośrodkom koordynacji, jest budowanie, koordynowanie oraz wspieranie działań Społeczności kompetentnej, rozumianej jako duża, otwarta, interdyscyplinarna i zróżnicowana grupa interesariuszy zaangażowanych w rozwój cyberbezpieczeństwa[[1]](#footnote-2). Celem tworzenia tej Społeczności jest wzmocnienie zdolności Unii Europejskiej i jej krajów członkowskich w zakresie cyberbezpieczeństwa oraz wspólna odpowiedź na wyzwania cyfrowego świata, poprzez budowanie współpracy ponad granicami i sektorami. Aby to zadanie zrealizować, NCC-PL powinien nawiązać kontakt z podmiotami prowadzącymi działalność w obszarze cyberbezpieczeństwa oraz zachęcić je do przystąpienia do Społeczności, zgodnie z wytycznymi na stronie <https://www.gov.pl/web/cyber-nccpl/spolecznosc-kompetentna> i zaangażowania się w jej prace.

1. **Cel zamówienia**

Głównym celem zamówienia jest opracowanie - na potrzeby Krajowego Centrum Kompetencji Cyberbezpieczeństwa - Strategii budowania krajowej Społeczności kompetentnej w obszarze cyberbezpieczeństwa (dalej: Strategia). Strategia powinna zostać zawarta w dokumencie opisującym krok po kroku jakie działania NCC-PL powinien podjąć, aby skutecznie dotrzeć do podmiotów, które mogłyby potencjalnie zostać członkami Społeczności. Lista podmiotów spełniających wymogi uzyskania statusu członka Społeczności została opisana w Rozporządzeniu. Dokument Strategii powinien zawierać również wskazówki w jaki sposób efektywnie przekonać te podmioty do zarejestrowania się jako członkowie europejskiej Społeczności kompetentnej i do zaangażowania się w jej działania oraz we współpracę z Europejskim Centrum Kompetencji Cyberbezpieczeństwa (dalej: ECCC) i siecią krajowych ośrodków koordynacji (dalej: NCC).

Celem dodatkowym, służącym realizacji celu głównego, jest stworzenie bazy krajowych interesariuszy działających w obszarze cyberbezpieczeństwa, posiadających potencjał do dołączenia do Społeczności kompetentnej (z wyłączeniem małych i średnich przedsiębiorstw), z uwzględnieniem m.in. takich zmiennych jak: lokalizacja, specjalność, zasięg działalności (krajowy/międzynarodowy).

1. **Odbiorcy Zamówienia**

Odbiorcami Zamówienia będą: Krajowe Centrum Kompetencji Cyberbezpieczeństwa w Ministerstwie Cyfryzacji oraz ECCC, jako podmiot przekazujący dofinansowanie do projektu. Odbiorcami mogą być również inne podmioty administracji publicznej, odpowiedzialne za projektowanie polityk w obszarze cyberbezpieczeństwa w Polsce.

1. **Zakres Zamówienia**
2. Przedmiotowy – elementy Zamówienia

Przedmiotem zamówienia jest usługa polegającą na opracowaniu Strategii budowania krajowej Społeczności kompetentnej w obszarze cyberbezpieczeństwa w ramach projektu National Coordination Centre – Poland (NCC-PL). Zamówienie składa się z następujących elementów:

* 1. Zmapowanie podmiotów zaangażowanych w tematykę cyberbezpieczeństwa, spełniających kryteria wskazane w zakresie podmiotowym Zamówienia (pkt 2.), które mogłyby potencjalnie wejść w skład Społeczności, tj.:
* Identyfikacja podmiotów prowadzących działalność w obszarze cyberbezpieczeństwa (z wyłączeniem małych i średnich przedsiębiorców) – zgodnie z pkt 2. ppk 1);
* Zweryfikowanie i wyodrębnienie spośród ww. podmiotów tych, które spełniają kryteria wskazane w pkt 2. ppk 2) – 4);
* Zweryfikowanie i wyodrębnienie spośród ww. podmiotów tych, które posiadają potencjał aby stać się członkami Społeczności Kompetentnej w zakresie cyberbezpieczeństwa, tj. które będą w stanie przyczynić się do realizacji misji ECCC   
  i Sieci NCC oraz wzmacniać i upowszechniać wiedzę fachową z zakresu cyberbezpieczeństwa (zgodnie z art. 8 Rozporządzenia) biorąc pod uwagę m. in. ich dotychczasowe osiągnięcia i dorobek, doświadczenie w branży cyberbezpieczeństwa, poziom zaangażowania w działania związane z cyberbezpieczeństwem, renomę dotyczącą posiadanej wiedzy fachowej i inne czynniki zidentyfikowane przez Wykonawcę jako istotne (pkt 2. Ppk 5));
* Stworzenie bazy ww. podmiotów (wyłonionych w wyniku selekcji opisanej w poprzednich punktach) wraz z określeniem dla każdego z nich:
  + nazwy podmiotu,
  + danych teleadresowych,
  + lokalizacji geograficznej (województwo i miejscowość),
  + rodzaju organizacji (zgodnie z pkt 1) zakresu podmiotowego),
  + specjalności (obszaru tematycznego działalności, w której dany podmiot się specjalizuje),
  + zasięgu działalności (krajowy/międzynarodowy);
* Przekazanie Zamawiającemu gotowej bazy podmiotów w formie osobnego pliku.
  1. Opracowanie Strategii nakierowanej na nawiązanie i podtrzymywanie kontaktu z podmiotami, które posiadają potencjał aby stać się członkami Społeczności Kompetentnej w obszarze cyberbezpieczeństwa oraz zaangażowanie ich w działania Społeczności. Strategia powinna zostać opracowana w oparciu o wyniki mapowania, o którym mowa w punkcie 1), a także o wyniki mapowania sektora małych i średnich przedsiębiorców działających w obszarze cyberbezpieczeństwa, które zostaną dostarczone Wykonawcy przez Zamawiającego. Strategia powinna obejmować co najmniej następujące elementy:
* wskazanie najefektywniejszych narzędzi i kanałów dotarcia do ww. podmiotów (zarówno cyfrowych jak i fizycznych) i nawiązania z nimi kontaktu,
* wskazanie efektywnego sposobu budowania przekazu kierowanego do ww. podmiotów, mającego na celu prezentację NCC-PL i koncepcji Społeczności kompetentnej oraz przekonanie adresatów do współpracy w ramach Społeczności, wraz z przykładami komunikatów, które mogą zostać w tym celu wykorzystane (minimum 4 propozycje),
* wskazówki w jaki sposób, w dłuższej perspektywie czasowej po nawiązaniu współpracy, utrzymać zaangażowanie podmiotów we współpracę w ramach Społeczności wraz z przykładami konkretnych działań, które mogą zostać w tym celu podjęte; wskazówki te powinny bazować również na doświadczeniach istniejących, dynamicznie funkcjonujących innych społeczności zawodowych,
* opracowanie planu działania: jakie działania, w jaki sposób i w jakiej kolejności powinny być realizowane, z uwzględnieniem wydarzeń zaplanowanych w projekcie.

Opracowując ww. elementy Wykonawca musi mieć na uwadze, iż adresaci działań zawartych w Strategii należą do różnych sektorów (akademicki, badawczy, przedsiębiorcy, administracja publiczna, pozarządowy) i różnią się w zakresie specjalizacji. Może zaistnieć konieczność zaplanowania innych sposobów nawiązania kontaktu i innego rodzaju przekazów dla poszczególnych grup adresatów. Strategia musi uwzględniać scenariusze nawiązania kontaktu i angażowania do współpracy każdej z ww. grup, aby doprowadzić do reprezentacji wszystkich tych grup w Społeczności. Różnorodność wśród członków Społeczności kompetentnej w obszarze cyberbezpieczeństwa jest warunkiem niezbędnym dla realizacji założeń leżących u podstaw jej utworzenia tj. wzmocnienia cyberodporności, dzięki połączeniu wiedzy eksperckiej i potencjału pochodzących od różnych podmiotów   
i płynących z różnych sektorów.

Ww. Strategia powinna zostać przekazana Zamawiającemu w formie dokumentu, przy czym stopień szczegółowości opisu działań powinien pozwalać na ich bezpośrednie wdrożenie. Dokument, poza częścią opisową, powinien zawierać również schematy obrazujące w przejrzysty sposób kolejność i rodzaj działań skierowanych do poszczególnych grup adresatów.

1. Podmiotowy

Podmioty podlegające mapowaniu w ramach niniejszego Zamówienia i jednocześnie grupa docelowa działań zaproponowanych w ramach opracowanej Strategii to podmioty realizujące działania w obszarze cyberbezpieczeństwa. Podmioty te powinny spełniać łącznie następujące warunki:

* 1. reprezentują jeden z następujących rodzajów organizacji:
* przedsiębiorcy,
* organizacje akademickie,
* organizacje badawcze,
* organizacje społeczeństwa obywatelskiego,
* podmioty publiczne,
* organizacje normalizacyjne,
* inne podmioty zajmujące się aspektami operacyjnymi i technicznymi cyberbezpieczeństwa;
  1. cyberbezpieczeństwo[[2]](#footnote-3) stanowi dla nich jedyną działalność

lub

cyberbezpieczeństwo stanowi jeden z rodzajów ich działalności i jednocześnie działania związane z cyberbezpieczeństwem są realizowane przez wyodrębnioną/możliwą do wyodrębnienia komórkę organizacyjną lub strukturę wewnętrzną lub podmiot jest w znacznym stopniu zaangażowany w obszar cyberbezpieczeństwa (angażuje w ten obszar co najmniej 30% swoich zasobów - czasowych, osobowych, pod kątem liczby produktów),

* 1. dysponują wiedzą fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin:
* środowisko akademickie, badania naukowe lub innowacje;
* rozwój przemysłowy lub rozwój produktów;
* szkolenie i kształcenie;
* bezpieczeństwo informacji lub operacje w zakresie reagowania na incydenty;
* etyka;
* formalna i techniczna standaryzacja oraz specyfikacje;
  1. są zarejestrowane na terenie RP,
  2. dysponują potencjałem pozwalającym na przyczynienie się do realizacji misji ECCC i Sieci NCC oraz do wzmacniania i upowszechniania wiedzy fachowej z zakresu cyberbezpieczeństwa, biorąc pod uwagę m. in. ich dotychczasowe osiągnięcia i dorobek, doświadczenie w branży cyberbezpieczeństwa, poziom zaangażowania w działania związane z cyberbezpieczeństwem, renomę dotyczącą posiadanej wiedzy fachowej i inne czynniki zidentyfikowane przez Wykonawcę jako istotne.

Mapowanie poprzedzające opracowanie Strategii powinno objąć podmioty spełniające ww. kryteria, **z wyłączeniem małych i średnich przedsiębiorców** (Zamawiający dostarczy Wykonawcy bazę danych dotyczącą tej grupy po podpisaniu umowy).

Natomiast działania zawarte w Strategii powinny objąć zarówno ww. podmioty, jak również małych i średnich przedsiębiorców z bazy dostarczonej przez Zamawiającego oraz podmioty działające w sektorach powiązanych z cyberbezpieczeństwem i mierzące się z wyzwaniami w tej dziedzinie. Działania te powinny zostać zaplanowane z uwzględnieniem charakterystyki wszystkich tych grup.

1. Terytorialny

Działania realizowane w ramach Zamówienia powinny objąć zasięgiem cały kraj. Wyniki mapowania powinny zostać zaprezentowane między innymi z uwzględnieniem rozkładu terytorialnego.

1. Czasowy

Działania w Strategii powinny zostać zaplanowane w ten sposób, aby możliwe było przeprowadzenie większości z nich w perspektywie 1,5 roku od dnia zakończenia realizacji Zamówienia. Strategia powinna uwzględniać również działania długookresowe, do realizacji w perspektywie 3 lat od dnia zakończenia realizacji zamówienia.

1. **Sposób realizacji zamówienia**
2. Metodologia

* Na Wykonawcy zamówienia spoczywa zadanie poszukiwania i zidentyfikowania podmiotów działających w branży cyberbezpieczeństwa. Następnie Wykonawca zweryfikuje, czy podmioty te spełniają kryteria wskazane w zakresie podmiotowym zamówienia (roz. IV pkt 2. „Zakres podmiotowy”). Kolejnym krokiem będzie opracowanie przez Wykonawcę bazy danych i umieszczenie w niej podmiotów wyłonionych w efekcie weryfikacji, o której mowa w poprzednim zdaniu, a także opisanie i skategoryzowanie każdego z tych podmiotów z użyciem kategorii wskazanych w zakresie przedmiotowym zamówienia (tj. nazwa podmiotu, dane teleadresowe, lokalizacja geograficzna, rodzaj organizacji, specjalność, zasięg działalności).

**Dlatego też, częścią oferty Wykonawcy powinna być koncepcja** zawierająca następujące informacje:

* + opis planowanego sposobu postępowania, mającego na celu zidentyfikowanie podmiotów działających w branży cyberbezpieczeństwa; koncepcja powinna obejmować również wskazanie źródeł danych, z jakich Wykonawca zamierza skorzystać;
  + metodologię jaką Wykonawca zamierza zastosować w celu weryfikacji, czy poszczególne zidentyfikowane podmioty spełniają kryteria wskazane w roz. IV pkt 2 - Wykonawca powinien wskazać jak będzie przebiegał planowany proces kwalifikacji oraz opisze sposób, w jaki zamierza zweryfikować spełnienie każdego z kryteriów przez każdy z analizowanych podmiotów; dodatkowo, w odniesieniu do kryterium „posiadania potencjału do dołączenia do Społeczności” Wykonawca zaproponuje w jaki sposób to posiadanie potencjału powinno być rozumiane, tj. wskaże czym charakteryzuje się podmiot, który ten potencjał posiada;
* Kolejnym zadaniem Wykonawcy będzie zaproponowanie Strategii nakierowanej na nawiązanie i podtrzymywanie kontaktu z podmiotami, które posiadają potencjał aby stać się członkami Społeczności Kompetentnej w obszarze cyberbezpieczeństwa oraz zaangażowanie ich w działania Społeczności.

**Dlatego też, częścią oferty Wykonawcy powinna być również propozycja co do zawartości Strategii** – wskazanie proponowanej struktury dokumentu, rozdziałów i wątków tematycznych, które zadaniem Wykonawcy powinny być ujęte w opracowaniu. Minimalny zakres Strategii został wskazany w rozdz. IV pkt 1. ppk 2), jednak wyjście poza ten zakres będzie dodatkowo punktowane na etapie oceny ofert (o ile propozycje będą uzasadnione).

* Tworząc bazę podmiotów posiadających potencjał do dołączenia do Społeczności kompetentnej w obszarze cyberbezpieczeństwa, Wykonawca zaproponuje katalog specjalności, który zostanie zastosowany do kategoryzacji podmiotów w bazie, z wyłączeniem kategorii dużych przedsiębiorców, dla których Zamawiający udostępni gotowy do zastosowania katalog specjalności (w oparciu o katalog projektowany dla MŚP).
* W celu zapewnienia wysokiej jakości i kompletności bazy podmiotów działających w obszarze cyberbezpieczeństwa, Wykonawca powinien przeprowadzić kontrolę sposobu realizacji przez swój personel działań polegających na identyfikowaniu i kwalifikowaniu podmiotów do mapowania, aby sprawdzić czy realizacja ta przebiega rzetelnie i zgodnie z ustaloną metodologią. Sposób przeprowadzenia tej kontroli i jej wyniki powinny zostać opisane w raporcie dokumentującym przebieg mapowania podmiotów zaangażowanych w tematykę cyberbezpieczeństwa, który będzie jednym z produktów zamówienia.
* Opracowując Strategię budowania krajowej Społeczności kompetentnej w obszarze cyberbezpieczeństwa, Wykonawca musi mieć na uwadze, iż adresaci działań zawartych w Strategii należą do różnych sektorów (akademicki, badawczy, przedsiębiorcy, administracja publiczna, pozarządowy) i różnią się w zakresie specjalizacji. Może zaistnieć konieczność zaplanowania innych sposobów nawiązania kontaktu i innego rodzaju przekazów dla poszczególnych grup adresatów. Strategia musi uwzględniać scenariusze nawiązania kontaktu i angażowania do współpracy każdej z ww. grup adresatów, aby doprowadzić do obecności wszystkich tych grup w Społeczności.
* Opracowując wskazówki co do tego w jaki sposób, w dłuższej perspektywie czasowej po nawiązaniu współpracy, utrzymać zaangażowanie podmiotów we współpracę w ramach Społeczności, Wykonawca powinien bazować również na doświadczeniach i dobrych praktykach istniejących, dynamicznie funkcjonujących społeczności zawodowych.

1. Etapy realizacji Zamówienia
   1. Spotkanie Wykonawcy z przedstawicielami Zamawiającego, którego celem jest przekazanie Wykonawcy wszelkich informacji niezbędnych do prawidłowej realizacji Zamówienia, udzielenie odpowiedzi na pytania Wykonawcy oraz ewentualne dodatkowe uzgodnienia miedzy Wykonawcą i Zamawiającym co do sposobu realizacji poszczególnych elementów Zamówienia. Dopuszcza się możliwość zorganizowania spotkania w trybie online.
   2. Mapowanie, którego efektem będzie stworzenie bazy krajowych interesariuszy działających w obszarze cyberbezpieczeństwa, posiadających potencjał do dołączenia do Społeczności kompetentnej (z wyłączeniem małych i średnich przedsiębiorstw),
   3. Przekazanie Zamawiającemu dotychczas wytworzonych produktów Zamówienia:

* Bazy krajowych interesariuszy działających w obszarze cyberbezpieczeństwa – w formie elektronicznej, zawierającej następujące elementy:
  + Lista podmiotów, zawierająca dla każdego z nich informacje wskazane w pkt IV.1.1), pozwalająca na sortowanie podmiotów według każdej z tych kategorii;
  + Wykresy statystyczne opracowane w oparciu o ww. dane oraz schemat mapy Polski z naniesionymi na niej podmiotami z listy;
* Raportu dokumentującego przebieg mapowania podmiotów zaangażowanych w tematykę cyberbezpieczeństwa – raport powinien opisywać w sposób szczegółowy w jaki sposób Wykonawca poszukiwał podmiotów w ramach poszczególnych grup podmiotowych, jakie były rezultaty poszukiwań i jakie ewentualne problemy zaistniały podczas realizacji tego etapu. Dokument powinien opisywać ponadto przebieg procesu kwalifikacji podmiotów do mapowania. Powinien zawierać także wyniki kontroli przeprowadzonej przez Wykonawcę, o której mowa w pkt V.1.

1. Weryfikacja przez Zamawiającego otrzymanych produktów Zamówienia, zgłoszenie ewentualnych uwag i wdrożenie przez Wykonawcę postulowanych zmian.
2. Opracowanie Strategii budowania krajowej społeczności kompetentnej w obszarze cyberbezpieczeństwa,

* Przekazanie Zamawiającemu dokumentu zawierającego Strategię, zgodnie z pkt IV.1.2):
  + forma elektroniczna,
  + wersje językowe: polska i angielska,
  + dokument powinien być zgodny z wymaganiami WCAG 2.1 na poziomie AA.,
  + dokument oraz wszelkie jego załączniki muszą zostać oznaczone znakami projektu zgodnie z wytycznymi Zamawiającego, które zostaną przekazane Wykonawcy po podpisaniu umowy,
  + dokument powinien spełniać warunki wskazane w pkt IV.1.2),
  + od Wykonawcy oczekuje się atrakcyjniej edytorsko formy dokumentu, z grafikami, tabelami i wykresami.

1. Weryfikacja przez Zamawiającego otrzymanego dokumentu zawierającego Strategię, zgłoszenie ewentualnych uwag i wdrożenie przez Wykonawcę postulowanych zmian.
2. **Harmonogram**

Wykonawca przedstawi harmonogram realizacji Zamówienia. Wszelkie zmiany w harmonogramie będą wymagały uzgodnienia z Zamawiającym. Harmonogram powinien uwzględniać daty realizacji każdego z etapów oraz produktów.

Termin realizacji zamówienia nie powinien przekroczyć 12 tygodni od dnia podpisania umowy.

1. **Koordynacja i współpraca**

* Zamawiający oczekuje jako minimum zorganizowania przez Wykonawcę w początkowym etapie realizacji Zamówienia spotkania z przedstawicielami Zamawiającego, którego celem jest przekazanie Wykonawcy wszelkich informacji niezbędnych do prawidłowej realizacji Zamówienia, udzielenie odpowiedzi na pytania Wykonawcy i Zamawiającego oraz ewentualne dodatkowe uzgodnienia między Wykonawcą i Zamawiającym co do sposobu realizacji poszczególnych elementów Zamówienia.
* Poza ww. spotkaniem, zalecany jest również dalszy roboczy kontakt Wykonawcy   
  z przedstawicielami Zamawiającego w celu wyjaśniania bieżących wątpliwości pojawiających się podczas realizacji kolejnych etapów Zamówienia oraz dokonywania dalszych szczegółowych ustaleń. Kontakt ten może być prowadzony w formie korespondencji mailowej, rozmowy telefonicznej lub spotkań online.
* Wykonawca będzie informował o zakończeniu każdego z etapów realizacji Zamówienia poprzez informację przekazywaną na wskazany przez Zamawiającego adres mailowy.
* Zamawiający ma prawo do zgłaszania uwag do każdego z produktów zamówienia przedstawionych przez Wykonawcę. Wykonawca ma obowiązek uwzględnienia tych uwag   
  i wdrożenia postulowanych zmian. Planując prace Wykonawca powinien uwzględnić czas potrzebny na weryfikację produktów zamówienia i wdrożenie zmian postulowanych przez Zamawiającego. W razie wątpliwości co do zgłoszonych przez Zamawiającego uwag, Wykonawca powinien odbyć spotkanie z przedstawicielami Zamawiającego w celu wyjaśnienia tych wątpliwości i podjęcia ostatecznej decyzji co do zakresu wdrażanych zmian.

1. **Podstawowe dokumenty i materiały źródłowe, które powinny zostać poddane analizie**
2. ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (t.j. Dz.U. z 2024 r. poz. 1077, 1222);
3. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. *ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji*;
4. Strona internetowa NCC-PL: <https://www.gov.pl/web/cyber-nccpl>
5. **Finansowanie zamówienia**

Zamówienie jest finansowane ze środków Programu Cyfrowa Europa oraz środków krajowych.

1. Zgodnie z Rozporządzeniem PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2021/887

   z dnia 20 maja 2021 r. ustanawiającym Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji: <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32021R0887> [↑](#footnote-ref-2)
2. Cyberbezpieczeństwo rozumiane zgodnie z definicją zawartą w *ustawie o krajowym systemie cyberbezpieczeństwa*. [↑](#footnote-ref-3)