www.doradcy365.pl

RAPORT O MOŻLIWOŚCIACH POZYSKIWANIA DOFINANSOWANIA NA PROJEKTY DUAL-USE

Przegląd krajowych i międzynarodowych programów wsparcia dla technologii bezpieczeństwa

Wrocław, 22.04.2026

Spis treści

Streszczenie

W ostatnich latach nastąpiła istotna zmiana w podejściu do finansowania technologii bezpieczeństwa oraz rozwiązań podwójnego zastosowania (dual-use). W odpowiedzi na wyzwania geopolityczne i rosnące znaczenie odporności systemowej, zarówno Unia Europejska, jak i państwa członkowskie oraz NATO znacząco zwiększają skalę wsparcia dla projektów wzmacniających bezpieczeństwo, infrastrukturę krytyczną oraz zdolności obronne.

Technologie dual-use – łączące zastosowania cywilne i wojskowe – stają się jednym z kluczowych kierunków inwestycyjnych. Dotyczy to m.in. obszarów takich jak sztuczna inteligencja, cyberbezpieczeństwo, systemy autonomiczne, analiza danych czy technologie dla infrastruktury krytycznej. W efekcie coraz więcej innowacji rozwijanych na potrzeby rynku cywilnego znajduje zastosowanie również w sektorze bezpieczeństwa i obronności.

Wraz z tym trendem dynamicznie rozwija się ekosystem finansowania. Obejmuje on nie tylko klasyczne dotacje badawczo-rozwojowe, ale również wsparcie inwestycyjne, programy infrastrukturalne, akceleratory, inicjatywy NATO oraz działania networkingowe i testowe. Instrumenty te funkcjonują równolegle na poziomie krajowym, regionalnym, unijnym i międzynarodowym, tworząc zintegrowany system wsparcia.

Obecne możliwości finansowania są dostępne dla szerokiego grona beneficjentów – od przedsiębiorstw (MŚP i dużych firm), przez startupy technologiczne, po jednostki samorządu terytorialnego, uczelnie i konsorcja przemysłowo-naukowe. Oznacza to, że wejście w obszar dual-use jest dziś możliwe także dla podmiotów bez wcześniejszego doświadczenia w sektorze obronnym.

Jednocześnie rosnąca liczba instrumentów powoduje, że kluczowym wyzwaniem staje się nie tyle dostęp do środków, co umiejętność ich właściwego wykorzystania. Skuteczny rozwój projektów wymaga podejścia etapowego – od wejścia do ekosystemu i walidacji technologii, przez rozwój i finansowanie, aż po wdrożenie i skalowanie działalności.

Niniejszy raport porządkuje dostępne możliwości wsparcia oraz wskazuje praktyczne ścieżki rozwoju projektów dual-use. Kluczowym wnioskiem jest to, że największy potencjał osiągają projekty, które łączą różne źródła finansowania i są rozwijane w sposób strategiczny, z uwzględnieniem specyfiki sektora bezpieczeństwa i obronności.

1. Wprowadzenie

Technologie bezpieczeństwa rozwijają się dziś w wyjątkowo dynamicznym tempie. Rosnące zagrożenia hybrydowe, rozwój narzędzi cyberprzestępczych, postępująca automatyzacja procesów przemysłowych, a także zwiększona podatność infrastruktury krytycznej na zakłócenia — wszystko to sprawia, że zarówno sektor publiczny, jak i prywatny poszukują nowych, bardziej zaawansowanych rozwiązań. W tym kontekście szczególne znaczenie mają **technologie podwójnego zastosowania (dual-use)**, łączące funkcje cywilne i obronne.

Rozwój technologii dual-use jest dodatkowo wzmacniany przez zmieniające się podejście instytucji publicznych do bezpieczeństwa — od modelu reaktywnego do modelu opartego na odporności, prewencji i zdolności szybkiej adaptacji. Oznacza to rosnące zapotrzebowanie na rozwiązania, które mogą być wykorzystywane zarówno w codziennym funkcjonowaniu gospodarki, jak i w sytuacjach kryzysowych lub operacyjnych.

Do kategorii technologii dual-use zaliczają się m.in.:

- zaawansowane systemy detekcji, monitoringu i analizy danych,
- technologie oparte na sztucznej inteligencji i uczeniu maszynowym,
- narzędzia cyberbezpieczeństwa, w tym systemy wykrywania anomalii i ochrony przed atakami,
- sensory i systemy obserwacji,
- mobilne i autonomiczne platformy bezpieczeństwa,
- rozwiązania do ochrony infrastruktury krytycznej,
- a także technologie służące przeciwdziałaniu nowym typom zagrożeń, takim jak drony czy systemy bezzałogowe.

Systemy przeciwdronowe (C-UAS) stanowią jedynie jeden z licznych przykładów, w których **zaawansowane technologie mogą pełnić rolę zarówno w sektorze cywilnym, jak i w obronności**, co czyni je typowym przypadkiem projektów dual-use. Podobny charakter mają również rozwiązania z zakresu cyberbezpieczeństwa, analizy danych czy automatyzacji procesów — rozwijane pierwotnie dla rynku komercyjnego, a następnie adaptowane do zastosowań związanych z bezpieczeństwem państwa.

Dynamiczny rozwój tej kategorii technologii znajduje bezpośrednie odzwierciedlenie w rosnącej liczbie programów wsparcia finansowego — krajowych, europejskich i międzynarodowych. Ich wspólnym celem jest wzmacnianie odporności państwa i gospodarki, zwiększenie innowacyjności oraz wspieranie rozwiązań podnoszących poziom bezpieczeństwa w wymiarze fizycznym, cyfrowym i operacyjnym.

Co istotne, obecny system wsparcia nie ogranicza się już do pojedynczych instrumentów finansowania, lecz tworzy złożony ekosystem obejmujący:

- testowanie technologii i walidację w warunkach zbliżonych do rynkowych,
- rozwój oprogramowania i integrację systemową,
- zwiększenie wiedzy technologicznej przedsiębiorstwa w obszarach krytycznych.

Wsparcie B+R w ramach FWTK ma na celu zwiększenie **TRL (Technology Readiness Level)** projektów tak, aby łatwiej przechodziły one do fazy komercyjnej i wdrożeniowej.

Wsparcie inwestycyjne

Program dopuszcza również finansowanie **inwestycji kapitałowych i rzeczowych**, takich jak:

- zakup wyposażenia technologicznego i lini produkcyjnych,
- budowa lub modernizacja laboratoriów i infrastruktury testowej,
- zakup aparatury pomiarowej oraz sprzętu IT dedykowanego projektom strategicznym,
- inwestycje prowadzące do zwiększenia zdolności produkcyjnych technologii krytycznych.

Takie podejście sprawia, że FWTK jest instrumentem **łączącym B+R z realną inwestycją w infrastrukturę produkcyjną i technologiczną**.

Dual-use jako kluczowy element programu

STEP / FWTK **wyraźnie dopuszcza projekty o charakterze dual-use** — czyli te, które mają zastosowania zarówno w sektorze cywilnym, jak i defensywnym — pod warunkiem, że nie są wyłącznie dedykowane militarnym systemom ofensywnym.

Program jest szczególnie ważny dla rozwoju:

- technologii bezpieczeństwa infrastruktury krytycznej,
- systemów obserwacji, detekcji i analizy sygnałów,
- AI i narzędzi wspierających podejmowanie decyzji w warunkach ryzyka,
- autonomicznych systemów operacyjnych i platform robotycznych,
- rozwiązań do przeciwdziałania zagrożeniom hybrydowym i cyberatakom.

W kontekście **systemów przeciwdronowych (C-UAS)** oraz innych technologii bezpieczeństwa, FWTK stanowi jedno z **najważniejszych źródeł wsparcia finansowego** na etapie rozwoju technologii do poziomów gotowości rynkowej i wdrożeniowej.

Dla kogo jest program?

Program adresowany jest do przedsiębiorstw:

- planujących realizację projektów technologicznych o wysokim znaczeniu strategicznym,
- rozwijających technologie dotychczas trudno finansowane klasycznymi dotacjami,

Zakres obejmuje m.in.:

- technologie poprawiające funkcjonowanie infrastruktury wojskowej,
- systemy zabezpieczania obiektów wojskowych,
- technologie monitoringu i ochrony,
- systemy wspomagające logistykę i mobilność wojskową,
- rozwiązania zwiększające bezpieczeństwo operacyjne instalacji wojskowych.

W odróżnieniu od SZAFIRU, który koncentruje się na sprzęcie wojskowym, **PERUN skupia się na infrastrukturze, logistyce i wsparciu operacyjnym**, ale jest również otwarty na technologie dual-use.

3. Inne konkursy tematyczne NCBR (bezpośrednio dla służb)

NCBR realizuje również konkursy ogłaszane przez:

- **MON**,
- **Policję**,
- **Straż Graniczną**,
- **Państwową Straż Pożarną**,
- **Służbę Więzienną**,
- **MSWiA**.

Są to często konkursy:

- dedykowane konkretnym typom technologii,
- organizowane „pod zapotrzebowanie formacji”,
- zawierające szczegółowe specyfikacje i wymagania techniczne.

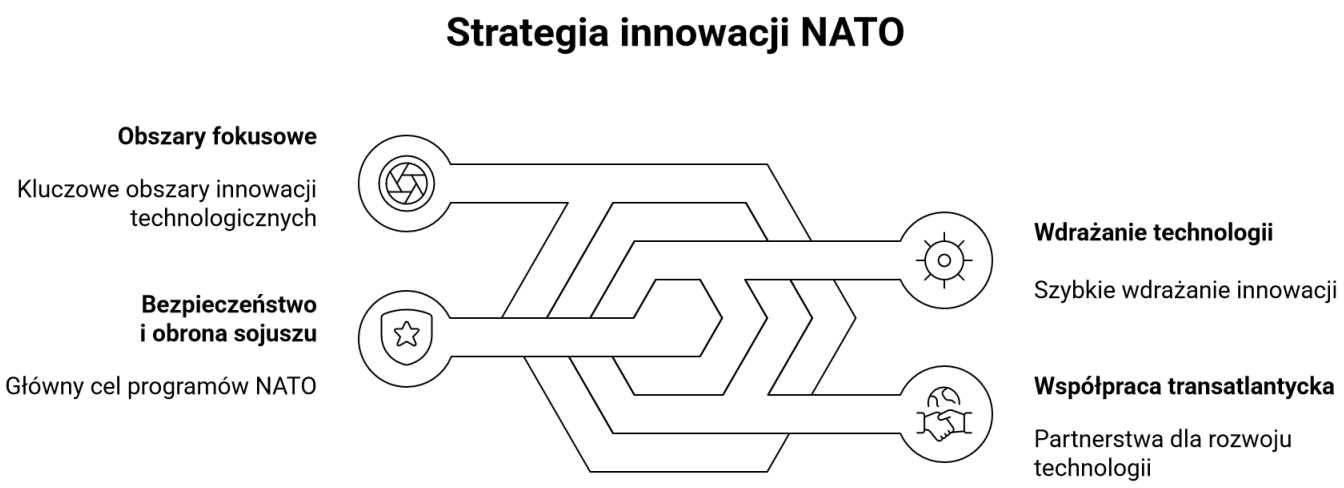
Przykłady obszarów:

- rozpoznanie obrazowe,
- radiolokacja,
- ochrona granic i infrastruktury krytycznej,
- systemy komunikacji szyfrowanej,
- technologie antydronowe i antyterrorystyczne,
- robotyka specjalna,
- technologie wczesnego wykrywania.

B. Programy NATO i inicjatywy transatlantyckie

Programy i inicjatywy NATO koncentrują się na przyspieszonym rozwoju innowacyjnych technologii o bezpośrednim znaczeniu dla bezpieczeństwa i obronności państw Sojuszu. Ich celem jest szybkie testowanie, walidacja i wdrażanie przełomowych rozwiązań technologicznych, w szczególności w obszarach **dual-use**, autonomii, sztucznej inteligencji, cyberbezpieczeństwa oraz systemów bezzałogowych.

Udział w inicjatywach NATO – takich jak akceleratory, programy innowacyjne czy platformy współpracy transatlantyckiej – pozwala przedsiębiorstwom nawiązać relacje z użytkownikami końcowymi technologii (siłami zbrojnymi, agencjami bezpieczeństwa), a także przygotować się do wdrożeń na rynkach międzynarodowych o wysokich wymaganiach technologicznych i certyfikacyjnych.



European Critical Infrastructure Hackathon (Gdańsk)

Inicjatywa skoncentrowana na budowie rozwiązań zwiększających odporność infrastruktury krytycznej, obejmująca:

- pracę zespołową nad prototypami,
- współpracę z ekspertami i instytucjami publicznymi,
- szybkie testowanie koncepcji technologicznych.

Funkcja:

- **walidacja pomysłów i budowa prototypów w środowisku problemowym**

Znaczenie:

- przyspiesza rozwój technologii na wczesnym etapie,
- umożliwia nawiązanie relacji z partnerami i ekspertami,
- może stanowić pierwszy krok do dalszych programów (IDA, EUDIS, DIANA).

EDF Info Days / EDA networking events

Oficjalne wydarzenia Komisji Europejskiej oraz Europejskiej Agencji Obrony (EDA), których celem jest:

- prezentacja tematów konkursowych EDF,
- łączenie partnerów projektowych,
- wsparcie w budowie konsorcjów międzynarodowych.

Funkcja:

- **narzędzie budowy konsorcjów i przygotowania projektów do EDF**

Znaczenie:

- kluczowe dla firm planujących udział w EDF,
- umożliwia wejście do projektów bez konieczności samodzielnego budowania konsorcjum,
- zwiększa szanse na skuteczną aplikację poprzez dopasowanie do priorytetów UE.

Znaczenie wydarzeń w strategii wejścia na rynek obronny

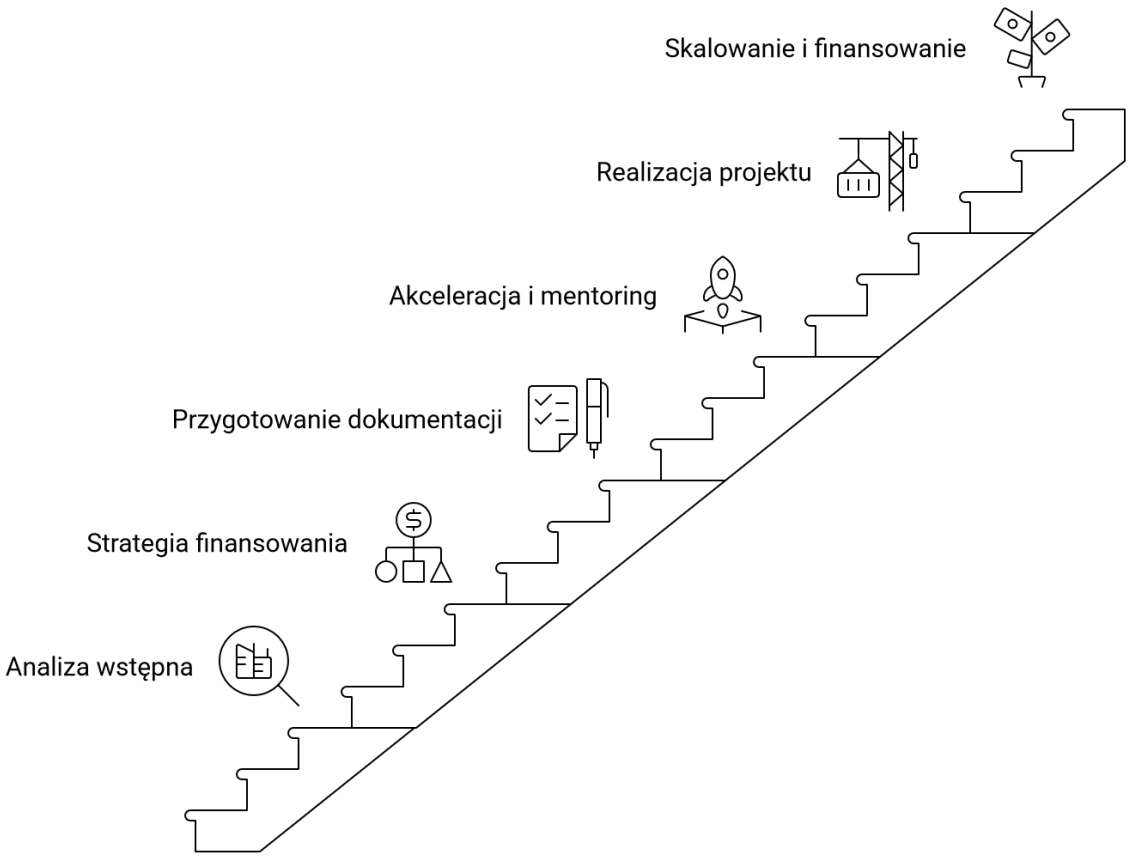
Z perspektywy przedsiębiorstw wydarzenia te:

- nie są dodatkiem, lecz **integralnym elementem strategii wejścia**,
- często stanowią pierwszy punkt kontaktu z ekosystemem obronnym,
- umożliwiają przejście od izolowanego projektu do udziału w realnych inicjatywach,
- zwiększają prawdopodobieństwo udziału w finansowanych projektach.

- doradztwo w zakresie ekspansji międzynarodowej,
- długofalowe wsparcie strategiczne.

Efekt dla Klienta:
ciągłość finansowania i rozwój technologii w perspektywie kilku lat.

Model współpracy z Doradcy365



Elastyczność współpracy

Model współpracy może być:

- **całościowy** (wszystkie etapy),
- **modułowy** (np. tylko strategia + aplikacja),
- **projektowy** (jeden wybrany program),
- **stały** (doradztwo stałe dla firm rozwijających portfel technologii).