Łukasz Czajkowski
Wojciech Dzięgiel
płk Sławomir Florek
Krzysztof Michalski (red.)
Jakub Wernik

Budowa odporności Polski w ramach nowych celów wydatkowych NATO

Lipiec 2026

Fundacja im. Kazimierza Pułaskiego

Klub Przemysłowy Bezpieczeństwa Narodowego

PIDU Polska Izba Dual Use

Łukasz Czajkowski, Wojciech Dzięgiel, płk Sławomir Florek, Krzysztof Michalski (red.), Jakub Wernik

Budowa odporności Polski w ramach nowych celów wydatkowych NATO

Fundacja im. Kazimierza Pułaskiego, Polska Izba Dual-Use / Warszawa 2026

PARTNERZY PROJEKTU

ATLAS WARD

HOLDFORT
PROTECTIVE STRUCTURES

JLL

Publikacja sfinansowana m.in. ze środków pozyskanych od Partnerów raportu.
Partnerzy nie mieli wpływu na treść raportu, który został przygotowany zgodnie z najlepszą wiedzą ekspertów i autorów.

PODZIĘKOWANIA ZA WSPÓŁPRACĘ I INSPIRACJE
Creotech Instruments, LIKI Mobile Solutions, Spyrosoft, SSW Law & Beyond

PARTNER MERYTORYCZNY

ZWIĄZEK BANKÓW POLSKICH

Budowa odporności Polski w ramach nowych celów wydatkowych NATO

AUTORZY
Łukasz Czajkowski,
Wojciech Dzięgiel,
płk Sławomir Florek,
Krzysztof Michalski,
Jakub Wernik

REDAKCJA
Krzysztof Michalski

WYDAWCA
Fundacja im. Kazimierza Pułaskiego
ul. Oleandrów 6, 00-629 Warszawa
www.pulaski.pl

Polska Izba Dual-Use
Rondo ONZ 1, 00-124 Warszawa
www.izbadualuse.pl

PROJEKT GRAFICZNY
Marta Duda (Dobry Skład)

SPIS TREŚCI

Słowo wstępne prezesów Fundacji im. Kazimierza Pułaskiego i Polskiej Izby Dual-Use / 5

Podsumowanie zarządcze / 7

część I **Wprowadzenie i kontekst strategiczny** / 9

1 Cel i zakres raportu / 10
1.1 Wstęp / 10
1.2 Geneza i ewolucja celu 5% PKB: Od szczytu w Walii do Deklaracji Haskiej / 11
1.3 Względność celu 5% PKB / 13
1.4 Definicja wydatków na rzecz bezpieczeństwa i odporności kraju / 15

2 Kontekst strategiczny / 17
2.1 Nowe typy zagrożeń niemilitarnych: rosnąca skala i zmieniający się charakter / 18
2.2 Masowe zagrożenia dla ludności cywilnej / 19
2.3 Kryzysy klimatyczne i technologiczne / 23
2.4 Zmiany klimatu i kwestia bezpieczeństwa w UE / 24
2.5 Cyberataki na administrację i usługi publiczne / 26
2.6 Wnioski: odporność cywilna jako wymóg strategiczny / 27

3 Praktyka w państwach NATO / 28
3.1 Metoda obliczania wydatków obronnych w ramach Sojuszu Północnoatlantyckiego / 28
3.2 Interpretacje narodowe: jak sojusznicy definiują swój 1,5% / 30
3.3 Zasady finansowania wydatków 1,5% / 34
3.4 Zasady wydatkowania środków kwalifikowanych do 1,5% PKB / 35
3.5 Ryzyka wdrożeniowe i rekomendacje / 37
3.6 Zasady wydatkowania 1,5% PKB w Polsce / 39

część II **Od alokacji do sektorów: priorytety wydatkowe i przemysł** / 41

4 Struktura wydatków – proponowana alokacja / 43

5 Dostępne źródła finansowania / 49
5.1 Instrumenty finansowania / 50
5.2 Luki, zasada dodatkowości i wąskie gardła absorpcyjne / 52
5.3 Propozycje działań / 54

6 Strategia budowy i modernizacji schronów / 57
6.1 Schrony a prawo międzynarodowe / 57
6.2 Ramy NATO i UE / 58
6.3 Przykłady polityk publicznych Finlandii, Szwajcarii, Szwecji i Estonii / 59
6.4 Diagnoza potrzeb infrastruktury ochronnej w Polsce / 60

6.5 Polskie ramy prawne: od próżni regulacyjnej do kompleksowej kaskady legislacyjnej / 62
6.6 Lokalizacja / 65
6.7 Model dual-use – wykorzystanie w czasie pokoju / 66
6.8 Cyfrowa paszportyzacja i monitoring gotowości obiektów ochrony ludności / 71
6.9 Obiekty czasowego zakwaterowania ewakuowanej ludności / 71
6.10 Inwestycje ochronne a prawo zamówień publicznych / 72

7 Architektura bezpieczeństwa infrastruktury krytycznej i cyberprzestrzeni / 73
7.1 Ochrona infrastruktury krytycznej – ramy prawne / 73
7.2 Cyberprzestrzeń i krajowy system cyberbezpieczeństwa / 79
7.3 Architektura cyberbezpieczeństwa, wykrywanie i reagowanie / 81
7.4 System Bezpiecznej Łączności Państwowej (SBŁP) i suwerenność cyfrowa / 84
7.5 Finansowanie wykonawców zewnętrznych i ochrona łańcucha dostaw / 88

8 Technologie kosmiczne dla odporności kraju i bezpieczeństwa ludności / 90
8.1 Rosnące znaczenie technologii kosmicznych / 90
8.2 Konieczność suwerenności technologicznej w kosmosie / 91
8.3 Polski wkład w europejską infrastrukturę satelitarną / 91

9 Odporność systemu ochrony zdrowia / 93
9.1 Koncepcja WAR-SOR: szpitale podwójnego zastosowania / 94
9.2 Doświadczenia zagraniczne: Izrael i Finlandia / 95
9.3 Podstawy prawne i status ochrony szpitali w prawie humanitarnym / 96
9.4 Strategia zachowania ciągłości opieki i relokacji pacjentów / 97
9.5 Strategiczne rezerwy leków, odporność farmaceutyczna i cyberbezpieczeństwo / 98
9.6 Rekomendacje wdrożeniowe / 99

10 Budowa krajowego przemysłu odpornościowego / 101
10.1 Koszyk odpornościowy jako instrument reindustrializacji i suwerenności technologicznej / 102
10.2 Doświadczenia europejskie w budowaniu zintegrowanego ekosystemu odporności / 102
10.3 Krajowy potencjał przemysłowy: stan obecny i perspektywy rozwoju sektora / 105
10.4 Implementacja celów odpornościowych poprzez rozwój rodzimych zdolności wytwórczych / 106
10.5 Lokalna treść w zamówieniach odpornościowych / 107

CZĘŚĆ III Efekty, mierniki i rekomendacje / 109

11 Efekty społeczne i gospodarcze oraz proponowane mierniki efektywności / 111
11.1 Potrójna dywidenda z odporności / 112
11.2 Efekty społeczno-gospodarcze wzrostu odporności / 112
11.3 Proponowane mierniki efektywności / 113

12 Propozycje i rekomendacje / 114
12.1 Proponowane zmiany ustawodawcze / 114
12.2 Organ koordynujący – Rada ds. Odporności / 115
12.3 Organ koordynujący – Minister ds. Odporności / 116
12.4 Rola samorządu terytorialnego / 117
12.5 Rola organizacji pozarządowych / 118

Słowo wstępne prezesów Fundacji im. Kazimierza Pułaskiego i Polskiej Izby Dual-Use

Oddajemy w Państwa ręce raport, który powstał z przekonania, że najważniejsza zmiana w polityce bezpieczeństwa Sojuszu ostatniej dekady rozegra się nie na poziomie deklaracji, lecz na poziomie jej wykonania. Decyzja haska otworzyła przed Polską znaczną szansę, ale również zadanie: komponent 1,5% PKB można potraktować jako realny program budowy odporności państwa albo jako pozycję sprawozdawczą, którą wypełni się tym, co i tak zostałoby sfinansowane. Różnica między tymi dwiema drogami zadecyduje o tym, czy najbliższa dekada przyniesie trwały wzrost zdolności, czy jedynie nowy wskaźnik do raportowania.

Komponent pozamilitarny leży dokładnie na styku dwóch perspektyw, które zbyt często analizowane są osobno: myślenia o bezpieczeństwie państwa w kategoriach strategicznych oraz wiedzy o tym, jak realnie powstają zdolności – w fabrykach, laboratoriach, łańcuchach dostaw i kontraktach. Przekonaliśmy się, że jednostronna perspektywa nie wystarcza: strategia bez przemysłu pozostaje postulatem, a rozwój przemysłu bez ram strategicznych – zbiorem rozproszonych zamówień. Niniejszy raport jest próbą połączenia tych obszarów w jeden, spójny model kształtowania polityki państwa.

Debata publiczna o nowych celach NATO koncentrowała się dotąd na pytaniu „ile". Ten raport stawia pytania trudniejsze i, naszym zdaniem, ważniejsze: *na co*, *według jakich priorytetów* i *jak zweryfikować*, że wydane środki przełożą się na realną gotowość. Autorzy świadomie podkreślają, że nie jest to dokument zamknięty ani wiążący. Jest propozycją ram decyzyjnych – katalogu wydatków kwalifikowanych, hierarchii priorytetów i mechanizmów rozliczania – adresowaną do decydentów odpowiedzialnych za przekucie zobowiązania sojuszniczego w prawo, budżet i instytucje. Jego ambicją jest dostarczenie jednolitego podejścia, a zarazem stanowi punkt wyjścia do rozmowy, która i tak musi się odbyć, a której jakość przesądzi o efekcie.

Spoiwem całej tej propozycji jest jedna zasada: logika podwójnego zastosowania. Jesteśmy przekonani, że odporności nie da się zbudować jako osobnego, kosztownego sektora, który czeka bezczynnie na kryzys, który może nie nadejść. Państwa nie stać – ani finansowo, ani politycznie – na utrzymywanie zasobów martwych przez większość czasu. Dlatego każda złotówka z komponentu 1,5% powinna pracować podwójnie: schron, który na co dzień jest parkingiem czy stacją metra; sieć łączności kryzysowej, która obsługuje bieżące zadania służb; szpital, magazyn rezerw czy zdolności produkcyjne, które mają realną funkcję w czasie pokoju, a w razie wstrząsu płynnie przechodzą w tryb obronny. Takie podejście nie tylko obniża rzeczywisty koszt odporności i zwiększa poparcie społeczne lecz także – co dla nas kluczowe – wiąże bezpieczeństwo z gospodarką: buduje krajowe kompetencje, miejsca pracy i potencjał eksportowy zamiast finansować import gotowych rozwiązań. Podwójne zastosowanie nie jest więc jedną z technik, lecz warunkiem, by program 1,5% PKB był zarazem skuteczny i trwały.

Apelujemy zatem, by komponent 1,5% PKB potraktować nie jako koszt narzucony z zewnątrz, lecz jako kluczową szansę modernizacji państwa i wzmocnienia krajowego potencjału – szansę, której okno, wyznaczone harmonogramem funduszy europejskich i trwających prac legislacyjnych, jest wąskie i nie powtórzy się w tej skali. Odporność, którą zbudujemy w tej dekadzie, będzie służyć obywatelom niezależnie od tego, czy nadejdzie kryzys, którego się obawiamy. To jest, w naszym przekonaniu, najlepsza definicja inwestycji w bezpieczeństwo.

Zbigniew Pisarski
Prezes Zarządu
Fundacja im. Kazimierza Pułaskiego

gen. bryg. rez. dr. Adam Duda
Prezes
Polska Izba Dual Use

Podsumowanie zarządcze

Deklaracja Haska, przyjęta na szczycie NATO 24–25 czerwca 2025 roku, ustanowiła nowy standard wydatkowy Sojuszu na poziomie 5% PKB do 2035 roku, podzielony na 3,5% PKB na klasyczne zdolności militarne oraz nowy komponent 1,5% PKB przeznaczony na ochronę infrastruktury krytycznej, cyberbezpieczeństwo, gotowość cywilną, innowacje i bazę przemysłową. O ile zdolności wojskowe są w NATO precyzyjnie skatalogowane i rozliczane, o tyle komponent 1,5% pozostaje pojęciem rozproszonym, pozbawionym jednolitej definicji wydatków kwalifikowanych i mechanizmów weryfikacji. Niniejszy raport stanowi propozycję operacjonalizacji tego komponentu w warunkach polskich. Jego tezą przewodnią jest stwierdzenie, że odporność cywilna nie zastępuje potencjału militarnego, lecz warunkuje jego skuteczność, a głównym ryzykiem wdrożeniowym pozostaje „kreatywna księgowość", czyli wykazywanie rutynowych inwestycji cywilnych jako nakładów na odporność.

Kontekst zagrożeń uzasadnia pilność tej agendy. Granica między zagrożeniami militarnymi, a niemilitarnymi uległa praktycznemu zatarciu: sabotaż infrastruktury podmorskiej na Bałtyku, systematyczne cyberataki na administrację i operatorów infrastruktury krytycznej, zaburzenia łańcuchów dostaw surowców i leków oraz nasilające się wyzwania klimatyczne tworzą jedno, sprzężone środowisko presji. Polska jest na tym tle szczególnie eksponowana, pozostaje głównym celem rosyjskich operacji sabotażowych w Europie, których liczba wzrosła o 246% między 2023 a 2024 rokiem. Doświadczenia ostatnich lat pokazują przy tym, że to nie pierwsze uderzenie, a pierwsze godziny niesprawnej reakcji instytucjonalnej decydują o skali strat.

Punktem wyjścia raportu jest definicja: **za komponent odpornościowy uznaje się rozwiązanie, które w mierzalny sposób zwiększa zdolność państwa do ochrony ludności, utrzymania ciągłości działania i odtwarzania funkcji po zakłóceniu.** Wydatki proponuje się analizować w trzech powiązanych wymiarach: zasobu, zdolności i weryfikacji, przy czym to właśnie zdolność do bieżącego potwierdzenia, które zasoby są dostępne, sprawne i gotowe do użycia, jest dziś najsłabszym ogniwem systemu.

W wymiarze alokacyjnym pula 1,5% PKB oznacza dla Polski strumień rzędu 50–60 mld zł rocznie. Raport proponuje kierunkową matrycę wydatków opartą na zidentyfikowanych lukach:

- Schrony i budowle ochronne – 20% (~12 mld zł)
- Ochrona infrastruktury krytycznej – 20% (~12 mld zł)
- Cyberbezpieczeństwo – 15% (~9 mld zł)
- Gotowość cywilna i reagowanie kryzysowe – 15% (~9 mld zł)
- Innowacje i technologie bezpieczeństwa – 15% (~9 mld zł)
- Przemysł odpornościowy i łańcuchy dostaw – 10% (~6 mld zł)
- Zarządzanie, audyt i rezerwy – 5% (~3 mld zł)

Podział ten ma charakter modelu wyjściowego, otwartego na kalibrację w miarę dojrzewania metodologii rozliczania 1,5% w ramach Sojuszu.

Wyzwaniem nie jest brak źródeł finansowania, lecz ich koordynacja. Polska dysponuje portfelem instrumentów: od Programu Ochrony Ludności i Obrony Cywilnej, przez Fundusz Bezpieczeństwa i Obronności, po instrumenty unijne i sojusznicze. Kluczowe są dwa warunki: przestrzeganie zasady dodatkowości (nowe środki nie mogą zastępować istniejących budżetów sektorowych) oraz uniknięcie „klifu finansowego" po wygaśnięciu kwalifikowalności wydatków KPO. Fiskalną kotwicą po tym terminie pozostaje ustawowy próg minimum 0,3% PKB rocznie na zadania ochrony ludności.

Pogłębionej analizie sektorowej raport poddaje pięć kierunków o najgłębszej luce wyjściowej: budowę sieci schronów w modelu podwójnego zastosowania (finansowanie wyłącznie kosztów różnicowych obiektów pełniących w czasie pokoju funkcje komercyjne), zintegrowaną ochronę infrastruktury krytycznej i cyberprzestrzeni wraz z budową Systemu Bezpiecznej Łączności Państwowej, suwerenność w obszarze technologii kosmicznych, odporność systemu ochrony zdrowia oraz budowę krajowego przemysłu odpornościowego jako instrumentu reindustrializacji.

Raport przeformułowuje wreszcie samą naturę tych wydatków. W świetle modelu „potrójnej dywidendy z odporności" nakłady prewencyjne generują zwrot niezależnie od tego, czy kryzys nastąpi: poprzez uniknięcie strat, odblokowanie inwestycji oraz codzienne korzyści z infrastruktury dual-use. Rekomendacje raportu obejmują:

- przyjęcie oficjalnej definicji odporności i katalogu wydatków kwalifikowanych w nowej Strategii Bezpieczeństwa Narodowego oraz niezbędne zmiany ustawodawcze;
- ustanowienie organu koordynującego – Rady ds. Odporności przy Kancelarii Prezesa Rady Ministrów (KPRM) oraz, docelowo, Ministra ds. Odporności – zapewniającego planowanie wieloletnie zsynchronizowane z cyklem planowania obronnego NATO;
- oparcie rozliczania środków na mierzalnych wskaźnikach efektywności (audytowanych przez niezależne centrum weryfikacji, obejmujących nie tylko produkty inwestycyjne, lecz także potwierdzoną gotowość operacyjną zasobów);
- systemowe włączenie samorządów terytorialnych i organizacji pozarządowych jako pełnoprawnych ogniw architektury odporności, w modelu *whole-of-society*.

Konsekwentnie wdrożony, komponent 1,5% PKB może stać się nie kosztem, lecz mechanizmem modernizacji państwa w dekadzie 2026–2035. Bez precyzyjnych definicji, twardych mierników i rygorystycznej zasady dodatkowości grozi mu natomiast los kolejnego martwego wskaźnika.

CZĘŚĆ I

Wprowadzenie i kontekst strategiczny

1 Cel i zakres raportu

1.1 Wstęp

Współczesna architektura bezpieczeństwa europejskiego znajduje się w punkcie zwrotnym, wymuszającym odejście od dotychczasowych, często fasadowych modeli gotowości na rzecz realnej zdolności do przetrwania w warunkach długotrwałego kryzysu lub konfliktu zbrojnego. Raport stanowi propozycję analitycznej odpowiedzi na nowy standard wydatkowania w ramach Sojuszu Północnoatlantyckiego, który zakłada przeznaczenie łącznie 5% PKB na szeroko rozumiane bezpieczeństwo. W tym nowym paradygmacie fundamentalne znaczenie ma precyzyjne rozdzielenie nakładów na klasyczną obronność militarną (3,5% PKB) od inwestycji w odporność państwa i gotowość cywilną (1,5% PKB). Głównym zadaniem opracowania jest pełna operacjonalizacja tego drugiego komponentu, który dotychczas, choć obecny w debacie, w przeciwieństwie do precyzyjnie skatalogowanych zdolności wojskowych, pozostawał pojęciem rozproszonym w budżetach wielu resortów i pozbawionym jednolitych mechanizmów raportowania na poziomie sojuszniczym.

Operacjonalizacja komponentu 1,5% PKB wymaga nie tylko wskazania obszarów wydatkowania, lecz także określenia, jakie zdolności państwa mają zostać dzięki tym środkom zbudowane, utrzymane lub zweryfikowane. Wydatki odpornościowe powinny być oceniane przez pryzmat mierzalnego wpływu na ochronę ludności, ciągłość działania administracji i infrastruktury, zdolność reagowania na zakłócenia oraz możliwość potwierdzenia gotowości zasobów w warunkach kryzysowych.

Przyczyną podjęcia tej kompleksowej analizy jest identyfikacja głębokiej luki strukturalnej i definicyjnej wewnątrz NATO. O ile proces planowania obronnego pozwala na ścisłe monitorowanie potencjału armii państw członkowskich, to odporność struktur cywilnych pozostaje niemal wyłącznie domeną narodową, co w praktyce prowadzi do ogromnych dysproporcji między sojusznikami i utrudnia koordynację kolektywnej obrony. Pierwszorzędnym celem raportu jest zatem **zdefiniowanie katalogu wydatków kwalifikowanych w ramach kategorii 1,5% PKB.** Takie rozwiązanie ma zapobiec zjawisku „kreatywnej księgowości", w której państwa mogłyby próbować wykazywać standardowe inwestycje infrastruktury cywilnej jako nakłady na odporność. Katalog ten ma stanowić filtr, oddzielający bieżące wydatki państwa od celowych inwestycji w zdolności do absorpcji wstrząsów, takich jak wzmacnianie węzłów energetycznych czy budowa cywilnych struktur dowodzenia na czas wojny. Kryterium kwalifikacji nie powinno ograniczać się do formalnego przypisania wydatku do określonego

sektora, lecz powinno obejmować jego wpływ na realną, możliwą do audytu zdolność państwa do ochrony ludności, utrzymania funkcji krytycznych i przywracania działania po zakłóceniu.

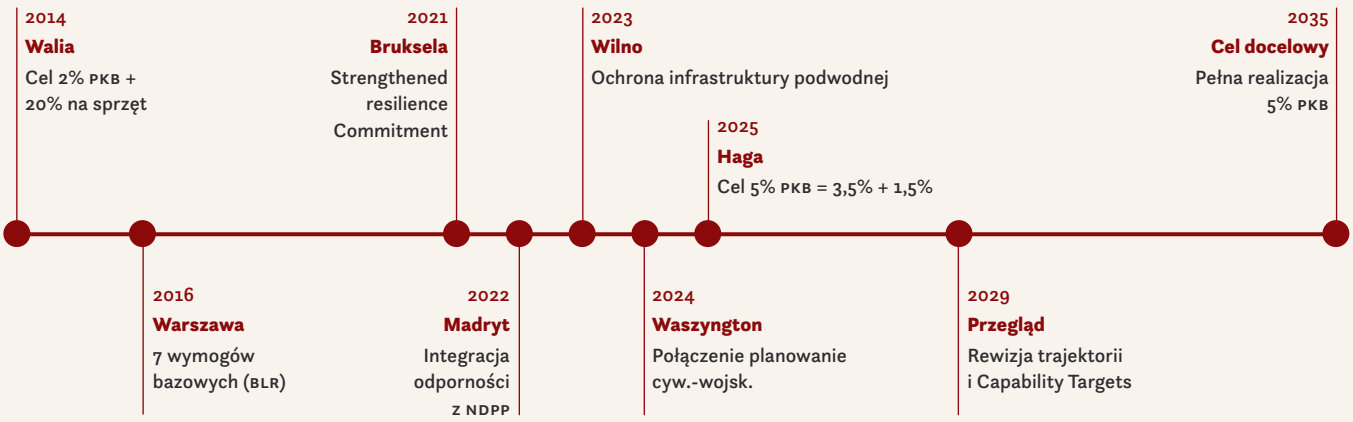
Kolejnym kluczowym zadaniem raportu jest **zaprojektowanie hierarchii priorytetów bezpieczeństwa i odporności.** W dobie ograniczonych zasobów i narastającej presji czasu, państwo musi dokonać strategicznego wyboru obszarów wymagających najszybszego dofinansowania. Raport proponuje odejście od rozproszonych działań na rzecz koncentracji na budowie bezpieczeństwa narodowego w sposób organiczny. Szeroki zakres analizy obejmuje schrony o podwójnym przeznaczeniu, prezentowane jako namacalny dowód gotowości państwa, budujący społeczną odporność psychologiczną, a także ochronę infrastruktury krytycznej oraz cyberbezpieczeństwo, traktowane jako system nerwowy państwa. Raport nie ogranicza się jednak do aspektów defensywnych, ale kładzie silny nacisk na innowacje i rozwój przemysłu. Wskazuje na konieczność budowy suwerenności technologicznej poprzez wspieranie krajowych rozwiązań B+R, które mogą stać się produktem eksportowym w ramach Sojuszu.

W wymiarze wykonawczym raport koncentruje się na wskazaniu mechanizmów wdrożeniowych i kontrolnych. Proponuje stworzenie architektury zarządzania funduszami, wykraczającej poza roczną perspektywę budżetową, wprowadzając trwałe mechanizmy finansowania przedsięwzięć realizujących cel 1,5%.

1.2 Geneza i ewolucja celu 5% PKB: Od szczytu w Walii do Deklaracji Haskiej

Ustanowienie nowego standardu wydatkowego na poziomie 5% PKB, obejmującego 3,5% na obronność militarną i 1,5% na odporność cywilną, stanowi jedną z kluczowych zmian doktrynalnych w planowaniu wydatków państw członkowskich Sojuszu Północnoatlantyckiego. Proces ten, choć będący wynikiem wieloletniej ewolucji postrzegania zagrożeń, został ostatecznie sformalizowany i przyjęty jako wiążący kierunek polityczny podczas Szczytu NATO w Hadze, który zakończył się przyjęciem Deklaracji Haskiej. Dokument ten ostatecznie pogrzebał podejście ze Szczytu w Walii z 2014 roku, które traktowało 2% PKB jako cel docelowy i zastąpił go nowym, dualnym miernikiem 5%, uznając, że w dobie wojny totalnej i zagrożeń wielodomenowych bezpieczeństwo militarne bez odporności cywilnej jest jedynie iluzją odstraszania.

Rysunek 1. Ewolucja paradygmatu odporności NATO 2014–2035



Geneza Deklaracji Haskiej tkwi w głębokiej weryfikacji zdolności operacyjnych państw europejskich w latach 2022–2024. Analiza konfliktów o wysokiej intensywności oraz operacji hybrydowych prowadzonych przez Federację Rosyjską wykazała, że **agresorzy coraz częściej uderzają w „miękkie podbrzusze" Sojuszu: systemy energetyczne, logistykę cywilną, nastroje społeczne oraz infrastrukturę krytyczną.** Podczas dyskusji poprzedzających szczyt, państwa wschodniej flanki NATO, z Polską na czele, podniosły argument o istnieniu „krytycznej luki odporności". Wskazywano, że nowoczesne armie, wyposażone w systemy piątej generacji, mogą zostać sparaliżowane w ciągu kilku dni, jeśli ich zaplecze cywilne nie będzie posiadało autonomicznych źródeł zasilania, bezpiecznych systemów łączności oraz wydolnego systemu schronów dla populacji. To właśnie ta argumentacja doprowadziła do sformułowania w Hadze podziału wydatków, który ma uchronić środki na odporność przed skonsumowaniem ich przez kapitałochłonne kontrakty zbrojeniowe.

Rysunek 2. Anatomia celu 5% PKB: „miecz i tarcza"

Deklaracja Haska, czerwca 2025 r. – podział na rdzeń militarny i filar odporności

Przyjęta w Hadze formuła 3,5% + 1,5% stała się nowym „złotym standardem" NATO. Deklaracja Haska precyzuje, że komponent 1,5% PKB ma być przeznaczony bezpośrednio na realizację siedmiu podstawowych wymogów odporności NATO (7 Baseline Requirements). Oznaczają one obowiązek finansowania przez państwa m.in. ciągłości funkcjonowania rządu, odporności sieci energetycznych, zdolności do zarządzania niekontrolowanymi ruchami ludności oraz, co kluczowe dla polskiego kontekstu, masowej budowy i modernizacji systemów budowli ochronnych. Realizacja tych wymogów wymaga nie tylko inwestycji infrastrukturalnych, lecz także zdolności do bieżącej oceny, czy finansowane zasoby pozostają dostępne, sprawne i możliwe do użycia w warunkach rzeczywistego kryzysu. Szczyt w Hadze nadał tym wymaganiom rangę zobowiązań operacyjnych, z których państwa członkowskie są rozliczane w ramach cyklu planowania obronnego NATO.

Perspektywa Deklaracji Haskiej zmienia również filozofię odstraszania. Przejście na model 5% PKB stanowi odejście od odstraszania przez odwet („deterrence by punishment") na rzecz odstraszania przez odmowę („deterrence by denial"). Dokument ze szczytu w Hadze wprost stwierdza, że państwo odporne, posiadające zabezpieczoną infrastrukturę krytyczną i chronioną ludność, jest celem nieopłacalnym dla agresora, gdyż koszt przełamania jego oporu psychologicznego i fizycznego przewyższa potencjalne zyski z agresji. W tym sensie inwestowanie w schrony, cyberbezpieczeństwo i odporność społeczną jest uznawane przez NATO za równie istotny wkład w bezpieczeństwo zbiorowe, co zakup eskadr samolotów wielozadaniowych.

Polska, przyjmując te standardy, staje się państwem referencyjnym NATO w dziedzinie odporności, wyznaczając kierunek modernizacji dla całego obszaru euroatlantyckiego. Deklaracja Haska z czerwca 2025 roku pozostaje fundamentem, na którym opiera się niniejszy raport, a podział wydatków na 3,5% – „miecz" i 1,5% – „tarczę" jest racjonalną strategią przetrwania i rozwoju państwa w nadchodzącej dekadzie 2026–2035.

1.3 Względność celu 5% PKB

Ustanowienie przez NATO w Deklaracji Haskiej nowego standardu wydatkowego na poziomie 5% PKB (3,5% + 1,5%) jest aktem o głębokim charakterze politycznym, który wykracza poza proste ramy planowania budżetowego. Jako wskaźnik makroekonomiczny, cel ten podlega zjawisku „politycznej względności" – jego realna skuteczność zależy nie od zapisów traktatowych, lecz od woli politycznej, stabilności koalicji rządzących oraz zdolności państw do absorpcji tak ogromnych środków bez naruszania fundamentów gospodarczych.

Fundamentalnym wyzwaniem dla wiarygodności nowego paradygmatu jest brak skutecznych narzędzi egzekwowania zobowiązań. Jak wskazuje raport International Centre for Defence and Security (ICDS) z września 2025 r.[1], historia progu 2% PKB z Walii (2014) udowodniła, że w strukturach NATO nie istnieją realne sankcje za niedopełnienie limitów wydatkowych. Względność celu 5% wynika z tego, że jego realizacja opiera się wyłącznie na mechanizmie nacisku sojuszniczego. Eksperci ICDS podkreślają, że złożenie obietnicy politycznej w blasku fleszy podczas szczytu jest relatywnie łatwe i przynosi natychmiastowe zyski dyplomatyczne. Jednak zapewnienie realnej implementacji w perspektywie dekady jest procesem znacznie trudniejszym. Istnieje uzasadnione ryzyko, że niektóre państwa będą stosować „kreatywną księgowość", wliczając do komponentu 1,5% bieżące wydatki na administrację czy infrastrukturę ogólnego przeznaczenia, tworząc iluzję bezpieczeństwa przy braku realnego wzrostu zdolności operacyjnych.

W kontekście tych wyzwań i obaw o kondycję finansów publicznych kluczowa staje się debata nad makroekonomicznym wpływem tak drastycznego skoku nakładów obronnych, często sprowadzana do klasycznego dylematu „masło czy armaty" (ang. *guns or butter*). Powszechnie zakłada się, że militaryzacja musi pociągać za sobą cięcia w sferze cywilnej, dławiąc konsumpcję i usługi państwowe. Jednakże, jak dowodzi raport Kilońskiego Instytutu Gospodarki Światowej[2], ten tradycyjny kompromis w rzeczywistości może być mylący. Autorzy opracowania argumentują przeciwko tezie, że kapitał, praca i surowce kierowane na wojsko zawsze hamują rozwój. Wręcz przeciwnie – z analiz IfW wynika, że jeśli państwa europejskie oprą swój rozwój na rodzimych innowacjach i produkcji regionalnej, zamiast masowo importować sprzęt, zwiększenie nakładów z 2% na 3,5% PKB może stymulować wzrost gospodarczy na poziomie od 0,9 do 1,5 punktu procentowego rocznie. Stąd też, silny nurt krytyczny płynie ze środowisk promujących ideę europejskiej autonomii strategicznej. Eksperci podważają zasadność skupiania się wyłącznie na wolumenie wydatków (ile?), postulując przejście do analizy jakościowej (jak i na co?). Wszystkie środki muszą być zainwestowane w sposób służący realnemu bezpieczeństwu Europy. Pogoń za wskaźnikiem 5% PKB może prowadzić do nieprzemyślanych zakupów „z półki" (głównie od dostawców spoza UE), co pogłębia technologiczną zależność Europy. Bez koordynacji na poziomie europejskim, gwałtowny wzrost wydatków o 1,5% PKB na odporność może doprowadzić do dublowania struktur i nieefektywnego rozdrobnienia przemysłowego. Z perspektywy autonomii strategicznej, cel 5% PKB ma sens tylko wtedy, gdy stymuluje europejską bazę przemysłowo-technologiczną. W przeciwnym razie jest to transfer kapitału, który osłabia europejską gospodarkę w długim terminie.

Umiarkowanie kategoryczny charakter celu 5% PKB jest również kontestowany przez państwa Europy Południowej, takie jak Hiszpania czy Włochy. Państwa południa argumentują, że ich główne wyzwania bezpieczeństwa – niestabilność w Sahelu, nielegalna migracja, terroryzm islamski – nie wymagają ciężkich dywizji pancernych, na które kładzie nacisk komponent 3,5% PKB. W krajach o wysokim zadłużeniu publicznym i problemach strukturalnych, decyzja o gwałtownym wzroście wydatków zbrojeniowych do 5% PKB jest „politycznie toksyczna". Władze Hiszpanii wielokrotnie podkreślały, że bezpieczeństwo to także spójność społeczna,

a radykalne przesunięcie środków z opieki zdrowotnej czy edukacji na schrony i rakiety może doprowadzić do destabilizacji wewnętrznej i wzrostu populizmu. Obiekcje te nie pozostały wyłącznie w sferze retoryki. W finalnym tekście przyjętym w Hadze Hiszpania, najniżej wydatkujący sojusznik, wynegocjowała faktyczne wyłączenie z wiążącego progu 5% PKB, deklarując utrzymanie nakładów na poziomie ok. 2,1% PKB, który jej zdaniem wystarcza do realizacji uzgodnionych celów zdolnościowych.

Względność celu 5% PKB sprawia, że jego sukces zależy od wypracowania nowej, inkluzywnej definicji „wydatków kwalifikowanych". Aby uniknąć paraliżu implementacyjnego i politycznej fragmentacji Sojuszu, zasadne jest ustanowienie jasnych wskaźników efektywności dla komponentu 1,5%, które będą audytowane przez niezależne instytucje sojusznicze, a nie tylko raportowane przez rządy. Wartym rozważenia jest również wzmocnienie preferencji europejskiej w zamówieniach publicznych, aby cel 5% PKB był postrzegany przez obywateli UE jako silnik wzrostu gospodarczego, a nie tylko koszt. Bez uwzględnienia powyższej krytyki, zwiększone cele w ramach Sojuszu mogą stać się kolejnym martwym wskaźnikiem, który zamiast budować odporność, pogłębi podziały wewnątrz świata zachodniego.

Osiągnięcie historycznego konsensusu w Hadze zapoczątkowało bezprecedensową reorientację w polityce fiskalnej i strukturalnej państw Sojuszu Północnoatlantyckiego. Przyjmując za punkt wyjścia obecne wskaźniki makroekonomiczne, łączny produkt krajowy brutto NATO można szacować na poziomie około 51 bilionów USD. Oznacza to, że alokacja zaledwie 1,5% tej sumy na pozamilitarny filar odpornościowy i ochronę infrastruktury krytycznej odblokowuje pulę środków rzędu ponad 800 miliardów USD rocznie. Jak wynika z modelowania długoterminowego SIPRI (Stockholm International Peace Research Institute – Sztokholmski Międzynarodowy Instytut Badań nad Pokojem), docelowa realizacja pełnego progu 5% PKB do 2035 roku, przy uwzględnieniu przewidywanej dynamiki wzrostu gospodarczego, wymusi na państwach członkowskich wygenerowanie nakładów w wysokości blisko 4,2 biliona USD rocznie[3]. Wartość ta stanowi przyrost o 2,7 biliona USD względem poziomu wydatków z 2024 roku, wynoszących wówczas około 1,5 biliona USD. Nawet w scenariuszu konserwatywnym, w którym zrealizowany zostaje wyłącznie tzw. rdzeń militarny na poziomie 3,5% PKB, oznaczałoby to niemal podwojenie dotychczasowych budżetów, podnosząc roczne wydatki Sojuszu do kwoty około 2,9 biliona USD. Skala tego obciążenia staje się jeszcze bardziej wyraźna z perspektywy największych gospodarek europejskich. Zgodnie z szacunkami SIPRI, do 2035 roku Niemcy zmuszone byłyby asygnować na szeroko pojęte bezpieczeństwo około 329 miliardów USD rocznie, Francja – 221 miliardów USD, a Włochy – 158 miliardów USD. Odstępstwem od tych projekcji wydają się prognozy ośrodka analitycznego Janes[4], wskazującego na pulę rzędu 2,36 biliona USD. Ten konserwatywny wariant analityczny uwypukla jednak wyzwania metodologiczne, w tym zróżnicowane podejścia do stóp inflacji, zmienności kursów walutowych oraz realnej absorpcji kapitału przez krajowe rynki zbrojeniowe.

1.4 Definicja wydatków na rzecz bezpieczeństwa i odporności kraju

Na potrzeby raportu, bezpieczeństwo i odporność kraju oznaczają zdolność państwa do:

- **ochrony ludności cywilnej**: ogół działań mających na celu zapewnienie bezpieczeństwa obywatelom państwa poprzez ochronę ich życia i zdrowia. Obejmuje ona również zabezpieczenie mienia, zwierząt, infrastruktury krytycznej niezbędnej do zaspokojenia potrzeb bytowych, a także dóbr kultury i środowiska naturalnego w sytuacjach bezpośredniego zagrożenia,
- **utrzymania ciągłości funkcjonowania instytucji publicznych:** zapewnienie niezakłóconego działania administracji państwowej oraz wspierających ją systemów teleinformatycznych i infrastrukturalnych, niezależnie od rodzaju wystąpienia zdarzenia kryzysowego. Proces ten obejmuje wdrożenie procedur zarządzania ciągłością działania, które pozwalają organom państwa na realizowanie swoich zadań publicznych w sytuacji wystąpienia zagrożeń o charakterze hybrydowym, naturalnym lub technicznym.
- **zapewnienia podstawowych usług (energia elektryczna, woda, łączność, transport):** tworzenie i utrzymywanie zasobów ochrony ludności, które są niezbędne do sprawnego udzielania pomocy doraźnej i humanitarnej. Działania te obejmują w szczególności gromadzenie zapasów wody wraz z systemami do jej magazynowania, transport i uzdatnianie, a także zabezpieczenie zapasowych źródeł energii oraz paliwa. W ramach tych zasobów utrzymuje się również zapasy żywności, odzieży, środków sanitarnych i higienicznych oraz produktów leczniczych i wyrobów medycznych. Ponadto system ten gwarantuje dostęp do miejsc tymczasowego pobytu, zapewniając kompleksowe wsparcie ludności w sytuacjach kryzysowych,
- **szybkiego reagowania i odtwarzania zdolności po zdarzeniu kryzysowym:** natychmiastowe podjęcie działań w momencie wystąpienia zagrożenia, w celu jego wyeliminowania lub zminimalizowania negatywnych skutków. Proces ten zakłada, że w jak najkrótszym czasie po ustąpieniu bezpośredniego niebezpieczeństwa, następuje odbudowa posiadanych wcześniej zasobów oraz potencjału ratowniczego. Integralnym elementem tego etapu jest szczegółowa analiza przyczyn i skutków kryzysu, która służy budowie nowych zdolności, mających na celu skuteczniejsze zapobieganie podobnym sytuacjom kryzysowym w przyszłości.

W ujęciu niniejszego raportu odporność państwa w obszarze ochrony ludności obejmuje zdolność administracji publicznej, infrastruktury publicznej, sektora prywatnego i obywateli do przygotowania, utrzymania oraz wykorzystania zasobów niezbędnych do ochrony ludzi w sytuacjach kryzysowych. Zasoby te obejmują w szczególności obiekty ochronne, miejsca czasowego pobytu i zakwaterowania, systemy łączności, cyberbezpieczeństwo, energię, wodę, logistykę, rezerwy materiałowe, kompetencje organizacyjne oraz mechanizmy bieżącej weryfikacji gotowości.

Za komponent odpornościowy należy uznać rozwiązanie, inwestycję, usługę lub zdolność organizacyjną, która w mierzalny sposób zwiększa zdolność państwa, samorządów, operatorów infrastruktury lub podmiotów wykonujących zadania publiczne do ochrony ludności, utrzymania ciągłości działania, ograniczania skutków kryzysu, przywracania podstawowych funkcji oraz podejmowania decyzji na podstawie wiarygodnych danych. Jedną z takich kategorii są systemy bieżącej weryfikacji gotowości zasobów odpornościowych, w tym systemy paszportyzacji, monitorowania i raportowania statusu obiektów ochrony ludności oraz miejsc czasowego zakwaterowania ewakuowanych. Ich rola polega na zapewnieniu administracji aktualnej informacji o tym, które zasoby są dostępne, sprawne, bezpieczne i możliwe do użycia.

Wydatki odpornościowe powinny być analizowane w trzech powiązanych wymiarach: zasobu, zdolności i weryfikacji.

- Zasób oznacza infrastrukturę, technologię, usługę, rezerwę lub kompetencję pozostającą do dyspozycji państwa.
- Zdolność oznacza możliwość użycia tego zasobu w określonym scenariuszu kryzysowym.
- Weryfikacja oznacza możliwość potwierdzenia, że zasób jest dostępny, sprawny, bezpieczny i możliwy do uruchomienia w wymaganym czasie.

W polskich dokumentach strategicznych nie ma jasno zdefiniowanego pojęcia „odporności", pomimo tego, że w Strategii Bezpieczeństwa Narodowego z 2020 roku poświęcono kwestii odporności państwa cały rozdział[5]. Pierwszy filar czyli *Odporność państwa i obrona powszechna* wskazuje na to, że odporność powiązana jest z obroną powszechną i całkowitym zaangażowaniem narodu w wysiłek obronny. Z kontekstu tego fragmentu strategii wynika, że chodzi głównie o zdolność struktur państwowych i społeczeństwa do działania w sytuacji zagrożenia; czyli zapewnienie ciągłości funkcjonowania państwa, ochrony ludności oraz wsparcia wojska[6]. Najlepszym rozwiązaniem tej kwestii byłoby uwzględnienie w nowej Strategii Bezpieczeństwa Narodowego standardu, w postaci oficjalnej definicji odporności państwa.

Próby usystematyzowania pojęcia odporności w polskim porządku prawno-strategicznym były już podejmowane. W 2021 roku Rządowe Centrum Bezpieczeństwa, w ramach prac nad Koncepcją kompleksowego wzmocnienia odporności, sformułowało roboczą definicję tego komponentu, określając go jako: „(...) zdolność państwa i społeczeństwa do przeciwstawienia się działaniom destrukcyjnym, zarówno zamierzonym jak i incydentalnym, a także zdolność do efektywnej odbudowy po ich wystąpieniu. Jest składową posiadanych zdolności cywilnych oraz potencjału militarnego". Mimo pełnej zgodności tego ujęcia z doktryną NATO, definicja ta nie została ostatecznie zaimplementowana do obowiązującego porządku prawnego. Wynikało to z braku finalnych rozstrzygnięć ustawodawczych w obszarze ochrony ludności oraz późniejszych sporów kompetencyjnych dotyczących docelowej roli i umiejscowienia Rządowego Centrum Bezpieczeństwa (RCB) w architekturze bezpieczeństwa państwa. Wymusza to konieczność ponownego zdefiniowania tego obszaru na potrzeby racjonalnego alokowania środków w ramach celu 1,5% PKB.[7]

W poszukiwaniu odpowiedniej definicji odporności pasującej do aktualnej sytuacji politycznej i międzynarodowej Polski należy przyjrzeć się definicjom stosowanym przez organizacje, w których Polska ma status członka. Tak na przykład, w Dyrektywie CER Unii Europejskiej (Critical Entities Resilience Directive) znajduje się definicja odporności: „[...] zdolność podmiotu krytycznego do zapobiegania incydentowi, ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie"[8]. Definicja Organizacja Traktatu Północnoatlantyckiego natomiast, wywodzi się z artykułu 3 *Traktatu Północnoatlantyckiego*: „Odporność odnosi się do zdolności do przygotowania się na wstrząsy i zakłócenia, stawiania im oporu, reagowania na nie i szybkiego odzyskiwania po nich równowagi."[9].

2 Kontekst strategiczny

Europa zmaga się z najbardziej złożonym środowiskiem zagrożeń od zakończenia zimnej wojny. W latach 2022–2025 czynniki, które jeszcze do niedawna funkcjonowały w dokumentach planistycznych jako scenariusze hipotetyczne, przeszły do operacyjnej codzienności. Sabotaż infrastruktury podwodnej, cyberataki paraliżujące systemy rządowe, zaburzenia łańcuchów dostaw surowców i leków, powodzie dezorganizujące logistykę wojskową to nie odrębne kategorie ryzyka, lecz sprzężone wymiary jednego środowiska, w którym granica między zagrożeniami militarnymi, a niemilitarnymi uległa praktycznemu zatarciu.

Szczyt NATO w Hadze był instytucjonalną odpowiedzią na tą rzeczywistość. Polska jako kraj zajmujący pierwsze miejsce w Europie pod względem liczby rosyjskich operacji sabotażowych, stoi przed wyzwaniem uzasadnienia, zaprojektowania i wdrożenia przewidzianych przez szczyt wydatków w sposób mierzalny i efektywny. Niniejszy rozdział określa kontekst zagrożeń, który to wyzwanie uzasadnia. Jego istotnym elementem jest również luka informacyjna dotycząca realnej gotowości zasobów cywilnych. W sytuacji kryzysowej państwo musi nie tylko posiadać infrastrukturę, procedury i zasoby, lecz także być zdolne do szybkiego ustalenia, które z nich są dostępne, sprawne, bezpieczne i możliwe do użycia. Brak takiej wiedzy wydłuża czas decyzji, zwiększa ryzyko błędnego rozmieszczenia ludności oraz ogranicza skuteczność reagowania administracji publicznej.

2.1 Nowe typy zagrożeń niemilitarnych: rosnąca skala i zmieniający się charakter

Wspólnym mianownikiem zagrożeń ostatnich lat jest ich hybrydowy charakter: są efektem działań poniżej progu otwartego konfliktu zbrojnego, uderzają w infrastrukturę cywilną i społeczną spoistość, a odpowiedzialność za nie jest trudna do jednoznacznego przypisania. Zagrożenia te nie są zjawiskiem jednorodnym. Narastają w kilku równoległy wymiarach, które razem tworzą presję strukturalną niemożliwą do zwalczenia przy użyciu środków militarnych wyłącznie.

Kolejną cechą łączącą ten typ zagrożeń jest również ich wpływ na dostępność i wiarygodność informacji operacyjnej. Ataki na infrastrukturę, zakłócenia łączności, awarie energetyczne, cyberincydenty oraz presja na administrację lokalną mogą prowadzić do sytuacji, w której państwo posiada zasoby formalnie ujęte w ewidencjach, ale nie ma aktualnej wiedzy o ich stanie, dostępności i zdolności do użycia. W warunkach kryzysowych taka luka informacyjna staje się samodzielnym czynnikiem ryzyka.

Najbardziej widoczny wymiar takich zagrożeń, to fizyczne ataki na infrastrukturę energetyczną i telekomunikacyjną. Rosja prowadziła wUkrainie najbardziej systematyczną kampanię niszczenia infrastruktury energetycznej od czasów drugiej wojny światowej: do połowy 2024 roku zniszczono lub uszkodzono prawie dwie trzecie ukraińskich zdolności wytwarzania energii elektrycznej, a tylko między marcem a wrześniem 2025 roku ukraiński sektor energetyczny doświadczył ponad 3100 przerw spowodowanych atakami.[10] Wzorzec ten przeniknął na terytorium NATO, a jego nowym teatrem stało się Morze Bałtyckie.

Od 2022 roku uszkodzeniu uległo około dziesięć podmorskich kabli i rurociągów na Bałtyku, z czego aż siedem w samym oknie czasowym od listopada 2024 do stycznia 2025 roku. We wrześniu 2022 roku sabotaż Nord Stream zniszczył trzy z czterech nitek gazociągu, uwalniając 778 mln m^3 gazu. W październiku 2023 roku chiński statek Newnew Polar Bear uszkodził gazociąg Balticconnector między Finlandią, a Estonią wraz z dwoma kablami telekomunikacyjnymi, powodując straty wymagające sześciu miesięcy napraw. W listopadzie 2024 roku chiński masowiec Yi Peng 3, wypływający z rosyjskiego portu Ust-Ługa, przeciął dwa kable telekomunikacyjne, wlokąc je kotwicą przez ok. 150 km dna morskiego. Jednym z nich był C-Lion1, stanowiący jedyne bezpośrednie połączenie kablowe Finlandii z Europą kontynentalną[11]. W Boże Narodzenie 2024 roku tankowiec floty cieni Eagle S uszkodził kabel energetyczny Estlink 2, redukując przepustowość transgraniczną z 1016 MW do 358 MW. Naprawa trwała do sierpnia 2025 roku, generując straty szacowane na 60–70 mln EUR[12]. NATO odpowiedziało środkami instytucjonalnymi. Szczyt wileński w 2023 roku po raz pierwszy wprost określił, że umyślny atak na krytyczną infrastrukturę sojuszników, w tym podwodną, spotka się ze zbiorową i zdecydowaną odpowiedzią[13]. W styczniu 2025 roku uruchomiono operację Baltic Sentry, rozmieszczając w regionie fregaty, okręty podwodne, morskie samoloty patrolowe i drony pod bezpośrednim dowództwem naczelnego dowódcy sojuszniczego w Europie (SACEUR)[14]. Szczyt waszyngtoński w 2024 roku ustanowił NATO Integrated Cyber Defence Centre przy SHAPE (ang. Supreme Headquarters Allied Powers Europe)[15].

Równolegle, szybciej rosnący wymiar to cyberzagrożenia. Polska stała się jednym z najczęściej atakowanych krajów na świecie: CERT Polska odnotowała ponad 80 200 incydentów w 2023 roku, a NASK ponad 100 000 incydentów w 2024 roku[16]. Dane CSIRT GOV (ang. Computer Security Incident Response Team) za 2024 rok dokumentują 1022 ataki na operatorów infrastruktury krytycznej, 736 na ministerstwa i 629 na urzędy publiczne, łącznie ponad 4000 ataków na sektor państwowy w ciągu jednego roku[17]. Skala tych ataków ma bezpośrednie przełożenie na zdolności operacyjne państwa. Uderzenie w ukraiński Kyivstar w grudniu 2023 roku pozbawiło łączności 24,3 mln abonentów na osiem dni, dezaktywowało systemy alarmów

przeciwlotniczych w Kijowie i Sumach oraz sparaliżowało terminale bankowe[18]. Analiza ENISA Threat Landscape 2024, obejmująca 11 079 incydentów w UE, wskazuje administrację publiczną jako najczęściej atakowany sektor – 19% wszystkich przypadków[19].

Kolejną kategorią są zagrożenia dla łańcuchów dostaw. Przegląd strategicznych zależności Komisji Europejskiej z 2021 roku zidentyfikował 137 produktów w newralgicznych ekosystemach jako krytycznie zależnych od zagranicznych dostawców, z Chinami odpowiadającymi za ok. 52% wartości importu najbardziej uzależnionych produktów unijnych[20]. W obszarze minerałów krytycznych Chiny dostarczają 100% pierwiastków ziem rzadkich i 97% magnezu do UE[21]. Po wprowadzeniu chińskich kontroli eksportowych w 2025 roku, kilku europejskich producentów samochodów zostało zmuszonych do wstrzymania produkcji. Polski Instytut Ekonomiczny w marcu 2025 roku oszacował, że nasz kraj importuje 321 kategorii towarów uznanych za kluczowe dla gospodarki, z najwyższymi wskaźnikami wrażliwości w sektorze biotechnologicznym i farmaceutyczno-obronnym[22].

2.2 Masowe zagrożenia dla ludności cywilnej

Zgodnie z prawem konfliktów zbrojnych – w szczególności Konwencjami Haskimi z 1899 i 1907 roku, IV Konwencji Genewskiej z 1949 roku[23], I Protokołem Dodatkowym do Konwencji Genewskich z 1977 roku (art. 1 ust. 4, Art. 8–34, a także cz. III, art. 35–79 oraz 80–91)[24] oraz zasadami prawa zwyczajowego, promowanymi przez Międzynarodowy Komitet Czerwonego Krzyża (MKCK)[25] – ludność cywilna podlega szczególnej ochronie w czasie konfliktów zbrojnych . Jednocześnie należy pamiętać, że aby móc kompleksowo spojrzeć na wyzwania bezpieczeństwa dla niewalczących, a także działać na rzecz zwiększenia odporności państwa oraz gotowości społeczeństwa do działania w sytuacjach kryzysowych, niezbędnym jest rozszerzenie definicji poza konflikty zbrojne. W wielu przypadkach masowe zagrożenie bywa również przedstawiane jako „katastrofa". Biuro Narodów Zjednoczonych ds. Redukcji Ryzyka Katastrof definiuje katastrofy jako „poważne zakłócenie funkcjonowania społeczności lub społeczeństwa na dowolną skalę, spowodowane niebezpiecznymi zdarzeniami oddziałującymi na warunki narażenia, podatności i zdolności, prowadzące do jednego lub kilku z następujących strat: strat (lub skutków) w ludziach, strat materialnych, ekonomicznych i środowiskowych"[26]. Definicja ta odnosi się do terminologii zawartej w Ramach z Sendai związanej z ograniczaniem ryzyk klęsk żywiołowych, promującej wspólne rozumienie i stosowanie wskazanej koncepcji (przyjęte przez Zgromadzenie Ogólne ONZ w lutym 2017 roku)[27]. Istnieją naturalnie również i odmienne metody analizowania omawianej tematyki. W wymiarze operacyjnym masowe zagrożenia dla ludności cywilnej wymagają nie tylko ewakuacji, lecz także wskazania, przygotowania i utrzymania miejsc, do których ludność może zostać skierowana. Obejmuje to zarówno obiekty ochronne i miejsca doraźnego schronienia, jak i obiekty czasowego pobytu oraz zakwaterowania ewakuowanych. Ich gotowość powinna być rozumiana szerzej niż sama dostępność przestrzeni, obejmuje dostęp do energii, wody, ogrzewania lub chłodzenia, sanitariatów, łączności, bezpieczeństwa, pojemności oraz warunków środowiskowych umożliwiających bezpieczne przebywanie ludzi.

Projekt EM-DAT, realizowany przez Uniwersytet Katolicki w Louvain oraz Centre for Research on the Epidemiology of Disasters, przedstawia „katastrofę" jako „sytuację lub wydarzenie,

przekraczające lokalne możliwości, wymagające zwrócenia się o pomoc zewnętrzną na szczeblu krajowym lub międzynarodowym; nieprzewidziane i często nagłe wydarzenie powodujące ogromne szkody, zniszczenia i cierpienie ludzi"[28]. Z kolei zgodnie z typologią zaproponowaną przez Andrzeja Żebrowskiego i Izabelę Szkurłat[29], kryzysy (wywołujące potencjalne masowe zagrożenia dla populacji cywilnej) podzielić można na dwie główne grupy (strefy), odnoszące się do państw członkowskich NATO:

1. Strefa bezpieczeństwa NATO:
- duże rozruchy lub kryzys społeczno-polityczny w państwie,
- operacja antyterrorystyczna (w odpowiedzi na ataki na ludność cywilną),

2. Poza strefą bezpieczeństwa NATO:
- wojny domowe w innych państwach,
- napięcia między państwami grożące wybuchem konfliktu lokalnego,
- przywracanie porządku po wybuchu konfliktu lokalnego,
- załamanie się władzy politycznej, czego rezultatem jest cierpienie ludności cywilnej,
- zagrożenie katastrofą nuklearną (środki wojskowe, awaria elektrowni, zagrożenia ekologiczne),
- zagrożenia dla obywateli NATO znajdującymi się na terytorium państw trzecich,
- zagrożenia morskich szlaków komunikacyjnych,
- międzynarodowa interwencja zbrojna przeciwko innemu państwu.

Dodatkowo, potencjalne zagrożenia tworzą bardzo szeroki katalog, do którego zaliczyć należy[30]:

1. **zagrożenia/katastrofy naturalne**

Zgodnie z definicją ONZ, „katastrofę naturalną" należy rozumieć jako „konsekwencje wydarzeń spowodowanych zagrożeniami naturalnymi, które przerosły lokalne zdolności odpowiedzi i w poważny sposób wpłynęły na społeczny i gospodarczy rozwój danego regionu"[31]. Zagrożenie katastrofami naturalnymi jest dodatkowo wzmacniane przez zmiany klimatyczne. Jak wskazują badacze z Uniwersytetu Nowojorskiego, rosnące temperatury przyczyniają się do zwiększania ilości pary wodnej w atmosferze, która to z kolei jest w stanie wywołać silniejsze burze. Również i wyższa temperatura wody oceanicznej prowadzi do zwiększenia prędkości wiatru, co prowadzi do powstania silniejszych huraganów, mogących wywoływać znacznie poważniejsze szkody. Susze z kolei niszczą i wprost uniemożliwiają uprawy, wpływając negatywnie na bezpieczeństwo żywnościowe i zdrowie publiczne (odwodnienie, udary cieplne, problemy z oddychaniem wywoływane burzami pyłowymi). Anomalie, które niegdyś zdarzały się rzadko, obecnie stają się codziennością, coraz silniej wpływając na życie i bezpieczeństwo ludzi[32]. Według danych EM-DAT, w 2024 roku odnotowano 393 katastrofy i zagrożenia naturalne, które doprowadziły do w sumie niemal 17 tys. śmierci, dotykając dodatkowo negatywnie 167,2 mln osób i powodując straty ekonomiczne wysokości 242 mld USD. Wśród najczęściej występujących katastrof należy wskazać na powodzie (142 przypadki) oraz gwałtowne burze (147 przypadków). Pod względem dotkliwości katastrof naturalnych dla lokalnej populacji, na pierwszych trzech miejscach uplasowały się Bangladesz (fale gorąca – 33 mln), Zambia (susza – 9,8 mln) oraz Filipiny (tajfun Trami – 9,7 mln)[33].

Przykłady największych zagrożeń/katastrof naturalnych w ostatnich latach:
- pandemia COVID-19 (2020–2023) – wybuch pandemii COVID-19 w skali globalnej nastąpił na przełomie 2019 i 2020 roku. Pierwsze epicentrum choroby zostało zlokalizowane w Chinach w grudniu 2019 roku, a w warunkach braku przygotowania znacznej większości państw, wirus SARS-CoV-2 szybko rozprzestrzenił się[34]. Pandemia ukazała ogromne braki w zapasach, gotowości oraz świadomości rządów, systemów opieki zdrowotnej i społeczeństw w zakresie zarządzania zdrowiem publicznym w warunkach rozprzestrzenienia patogenów o wysokiej zaraźliwości. Uwydatnione zostały braki kadrowe w zakresie rezerw, a także zdolności zdobycia środków zaradczych (szczepionki).
- powódź w Belgii (Walonia) (2021) – w powodzi zginęło 39 osób, poszkodowanych zostało 209 gmin, co przekłada się na ok. 32 tys. obiektów mieszkalnych. Analiza post-kryzysowa wykazała liczne zaniedbania oraz trudności w ramach zarządzania odpowiedzią na powódź. Przede wszystkim, złożony system struktur zarządzania w Belgii (podział kompetencji w ramach federacji) skomplikował efektywne, międzysektorowe i międzyagencyjne koordynowanie działań (pojawiły się

niejednoznaczności odnośnie ról, obowiązków i decyzyjności poszczególnych szczebli). Na to nałożyły się problemy komunikacyjne (opóźnienia w przepływie informacji między szczeblami), brak przygotowania i świadomości społecznej[35].

- powodzie w Pakistanie (2022) – pomiędzy czerwcem a sierpniem 2022 roku doszło do ogromnej powodzi, spowodowanej długim okresem ulewnych deszczy oraz przebraniem rzek. W katastrofie śmierć poniosło 1700 osób, ucierpiało ok. 33 mln, z czego niemal 8 mln zostało przymusowo przesiedlonych. Sytuacja stanowi dowód na to, jak bardzo zmiany klimatyczne są w stanie wpłynąć na życie i bezpieczeństwo ludzi. Pakistan uznaje się za jedno z dziesięciu najbardziej dotkniętych przez ocieplenie klimatu państw na świecie i już od pewnego czasu zmaga się on z ogromnymi wahaniami pogodowymi i ekstremalnymi zjawiskami. Latem 2022 roku, gdy doszło do powodzi, w Pakistanie odnotowano największą wilgoć powietrza od 1961 roku, a także znaczną ilość opadów deszczu (190% opadów tradycyjnie odnotowywanych w lipcu i sierpniu). Te z kolei nastąpiły po okresie fal upałów i suszy[36]. Pogorszenie warunków bytowych ludności doprowadziło ponadto do wzrostu przypadków zachorowań na malarię, a także cholerę (szczególnie u dzieci, które miały kontakt ze stojącą, brudną wodą)[37]. Kryzys nadszedł w wyjątkowo trudnym dla państwa okresie niestabilności politycznej i gospodarczej (rekordowy poziom inflacji, nadchodzące wybory, deficyt budżetowy oraz poważny deficyt w handlu zagranicznym), utrudniając zdolność szybkiej reakcji i zmuszając Pakistan do ubiegania się o międzynarodowe wsparcie[38].
- pożary w Kalifornii (2025) – w styczniu 2025 roku hrabstwo Los Angeles walczyło z serią katastrofalnych pożarów. Zgodnie z danymi California Department of Forestry and Fire Protection, w pożarach spłonęło ok. 23 tys. ha lasów, doszło również do zniszczenia 18 tys. budynków. Szybką odpowiedź na katastrofę utrudniały niebezpieczne warunki wiatrowe, a także ograniczenia w zapasach wody. Pożary stały się poważnym zagrożeniem dla lokalnej infrastruktury przeciwpowodziowej, wskazywano również na możliwość osuwisk[39]. W wyniku pożarów zginęło 31 osób. Badania Uniwersytetu Bostońskiego wykazały, że pożary mogą również wpłynąć na krótkoterminowy wzrost śmiertelności. Według szacunków w wyniku powikłań zmarło kolejne 409 osób.[40]
- Powódź w dolinie Ahr w Niemczech w lipcu 2021 roku pochłonęła ponad 130 ofiar, mimo że zagrożenie było prognozowane z kilkudziesięciogodzinny wyprzedzeniem przez Europejski System Ostrzegania Przeciwpowodziowego. Kluczowe uchybienia były systemowe, nie techniczne: syreny nie były w odpowiedni sposób utrzymywane lub mieszkańcy nie wiedzieli, jak interpretować ich sygnały; informacje między służbami federalnymi, landowymi i powiatowymi krążyły w zamkniętych pętlach, nie docierając do osób zagrożonych; urzędnicy na poziomie powiatów czekali na autoryzacje z wyższych szczebli zamiast działać. Raport komisji śledczej Bundestagu stwierdził, że system ostrzegania był technicznie sprawny, lecz proceduralnie niezdolny do skutecznego działania.[41]
- Trzęsienie ziemi w Turcji w lutym 2023 roku, które pochłonęło ponad 50 000 ofiar, pokazuje skalę, jaka moze osiagnac paraliż instytucjonalny innego rodzaju. Lokalne jednostki tureckiej agencji zarządzania kryzysowego (AFAD), dysponujące sprzętem i przeszkolonym personelem, czekały na instrukcje z Ankary zamiast natychmiast przystąpić do akcji ratunkowej. Zmarnowano krytyczne pierwsze 48 godzin, w których szanse przeżycia osób uwięzionych pod gruzami są najwyższe. Oceny humanitarne wskazują, że przynajmniej część ofiar mogła przeżyć przy szybszej mobilizacji lokalnych zasobów. Nadmierna centralizacja systemu dowodzenia, połączona z niedostatkami infrastruktury sejsmiczno-budowlanej, dała efekt skumulowany.[42]
- Pożary lasów w Grecji latem 2023 roku, w tym katastrofa na Rodos, wymusiły ewakuację około 20 000 osób, głównie turystów zagranicznych, bez przygotowanego zaplecza logistycznego. Kluczowym uchybieniem był brak spójnego przekazu między rządem centralnym, lokalnymi służbami ochrony ludności a branżą hotelarską. Turyści ewakuowali się bez informacji o drogach ewakuacji i miejscach docelowych. System alarmowy 112 wysyłał komunikaty do zbyt szerokich grup odbiorców, generując chaos zamiast porządku. Infrastruktura transportowa i komunikacyjna istniała, zabrakło protokołów koordynacji.[43]

2. **zagrożenia/katastrofy techniczne/technologiczne**

Zgodnie z danymi zebranymi w międzynarodowej bazie EM-DAT, katastrofy techniczne stanowią ok. 36,4% wszystkich zdarzeń zarejestrowanych od 1990 roku. Projekt Katolickiego Uniwersytetu w Louvain dzieli je na trzy główne podtypy: przemysłowe (wycieki chemiczne, eksplozje, pożary, zatrucia, promieniowanie, zawalenia, itp.), transportowe (powietrzne, kolejowe, drogowe, wodne), a także mieszane, integrujące elementy obu wcześniejszych kategorii[44].

- eksplozja w Libanie (sierpień 2020) – eksplozja azotanu amonu, który był składowany w bejruckim porcie, doprowadziła do 220 zgonów. Eksplozja rozbudziła również już istniejące niepokoje społeczne. Państwo wpadło w spiralę załamania gospodarczego, doprowadzając do pogłębienia katastrofy humanitarnej.
- awaria sieci energetycznej w Teksasie (2021) – ponad 4,5 mln gospodarstw w Teksasie utraciło dostęp do zasilania w czasie silnych mrozów. Awaria ujawniła krytyczne luki w zabezpieczeniach sieci elektroenergetycznej – jak się okazało, jej elementy nie zostały przygotowane do pracy w temperaturach poniżej zera, a w czasie jej budowy zastosowano nieodpowiednio modelowane obciążenia, które nie uwzględniały ekstremalnych warunków pogodowych[45].
- lokalne blackouty i niestabilność systemów przesyłowych – rosnący udział niestabilnych źródeł energii w miksie energetycznym stwarza nowe wyzwania dla bezpiecznego bilansowania sieci elektroenergetycznych. Przy jednoczesnym deficycie wielkoskalowych magazynów energii oraz elastycznych mocy rezerwowych, nagłe wahania generacji prowadzą do trudności z utrzymaniem parametrów jakościowych energii . Skutkuje to rosnącą podatnością na przeciążenia, co w konsekwencji prowadzi do coraz częstszych, lokalnych przerw w dostawach prądu lub wymusza planowe, prewencyjne odłączanie odbiorców w celu ratowania stabilności całego systemu.

3. **zagrożenia/katastrofy społeczne**

Zagrożenia społeczne mogą być w szerokim ujęciu rozumiane jako wydarzenia wiążące się z destabilizacją życia społecznego. Wymagają one reakcji organów państwowych, która może okazać się niewystarczająca i w efekcie prowadzić do dalszych trudności i pojawienia się nowych, jeszcze poważniejszych zagrożeń. Pierpaolo Donati definiuje katastrofy społeczne bardzo szeroko, uznając, że należy do ich grona zaliczyć wszystkie zjawiska będące „bezpośrednim lub pośrednim produktem działań człowieka, rozwinęły się w specyficznym kontekście społecznym i są ważne z punktu widzenia struktur społecznych i relacji społecznych", które mogą je dodatkowo zasilać. Do katastrof tych wlicza się m.in. pandemie (opisane już wcześniej), masowe migracje, czystki etniczne, czy ocieplenie klimatu – jako zjawiska, wywołane przez konkretną decyzję człowieka, lub będące wynikiem szeregu czynników wynikających z ludzkiej działalności[46]. Złożoność i mnogość zagrożeń społecznych wymaga więc wypracowania kompleksowego podejścia do problemu, który pozwoliłby na połączenie aspektów związanych z odpornością społeczną oraz świadomością obywatelską, z perspektywą „twardego bezpieczeństwa", związanego z przygotowaniem militarnym. Chociaż te dwa wymiary dość rzadko łączy się ze sobą, część ekspertów argumentuje, że w coraz szybszej erozji zaufania do instytucji oraz struktur społecznych zmiana myślenia jest niezbędna[47] – szczególnie obserwując aktualną „wojnę z cienia"[48], prowadzoną przez Rosję na terytorium państw Unii Europejskiej (korzystającą z tanich narzędzi pozwalających na podważanie zaufania do instytucji publicznych, normalizację przemocy, podsycanie polaryzacji oraz podważania spójności sojuszniczego aparatu bezpieczeństwa)[49].

2.3 Kryzysy klimatyczne i technologiczne

Zgodnie z definicją Programu Narodów Zjednoczonych ds. Rozwoju, kryzys klimatyczny jest zbiorem „poważnych problemów, które są lub mogą być spowodowane zmianami klimatu planety, w tym ekstremalnymi zjawiskami pogodowymi, zakwaszaniem oceanów i wzrostem poziomu mórz, obniżeniem bezpieczeństwa żywnościowego i wodnego, utratą bioróżnorodności, zagrożeniami dla zdrowia, wstrząsami gospodarczymi, przesiedleniami, a także konfliktami”[50]. Wzrost temperatury Ziemi o ok. 1,2 stopnia Celsjusza (w perspektywie ostatnich 200 lat) już obecnie prowadzi do istotnych trudności i zniszczeń, a ok. 3 mld osób żyje obecnie na terenach szczególnie zagrożonych skutkami zmian klimatycznych.

Najważniejsze wyzwania związane ze zmianami klimatu, dotykające Europy:

1. migracje klimatyczne (państwa UE jako potencjalny kierunek imigracji) – migracje klimatyczne definiowane są jako „stała lub czasowa zmiana miejsca zamieszkania, wywołana przyczynami środowiskowymi, związanymi z globalnym ociepleniem”. Tego rodzaju zmiany mogą dokonywać się nagle, lub stopniowo (np. w związku z katastrofami naturalnymi lub spodziewanym pogorszeniem stanu środowiska i zdolności do godnego życia w danym miejscu)[51].
2. ekstremalne zjawiska pogodowe i fale upałów – Europa ociepla się w tempie dwukrotnie wyższym niż średnia globalna, a skutki są już wymierne. W 2024 roku rekordowo wysokie temperatury roczne odnotowano na ok. 48% powierzchni kontynentu, przede wszystkim w Europie Środkowej, Wschodniej i Południowo-Wschodniej.[52] Latem 2024 roku (1 czerwca–30 września) w Europie odnotowano ok. 62 775 zgonów powiązanych z upałami, przy czym największe obciążenie dotyczyło osób starszych i kobiet[53]. W kolejnym sezonie skala zjawiska nie zmalała – szacuje się, że latem 2025 roku z upałami wiązało się ok. 24 400 zgonów w 854 europejskich miastach, z czego ok. 16 500 (ok. 68%) przypisano bezpośrednio zmianom klimatu; ponieważ analiza objęła miasta reprezentujące jedynie ok. 30% populacji Europy, rzeczywista liczba ofiar jest prawdopodobnie znacznie wyższa[54];
3. koszty gospodarcze i presja na finanse publiczne – skutki ekonomiczne zjawisk pogodowych i klimatycznych w UE wyniosły w latach 1980–2024 łącznie 822 mld EUR, przy czym aż 25% tej kwoty (ok. 208 mld EUR) zarejestrowano wyłącznie w ostatnich czterech latach (2021–2024), co wskazuje na rosnącą intensywność i częstotliwość zdarzeń[55]. Tempo narastania strat jest wyraźne: średnie roczne straty klimatyczne w UE wzrosły z ok. 8,5 mld EUR w latach 1980–1989 do 44,5 mld EUR w latach 2020–2023 – 2,5-krotnie więcej niż w poprzedniej dekadzie; w dłuższej perspektywie zmiany klimatu mogą obniżyć unijne PKB o ok. 7% do końca stulecia, przy stratach rzędu 2,4 bln EUR w latach 2031–2050, jeśli ocieplenie przekroczy 1,5°C[56]. Najnowsze szacunki – opracowane przez badaczy z Uniwersytetu w Mannheim we współpracy z ekonomistami Europejskiego Banku Centralnego – wskazują, że fale upałów, susze i powodzie z lata 2025 roku przyniosły co najmniej 43 mld EUR strat krótkoterminowych, a skumulowane straty makroekonomiczne mogą sięgnąć 126 mld EUR do 2029 roku[57];
4. niedobory wody i zagrożenie bezpieczeństwa żywnościowego – w 2023 roku warunki deficytu wodnego dotknęły ok. 28% terytorium UE przez co najmniej jeden sezon, a w maju 2024 roku poważna susza wiosenna objęła ok. 30% powierzchni lądowej Europy, głównie obszarów uprawnych[58]. W 2024 roku poważne susze objęły łącznie 601 193 km² Europy, a na obszarze 156 703 km² produktywność roślinności nie powróciła do poziomu referencyjnego (ok. 152 000 km²) – sygnał postępującego stresu adaptacyjnego ekosystemów[59];
5. utrata bioróżnorodności i degradacja ekosystemów – wzrost temperatury, zmiany wzorców opadów, zakwaszenie oceanów oraz rosnąca częstotliwość ekstremalnych zdarzeń pogodowych prowadzą do przesunięć

zasięgów habitatów i wymierania gatunków. Europejska Ocena Ryzyka Klimatycznego (EUCRA) z 2024 roku zidentyfikowała 10 kategorii poważnych zagrożeń klimatycznych dla ekosystemów lądowych i słodkowodnych kontynentu, podkreślając, że ryzyka krótkoterminowe są już dobrze udokumentowane, zaś skala zagrożeń długoterminowych w decydującej mierze zależy od poziomu globalnej redukcji emisji[60].

Powyższe wyzwania nie istnieją w oderwaniu od kwestii bezpieczeństwa i odporności – coraz wyraźniej je współkształtują. Zmiana klimatu działa jako „mnożnik zagrożeń" (threat multiplier): destabilizuje środowisko operacyjne sił zbrojnych, osłabia infrastrukturę krytyczną oraz generuje presje migracyjne i żywnościowe, które mogą stać się źródłem niestabilności politycznej. Zależność ta jest już uwzględniana w kluczowych dokumentach strategicznych Unii Europejskiej.

Kryzysy klimatyczne i technologiczne zwiększają znaczenie bieżącej wiedzy o stanie infrastruktury cywilnej. Fale upałów, powodzie, przerwy w dostawach energii, awarie sieci wodnych, zakłócenia transportu lub awarie systemów teleinformatycznych mogą szybko zmienić status obiektów przeznaczonych do ochrony, pomocy lub czasowego pobytu ludności. Dlatego odporność w tym obszarze wymaga nie tylko planów awaryjnych, lecz także zdolności do oceny stanu zasobów w czasie rzeczywistym lub w krótkich cyklach aktualizacji.

2.4 Zmiany klimatu i kwestia bezpieczeństwa w UE

Globalna Strategia UE 2016 wskazuje, że „zmiana klimatu i degradacja środowiska zwiększa prawdopodobieństwo potencjalnego konfliktu, w świetle wpływu na pustynnienie, degradację ziemi uprawnej, a także niedobory wody i pożywienia"[61].

Globalna Strategia UE postrzega zmiany klimatyczne jako przyczynę wstrząsów (zwłaszcza w krajach Afryki, Bliskiego Wschodu) i źródła zagrożeń bezpieczeństwa dla Unii (w kontekście m.in. bezpieczeństwa energetycznego, gospodarki). W kontekście zewnętrznym wskazuje na możliwość wpłynięcia na potencjalne konflikty (degradacja środowiska, pustynnienie, braki wody i żywności – konflikty o surowce niezbędne do życia) – zmiana klimatu wpływająca na brak pożywienia, pandemie czy przesiedlenia; wskazanie na współpracę z partnerami zewnętrznymi w kontekście przeciwdziałania zmianom klimatu, ale nie postrzega się tego w kontekście wojskowym oraz jako bezpośrednie przełożenie np. na europejskie zdolności obronne.

W ramach Strategicznego Kompasu, analizy zagrożeń, czyli tajnego raportu badającego kluczowe trendy globalne i regionalne, sporządzonego w listopadzie 2020 r. przez UE-27, wskazuje na „potencjał... czynników związanych z klimatem wpływających na stabilność krajową i regionalną". Zmiana klimatu jest wymieniona w Kompasie 17 razy, często odnosząc się do jej „efektu mnożnika zagrożeń". Wśród licznych sugerowanych działań dokument przedstawia propozycje dla sektora obronnego UE, takie jak większa efektywność energetyczna i zasoobooszczędność, w tym cel zmniejszenia śladu środowiskowego misji w ramach wspólnej polityki bezpieczeństwa i obrony (WPBiO), zgodnie z EGD, przy jednoczesnym zachowaniu skuteczności operacyjnej. Kompas podkreśla również rolę zielonych technologii i zrównoważonej cyfryzacji w siłach zbrojnych i sektorze obronnym. Zmiany klimatyczne są także uwzględniane w filarach odporności i partnerstwa planów UE w ramach Strategicznego Kompasu, w tym jako kluczowy temat współpracy z partnerami

wielostronnymi i regionalnymi w zakresie bezpieczeństwa i obrony.

Wskazuje się, że przyspieszone wydatki na obronność i działania w tym zakresie mogą być sprzeczne z częścią założeń klimatycznych UE – podniesienie wydatków na obronność i klimat jednocześnie może być niezrównoważone[62]. Istnieją jednak punkty wspólne obu tych obszarów, które można wykorzystać, aby sensownie zarządzać funduszami:

- czysta energia elektryczna – obniżenie europejskiej zależności od importu surowców i oparcie się na lokalnych źródłach OZE
- rozwój odnawialnych i niskoemisyjnych paliw – kluczowe dla dekarbonizacji lotnictwa, transportu morskiego oraz ciężkiego transportu drogowego, a także zapewnienia paliwa dla sektora wojskowego (które to jest zależne od cywilnego rynku paliw)
- zielone zaopatrzenie – kwestia transformacji przemysłowej w sektorze obronnym, niskoemisyjny przemysł
- sprawiedliwa transformacja w sektorze motoryzacyjnym – niewykorzystaną infrastrukturę produkcyjną przemysłu motoryzacyjnego należy wykorzystać do przyspieszenia modernizacji zdolności obronnych Europy, a jednocześnie do rozwiązania wrażliwego problemu społecznego związanego z zieloną transformacją
- krytyczne minerały – zabezpieczenie dostaw, kwestia dual-use wielu z tych minerałów, strategie magazynowania
- innowacje – wykorzystanie we współpracy ze środkami oferowanymi przez NATO (NATO Innovation Fund, DIANA)
- bezpieczeństwo i gotowość – zdolność planowania i gotowość na zaburzenia, monitorowanie infrastruktury, zagrożenie infrastruktury energetycznej atakami hybrydowymi

Swoje propozycje względem pogodzenia kwestii bezpieczeństwa z transformacją energetyczną i zmianami klimatycznymi przedstawił także Instytut Jacquesa Delorsa[63]. Instytucje wojskowe znalazły się w gronie pierwszych, które dostrzegły istotny wpływ klimatu, głównie w kwestii wpływu na misje humanitarne oraz zmieniający się charakter konfliktów. Niemniej w większości analiz kwestie klimatyczne wciąż często traktuje się jako drugorzędne, a czasem nawet w kontekście przeszkód regulacyjnych dla produkcji przemysłowej (przemysł obronny). Jednak takie spojrzenie jest błędne, a transformacja reprezentuje rzeczywistą szansę podążania w kierunku odpornego modelu energetycznego, który redukuje zależność od zasobów nieodnawialnych, wzmacnia autonomię baz militarnych poprzez mikro-sieci, a także dostarcza przewagi taktycznej (poprzez elektryfikację).

Podwójny priorytet w Deklaracji Wersalskiej z marca 2022 roku – silny mandat polityczny do inwestycji w EDTIB, a także zmniejszenie uzależnienia od rosyjskich surowców – te dwa zjawiska stały się ze sobą blisko zbieżne i współzależne. Kwestie te zostały również podkreślone w unijnych dokumentach (m.in. komunikat KE climate-energy nexus, a także Kompas Strategiczny, Readiness 2030). Warto jednak zauważyć, że w tych dokumentach sprawy klimatyczne są traktowane raczej płytko, postrzegane głównie jako „threat multiplier". Ochrona środowiska nie zostaje zniesiona, lecz podporządkowana imperatywowi przygotowania strategicznego. W ten sposób np. Europejski Omnibus (pakiet na rzecz uproszczeń regulacyjnych) ustanawia hierarchię, w której bezpieczeństwo staje się zasadą organizującą europejskie ramy prawne.

2.5 Cyberataki na administrację i usługi publiczne

Zgodnie z raportem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), dotyczącym cyberbezpieczeństwa administracji publicznej, na przestrzeni 2024 roku (od stycznia do grudnia) odnotowano 586 zgłoszonych incydentów. Większość instytucji administracji publicznej, które znalazły się na celowniku, to centralne instytucje rządowe, które padły ofiarą agresji w 69% wszystkich odnotowanych przypadków. Ataki na lokalne jednostki stanowiły ok. 24% zgłoszonych incydentów, natomiast na regionalne – 6,8%.

Ponad połowa ataków na centralne jednostki rządowe dotyczyła stron internetowych takich instytucji jak parlamenty, ministerstwa, czy agencje[64]. Wśród najpopularniejszych form wskazać należy na ataki DDoS (64%, w tym 46% zarejestrowanych przypadków przypisywane pro-rosyjskim haktywistom), zagrożenia związane z dostępem do danych (17,4%) oraz wykorzystanie ransomware (10%). Na przestrzeni ostatnich lat państwa europejskie musiały zmierzyć się ze stale rosnącą liczbą cyberataków, które – wraz z rozwojem technologii (szczególnie wyzwania wynikające z wykorzystania sztucznej inteligencji) – stają się coraz trudniejsze do odparcia i wymagają nowych form przeciwdziałania.

- Luty 2026 (Francja) – Ministerstwo Gospodarki Republiki Francuskiej ujawniło, że posługując się skradzionymi danymi uwierzytelniającymi, haker uzyskał dostęp do krajowego rejestru kont bankowych, wykradając wrażliwe informacje powiązane z ok. 1,2 mln kont (numery IBAN, nazwiska właścicieli, numery identyfikacji pocztowej, adresy zamieszkania);
- wrzesień 2025 (Wielka Brytania/Belgia/Niemcy) – w związku z atakiem ransomware doszło do zaburzeń w procesach boardingu na trzech europejskich lotniskach – w Londynie, Brukseli i Berlinie. Incydent wywołał konieczność manualnej odprawy i doprowadził do opóźnienia kilkuset lotów;
- luty 2024 (Niderlandy) – upublicznienie informacji o wykryciu złośliwego oprogramowania w sieci wojskowej Niderlandów, jeszcze w 2023 roku. Oprogramowanie zostało tam umieszczone przez chińskich szpiegów, którzy usiłowali uzyskać dostęp do wewnętrznego systemu Ministerstwa Obrony;
- styczeń 2024 (Szwecja) – rosyjscy hakerzy dokonali ataku z wykorzystaniem ransomware, którego celem padł dostawca usług cyfrowych dla rządu szwedzkiego. Atak doprowadził do kilkudniowych przestojów, a ich skutki odczuwane były w administracji publicznej jeszcze przez kilka następnych tygodni. Incydent miał miejsce w kontekście przygotowań Szwecji do wstąpienia do NATO;
- wrzesień 2023 (Wielka Brytania) – rosyjskim hakerom udało się wykraść tysiące dokumentów Ministerstwa Obrony Wielkiej Brytanii, które zostały następnie umieszczone w dark webie. W dokumentach znajdowały się informacje dotyczące m.in. bazy nuklearnej w Szkocji;
- sierpień 2023 (Polska) – atak rosyjskich hakerów doprowadził do paraliżu polskiego systemu kolejowego, co było możliwe dzięki dostępowi atakujących do częstotliwości linii kolejowych oraz wysłania złośliwego sygnału wstrzymującego ruch pociągów. W tym samym czasie hakerzy puścili przez głośniki na dworcach hymn Rosji oraz jedno z przemówień Putina, w którym mówi on o „operacji specjalnej" w Ukrainie.

Cyberataki nie odbywają się w próżni, ale w bardzo wielu przypadkach ich intensywność i liczba jest wprost uzależniona od aktualnego kontekstu polityki międzynarodowej, w ramach którego stają się one narzędziem nastawionym na celowe wyrządzenie szkody oraz zasianie niepokoju w społeczeństwie przeciwnika (element tzw. zagrożeń hybrydowych). Jak wskazują dane Eurostatu, Polska znajduje się w grupie państw najbardziej zagrożonych atakami; jest także trzecim (po Ukrainie i Wielkiej Brytanii) najczęstszym celem na kontynencie europejskim[65]. Z punktu widzenia odporności cywilnej cyberatak na administrację lub usługi publiczne nie oznacza wyłącznie utraty systemów informatycznych.

Może on również ograniczyć zdolność państwa i samorządów do ustalenia, które obiekty, usługi i zasoby pozostają dostępne dla ludności. Dlatego systemy wspierające ochronę ludności powinny być projektowane tak, aby zapewniały ciągłość dostępu do danych krytycznych, integralność informacji o gotowości zasobów oraz możliwość działania w warunkach ograniczonej łączności.

2.6 Wnioski: odporność cywilna jako wymóg strategiczny

Przywołane przypadki łączy wspólny mechanizm: zagrożenie lub katastrofa naturalna przekształca się w tragedię na dużą skalę nie w momencie pierwszego uderzenia, a w trakcie pierwszych godzin reakcji instytucjonalnej. Brak koordynacji między szczeblami administracji, niesprawne systemy ostrzegania, niedobory sprzętu utrzymywanego w gotowości, brak procedur dla ratowników i obywateli wielokrotnie przekładają się na ludzkie ofiary. Doświadczenia Ukrainy po 2022 roku potwierdzają to z drugiej strony: ponad 110 000 ochotników, którzy zaciągnęli się do Obrony Terytorialnej, oraz silne społeczeństwo obywatelskie okazały się czynnikami decydującymi o zdolności państwa do przetrwania. Badania AidData konkludują jednoznacznie: inwestowanie w odporność cywilną to nie opcjonalny dodatek, lecz fundament zdolności społeczeństwa do odstraszania, znoszenia i odbudowy po agresji.[66]

NATO formalnie uznało ten wymiar bezpieczeństwa na szczycie warszawskim w 2016 roku, definiując siedem wymogów bazowych odporności narodowej (Baseline Requirements for National Resilience): ciągłość rządzenia, odporne zaopatrzenie energetyczne, zarządzanie niekontrolowanymi ruchami ludności, bezpieczeństwo żywnościowe i wodne, zdolność do zarządzania masowymi stratami, odporna łączność oraz odporny transport. Decyzja haskiego szczytu z 2025 roku o dedykowaniu do 1,5% PKB na wydatki związane z obronnością i bezpieczeństwem niemilitarnym jest operacjonalizacją tego zobowiązania. Dla Polski ta decyzja stwarza zarówno obowiązek, jak i strategiczną szansę na nadrobienie wieloletnich zaległości. Zidentyfikowane powyżej zagrożenia stanowią ramę analityczną dla dalszej części raportu: definiują katalog wydatków kwalifikowanych, hierarchię priorytetów oraz mechanizmy wdrożeniowe opisane w kolejnych rozdziałach.

Z powyższych względów odporność cywilna powinna być traktowana jako zdolność do przygotowania, utrzymania, użycia i bieżącej weryfikacji zasobów potrzebnych do ochrony ludności oraz utrzymania ciągłości działania państwa. W praktyce oznacza to konieczność łączenia inwestycji infrastrukturalnych, organizacyjnych i technologicznych z mechanizmami aktualizacji danych, testowania gotowości, raportowania statusu zasobów oraz ćwiczenia procedur ich użycia.

3 Praktyka w państwach NATO

3.1 Metoda obliczania wydatków obronnych w ramach Sojuszu Północnoatlantyckiego

Metoda obliczania wydatków obronnych w ramach Sojuszu Północnoatlantyckiego stanowi fundament debaty o sprawiedliwym podziale obciążeń (burden sharing) i jest procesem znacznie bardziej złożonym niż proste sumowanie budżetów narodowych ministerstw obrony. Obecny standard, ewoluujący z historycznego celu 2% PKB w stronę nowej ambicji 3,5% na cele ściśle militarne, opiera się na ujednoliconej definicji NATO Defense Expenditure, która ma na celu zapewnienie porównywalności wysiłków państw o skrajnie różnych systemach budżetowych i strukturach sił zbrojnych[67]. NATO posługuje się ujęciem kasowym. W oficjalnym opisie metodologii (powtarzanym co roku w komunikacie *Defence Expenditure of NATO Countries*, czerwiec 2025) stwierdza się: „The amounts represent payments by a national government that have been or will be made during the course of the fiscal year to meet the needs of its armed forces, those of Allies or of the Alliance." Liczone są zatem płatności faktycznie zrealizowane (lub planowane do realizacji) w danym roku budżetowym, a nie zobowiązania w ujęciu memoriałowym ani szacunki rzeczowej wartości dostarczanego sprzętu. NATO równolegle korzysta ze źródeł makroekonomicznych: DG ECFIN Komisji Europejskiej, MFW i OECD, co oznacza, że publikowane przez NATO udziały wydatków w PKB mogą rozjeżdżać się z liczbami podawanymi przez stolice.

Dla komponentu 1,5% PKB ważne znaczenie ma nie tylko porównywalność kategorii wydatkowych między państwami, lecz także porównywalność efektów odpornościowych. Oznacza to, że praktyka raportowania powinna obejmować nie tylko informację o poniesionych nakładach, ale również o zdolnościach, które zostały dzięki nim zbudowane, utrzymane, zweryfikowane lub odtworzone.

Definicja obowiązująca od początku lat 50. (zaktualizowana w 2005 i 2018 r.) brzmi: „Defence expenditure is defined by NATO as payments made by an Allied national government (excluding regional, local and municipal authorities) specifically to meet the needs of (1) its own armed forces, (2) those of other Allies or (3) the needs of the Alliance as a whole." Władze regionalne, lokalne i samorządowe są więc z definicji wyłączone, a „potrzeby Sojuszu" oznaczają wyłącznie wspólne finansowanie NATO (NATO common funding) i fundusze powiernicze NATO (NATO-managed trust funds), których lista jest zatwierdzana przez wszystkich sojuszników.

Wewnątrz definicji wyodrębnia się cztery podstawowe kategorie:

- Personel, czyli wydatki na żołnierzy oraz pracowników cywilnych resortu obrony, w tym świadczenia emerytalne wypłacane bezpośrednio przez rząd zarówno emerytom wojskowym, jak i cywilnym pracownikom resortów wojskowych (tzw. military pensions), a także świadczenia dla aktywnego personelu.
- Sprzęt (equipment). „Equipment expenditure includes expenditure on major equipment as well as on research and development devoted to major equipment." Wydatki na B+R wliczane są nawet wtedy, gdy projekt nie zakończył się produkcją sprzętu. Składowanie zapasów wojennych gotowego sprzętu i materiałów do bezpośredniego użytku sił zbrojnych również jest zaliczane.
- Operacje i utrzymanie (O&M). Obejmują wydatki bieżące, paliwo, naprawy, transport, łączność, szkolenie, koszty operacji, misji i innych działań finansowanych z budżetu obronnego.
- Infrastruktura. „Expenditure on NATO common infrastructure is included in the total defence expenditure of each Ally only to the extent of that country's net contribution" – wydatki na wspólną infrastrukturę NATO uwzględnia się tylko w wysokości wkładu netto danego sojusznika (po pomniejszeniu o środki, które wraca do niego z NATO).

NATO dodatkowo wlicza wydatki na komponent wojskowy mieszanej działalności cywilno-wojskowej (lotniska, służby meteorologiczne, pomoce nawigacyjne, wspólne usługi zaopatrzeniowe, B+R), ale „only when the military component can be specifically accounted for or estimated". Pomoc finansowa i wojskowa udzielana sojusznikowi jest zaliczana donatorowi, a nie odbiorcy. Pomoc dla państw partnerskich może być wliczana wyłącznie poprzez wpłaty do uznanych przez Radę Północnoatlantycką funduszy powierniczych (a od 2025 r. także bezpośrednie wsparcie wojskowe Ukrainy).

W przypadku komponentu odpornościowego analogiczna metodologia powinna obejmować nie tylko przypisanie wydatku do określonej kategorii, lecz także wskazanie funkcji odpornościowej, którą dany wydatek realizuje. Oznacza to konieczność rozróżnienia między wydatkiem cywilnym o charakterze ogólnym a wydatkiem, który tworzy, wzmacnia lub weryfikuje zdolność państwa do działania w warunkach kryzysu.

Pakiet *Wales Defence Investment Pledge* z 5 września 2014 r. ustanowił dwa równoległe wskaźniki: 2% PKB na obronę oraz „at least 20% of defence expenditures should be devoted to spending on major equipment, including the associated research and development". NATO uzasadnia ten wskaźnik jako „crucial indicator for the scale and pace of modernisation", ostrzegając że jego niespełnienie grozi starzeniem się sprzętu, lukami zdolnościowymi i osłabieniem bazy przemysłowej. Wskaźnik 20% obejmuje sprzęt i wydatki B+R poświęcone temu sprzętowi, to definicja węższa niż całe wydatki sprzętowe i nie obejmuje bieżących zakupów drobnego wyposażenia czy umundurowania. W 2024 r. próg 20% osiągnęło 28 sojuszników (wg brytyjskiego MoD korzystającego z danych NATO z 28 sierpnia 2025 r.); w deklaracji haskiej 2025 wytyczna 20% nie została zniesiona, lecz rozpływa się w nowym, znacznie wyższym docelowym poziomie 3,5% PKB na rdzeń obronny.

Istotnym ograniczeniem jest również kwalifikowalność formacji paramilitarnych. NATO przyjmuje test funkcjonalny zaostrzony w 2004 r. Cytując definicję: „Armed Forces include land, maritime and air forces as well as joint formations, such as Administration and Command, Special Operations Forces, Medical Service, Logistic Command, Space Command, Cyber Command. They might also include parts of other forces such as Ministry of Interior troops, national police forces, coast guards etc. In such cases, expenditure is included only in proportion to the forces that are trained in military tactics, are equipped as a military force, can operate under direct military authority in deployed operations, and can, realistically, be deployed outside national territory in support of a military force."

Cztery kryteria kumulatywne to zatem: (1) wyszkolenie wojskowe; (2) wyposażenie wojskowe; (3) możliwość działania pod bezpośrednią komendą wojskową w operacjach ekspedycyjnych; (4) realna zdolność rozmieszczenia poza terytorium narodowym. Zmiana z 2004/2005 r. – określana przez SIPRI jako „NATO changed its definition in 2004 to exclude expenditure on paramilitary forces if they are not 'realistically deployable' " – miała znaczące skutki praktyczne. Najwyraźniejszy przypadek to Francja: od 2009 r. wydatki na Gendarmerie nationale zostały wyłączone z francuskich wydatków obronnych raportowanych do NATO, gdy formację przeniesiono do budżetu MSW (raport brytyjskiego Ministerstwa

Obrony *International Defence 2025*: „From 2009 French defence expenditure excludes the Gendarmerie which is now financed separately by the Ministry of the Interior. This change more accurately reflects the NATO definition for defence expenditure, but has led to lower levels of defence spending"). W konsekwencji Francja przekroczyła ponownie próg 2% PKB dopiero w 2024 r. – po raz pierwszy od 2009 r.

W przypadku polskich Wojsk Obrony Terytorialnej kryterium NATO jest spełnione w całości, ponieważ WOT są częścią Sił Zbrojnych RP finansowaną z budżetu MON i podlegają bezpośrednio ministrowi obrony. Z analogicznego klucza wlicza się włoskich Carabinieri (w proporcji wykonywania zadań wojskowych), Guardia Civil hiszpańską oraz amerykańską Coast Guard w wymiarze zadań związanych z obronnością.

Należy pamiętać również o potrzebie ujednolicenia różnic kursowych. NATO publikuje dwa zestawy szeregów: w cenach bieżących i bieżących kursach walutowych oraz w cenach i kursach stałych z 2021 r. (w wcześniejszych edycjach – z 2015 r.). Kurs przeliczeniowy to średnia roczna stopa publikowana przez Międzynarodowy Fundusz Walutowy dla każdego sojusznika. NATO zastrzega: „NATO uses United States dollars (USD) as the common currency denominator. The exchange rate applied to each Ally is the average annual rate published by the International Monetary Fund". Deflatory używane do przeliczeń na ceny stałe są wnioskowane z zestawienia szeregów cen bieżących i stałych publikowanych przez NATO. Skutkiem tej metody są zauważalne rozbieżności między danymi NATO a krajowymi: wahania kursowe (np. silna deprecjacja liry tureckiej) potrafią obniżyć dolarową wartość wydatków o 30–50% rok do roku, mimo wzrostów w walucie krajowej.

3.2 Interpretacje narodowe: jak sojusznicy definiują swój 1,5%

Deklaracja Haska z 25 czerwca 2025 roku pozostawiła cel 1,5% PKB celowo nieokreślony, pięć wymienionych obszarów poprzedzono formułą „*inter alia*". Polityczna elastyczność, która umożliwiła konsensus trzydziestu dwóch rządów, stała się jednocześnie źródłem zróżnicowanych, niekiedy sprzecznych, interpretacji krajowych. Sposób, w jaki poszczególne stolice wypełniają tę przestrzeń treścią, odsłania różnice nie tylko budżetowe, lecz przede wszystkim doktrynalne: fundamentalnie inne rozumienie tego, czym jest odporność i kto jest za nią odpowiedzialny.

Wielka Brytania

Zjednoczone Królestwo w *Rządowym Planie Działań na rzecz Odporności Wielkiej Brytanii* zdefiniowała odporność jako: „Zdolność do przewidywania, oceniania, zapobiegania, łagodzenia, weryfikowania, reagowania oraz odzyskiwania sprawności i wyciągania wniosków z zagrożeń naturalnych, celowych ataków, niestabilności geopolitycznej, wybuchów epidemii i innych zakłócających zdarzeń, sytuacji kryzysowych lub zagrożeń dla naszego stylu życia"[68]. Wielka Brytania jako jedna z pierwszych sformalizowała zobowiązanie haskie w ramach krajowego planowania budżetowego. Premier Keir Starmer ogłosił w czerwcu 2025 r., że Zjednoczone Królestwo osiągnie próg 5% PKB do 2035 roku w podziale na 3,5% na rdzeń obronny i 1,5% na odporność i bezpieczeństwo[69]. Kluczowe znaczenie dla oceny realności tego zobowiązania ma jednak jedno zdanie z towarzyszących dokumentów rządowych: kategoria 1,5% *„would be achieved by 2027–28 under pre-existing Spending Review plans"*[70]. Oznacza to, że przynajmniej w brytyjskim ujęciu, nowy cel formalnie nie wymaga zwiększenia łącznych wydatków publicznych, lecz jedynie przeklasyfikowania pozycji już zaplanowanych. Na podstawie tej nowej, dwuwarstwowej definicji

rząd szacuje, że łączny udział w PKB wyniesie „*at least 4,1% of GDP in 2027*" – do czego zaliczane będą m.in. wydatki wywiadowcze i środki funduszy bezpieczeństwa zintegrowanego pozostające poza budżetem Ministerstwa Obrony[71].

Merytoryczną podbudowę tego zobowiązania stanowi *Strategic Defence Review* (SDR) opublikowany w czerwcu 2025 roku, który formułuje odporność jako wymiar obejmujący całe społeczeństwo *„whole of society approach"* , i określa 62 rekomendacje transformacyjne do wdrożenia w ciągu dekady. SDR wskazuje, że Wielka Brytania stoi w obliczu zagrożeń nienotowanych od końca zimnej wojny[72]. W praktyce do kategorii 1,5% mogą trafiać wydatki Ministerstwa Spraw Wewnętrznych na infrastrukturę krytyczną, agencji wywiadowczych, programów cyberbezpieczeństwa National Cyber Security Centre oraz środki przeznaczone na wsparcie wojskowe Ukrainy[73].

Izba Gmin odnotowała precedens: Wielka Brytania sięgała już po elastyczność definicji NATO, by utrzymać deklarowany poziom 2% PKB w przeszłości – Komitet Obrony stwierdził w 2015 roku, że rząd niekiedy przesuwał słupki, reklasyfikując wydatki, zamiast rzeczywiście je zwiększać.[74] Krytycy wskazują, że schemat ten może się powtórzyć przy celu 1,5%, gdzie przestrzeń interpretacyjna jest jeszcze szersza. Institute for Fiscal Studies podkreśla, że wiarygodność zobowiązania haskiego zostanie poddana próbie dopiero wtedy, gdy rząd przedstawi szczegółowy podział między wydatkami już planowanymi a naprawdę nowymi nakładami.

Niemcy

Republika Federalna Niemiec w *Strategii odporności* swoją definicję odporności w bezpośredni sposób wywodzi z definicji stosowanej przez Organizację Narodów Zjednoczonych: „Odporność opisuje zdolność systemu, społeczności lub społeczeństwa narażonego na zagrożenia do stawiania oporu, absorbowania, przystosowywania się, przekształcania i odzyskiwania po skutkach zagrożenia w odpowiednim czasie i w sposób skuteczny, w tym poprzez utrzymywanie i przywracanie podstawowych struktur i funkcji za pomocą zarządzania ryzykiem"[75].

Podejście Niemiec jest pod wieloma względami najbardziej złożone ze wszystkich sojuszników, ale też, paradoksalnie, najbardziej transparentne, ponieważ wpisuje 1,5% w konkretny instrument legislacyjny. Kanclerz Friedrich Merz wymagał reformy konstytucyjnego hamulca zadłużeniowego jeszcze przed szczytem haskim: w marcu 2025 roku, większością dwóch trzecich głosów w Bundestagu i Bundesracie, znowelizowano Ustawę Zasadniczą, wyłączając wydatki obronne powyżej 1% PKB z liczenia do limitu zadłużenia[76]. Równolegle powołano Specjalny Fundusz Infrastruktury i Neutralności Klimatycznej (SVIK) z autoryzacją pożyczkową wynoszącą 500 mld euro na dwanaście lat, z których 300 mld euro przeznaczono na inwestycje federalne w siedmiu obszarach: ochronę cywilną, transport, cyfryzację, szpitale, infrastrukturę energetyczną, edukację oraz badania i rozwój[77].

Semantyczna ciągłość między SVIK a celem 1,5% NATO jest nieprzypadkowa. Business Sweden, analizując strategię modernizacyjną Bundeswehry, stwierdza wprost, że fundusz *„will contribute to NATO's goal of allocating 1,5% of GDP to infrastructure investment"*[78]. Budżet obronny Niemiec ma wzrosnąć z ok. 62 mld euro w 2025 roku do ponad 152 mld euro w 2029 roku, co według ministra finansów Larsa Klingbeila, pozwoli osiągnąć próg 3,5% PKB już przed 2030 rokiem[79]. Niemcy deklarują zatem spełnienie obu celów haskich z kilkuletnim wyprzedzeniem wobec terminu 2035 roku.

Dla celów 1,5% Niemcy przyjęły de facto podejście infrastrukturalne i jest to świadomy wybór geopolityczny. RFN jest logistycznym hubem wschodniej flanki NATO: przez jej terytorium przechodzi większość dróg zaopatrzenia dla sił rozmieszczonych w Polsce i państwach bałtyckich. Modernizacja tych sieci jest jednocześnie wymogiem cywilnym, ekonomicznym i wojskowym, klasyczny przypadek infrastruktury dual-use w rozumieniu definicji NATO[80]. Krytycy wskazują jednak na ryzyko: część środków SVIK trafi do projektów klimatycznych i edukacyjnych niemających bezpośredniego przełożenia na odporność wojskową, co może skutkować „kosmetycznym" wypełnianiem progu 1,5% wydatkami, które bez szczytu haskiego i tak by powstały.

Francja

Francja w *Narodowym Przeglądzie Strategicznym* odporność definiuje jako: „gotowość i zdolność kraju, społeczeństwa i rządu do przetrwania

skutków poważnego ataku lub katastrofy, a następnie szybkiego przywrócenia zdolności do normalnego funkcjonowania lub przynajmniej w sposób społecznie akceptowalny. Dotyczy to nie tylko władz publicznych, ale także podmiotów gospodarczych i całego społeczeństwa obywatelskiego”[81]. Paryż zaanonsował wzrost wydatków obronnych do 3,5% PKB, nie podając jednak wiążącego harmonogramu, co od razu spotkało się z krytyką jako nieprecyzyjne zobowiązanie[82]. Z perspektywy metodologicznej sytuacja Francji jest szczególna ze względu na historię Gendarmerie nationale, formacji liczącej ok. 100 000 żołnierzy, która od 2009 roku, po przeniesieniu do budżetu Ministerstwa Spraw Wewnętrznych, przestała być wliczana do wydatków obronnych raportowanych do NATO. Rzetelna dokumentacja NATO wyjaśnia tę zmianę jako zbliżenie do definicji sojuszniczej, jednocześnie przyznając, że spowodowała ona *„lower levels of defence spending”* w statystykach Sojuszu[83]. Gendarmerie spełnia jednak wojskowe kryteria NATO (szkolenie taktyczne, wyposażenie wojskowe, możliwość podporządkowania dowództwu wojskowemu), wobec czego Paryż ma techniczny argument za jej ewentualnym zaliczeniem, całościowym lub częściowym, do koszyka 1,5%.

Szerszą ilustracją jest kontekst systemowy: Francja po 1990 roku, podobnie jak Niemcy i Włochy, w znacznej mierze rozmontowała instytucjonalne struktury obrony cywilnej, przenosząc ciężar na zarządzanie kryzysowe w wymiarze niemilitarnym.[84] Odbudowa tych zdolności: zapasów strategicznych, planowania ewakuacji, sieci schronów, wymagałaby realnych nakładów i wieloletnich programów legislacyjnych, których Paryż dotychczas nie ogłosił. Obowiązująca *Loi de Programmation Militaire 2024–2030* koncentruje się na Armée de Terre, lotnictwie i programie nuklearnym, nie tworząc ram dla kategorii cywilnej odporności.

Holandia

Holandia w *Strategii bezpieczeństwa dla Królestwa Niderlandów* z 2023 roku zdefiniowała odporność jako: „Zdolność do przeciwdziałania zagrożeniom poprzez zmniejszenie prawdopodobieństwa ich wystąpienia, ograniczenie szkód w przypadku materializacji zagrożeń oraz umożliwienie odpowiedniej odbudowy. W tym celu wdraża działania na różnych etapach: od proaktywności (eliminowania przyczyn braku bezpieczeństwa) i prewencji (zapobiegania lub powstrzymywania zagrożeń na wczesnym etapie), poprzez przygotowanie (przygotowanie do skutecznej reakcji w przypadku wystąpienia zagrożeń), reagowanie (zwalczanie zagrożeń w momencie ich wystąpienia) i odbudowę (przywrócenie sytuacji do stanu normalnego lub nowego)”[85].

Jeszcze przed szczytem haskim holenderski rząd podjął decyzję o bezprecedensowym zwiększeniu budżetu obronnego do 3,5% PKB, z czego 1,5% PKB zostało wyraźnie wyodrębnione na wydatki zdefiniowane jako „matters that benefit defence”[86]. Początkowe komunikaty, w tym te publikowane na oficjalnej stronie government.nl, precyzowały to pojęcie dość wąsko, ograniczając je w głównej mierze do cyberbezpieczeństwa oraz wsparcia przemysłu obronnego. Taka interpretacja, zauważalnie węższa niż katalog wynikający z deklaracji haskiej, sugerowała początkowo dużą powściągliwość rządu w Hadze w odniesieniu do cywilnego wymiaru odporności państwa. Wynika to z głębokich uwarunkowań historycznych i instytucjonalnych:

Jak trafnie diagnozuje Bertelsmann Stiftung Europe, Holandia *„has never adopted a total defence concept and remains hesitant to embrace a whole-of-society approach to defence”*[87]. Przez trzy dekady od zakończenia zimnej wojny państwa Europy Zachodniej skupiały się na zarządzaniu kryzysowym w kontekście katastrof naturalnych i awarii przemysłowych, nie budując systemowej gotowości na wypadek konfliktu zbrojnego. W tym świetle, początkowe ograniczenie wydatkowania puli 1,5% PKB wyłącznie do cyberbezpieczeństwa i bazy przemysłowej wydawało się podyktowane politycznym pragmatyzmem. Był to wybór celów, które są łatwe do uzasadnienia przed opinią publiczną, a jednocześnie nie wymagają przełamywania wieloletnich oporów instytucjonalnych.

Hiszpania

Hiszpania ma długą historię umieszczania odporności w swoich dokumentach strategicznych. Nie tylko pod względem strategii bezpieczeństwa całego państwa, ale również w strategiach poświęconych konkretnym sektorom: cyberbezpieczeństwu, obronie cywilnej, dezinformacji, polityce obronnej, przeciwdziałaniu terroryzmowi, przestępczości zorganizowanej, zmianom klimatu itd[88]. W *Strategii Bezpieczeństwa Narodowego 2021* odporności opisano jako: „Aby zmniejszyć podatność na zagrożenia, łagodzenie ryzyka jest

równie istotne, jak wzmacnianie odporności, czyli zdolności do stawiania oporu, transformacji i odzyskiwania równowagi po niekorzystnych sytuacjach. Ponadto, aby zarządzać przyszłymi kryzysami i zapewnić dostęp do kluczowych zasobów, ważne jest zagwarantowanie, że łańcuchy dostaw tych zasobów nie będą nadmiernie uzależnione od źródeł zewnętrznych. Pomoże to również powstrzymać rozprzestrzenianie się kryzysów poprzez wzmocnienie odporności społeczeństwa i gospodarki"[89].

Pomimo to, Hiszpania jest jedynym sojusznikiem, który otrzymał explicite wyłączenie z celu haskiego. Premier Pedro Sánchez argumentował, że Hiszpania nie graniczy z Rosją i nie jest geograficznie narażona na te same ryzyka co państwa flanki wschodniej. Wskazywał też na priorytety polityki społecznej i ograniczenia budżetowe. Formalnie harmonogram do 2035 roku i przegląd w 2029 roku pozostają w mocy dla Madrytu, co oznacza, że wyłączenie jest politycznym rozejmem, nie trwałą derogacją. Napięcie transatlantyckie wokół przypadku Hiszpanii jest symptomatyczne. Stany Zjednoczone zareagowały zapowiedzią kompensat celnych, sygnalizując, że administracja Trumpa traktuje cel 5% nie tylko jako kwestię obronną, lecz także negocjacyjną. Analitycy wskazują jednocześnie, że Hiszpania historycznie wydaje więcej na obronę niż wynika z oficjalnych budżetów. Szacunki mówią o 20–30% ponadnormatywnych nakładach realizowanych poza linią budżetową MON, co oznacza, że faktyczna luka może być mniejsza, niż sugerują statystyki NATO.

Stany Zjednoczone

Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych na swojej stronie definiuje odporność jako: „Zdolność do przeciwstawiania się celowym atakom, wypadkom, klęskom żywiołowym, a także niekonwencjonalnym napięciom, wstrząsom i zagrożeniom dla naszej gospodarki i systemu demokratycznego oraz do szybkiego odzyskiwania po nich równowagi"[90].

Stany Zjednoczone nie mają problemu ze spełnieniem obu progów haskich – Sekretarz Generalny Rutte stwierdził publicznie, że USA *„are already spending almost 3,5% on core defence, and no doubt they are close to spending the 1,5% on defence-related capabilities"*. Przy wydatkach obronnych rzędu 967–980 mld dolarów rocznie i PKB przekraczającym 28 bln dolarów udział USA wynosi ok. 3,4–3,5% w komponencie militarnym. Komponent 1,5% jest de facto wypełniany przez wydatki Department of Homeland Security, inwestycje regulowane w sieci energetyczne i telekomunikacyjne (wymogi FERC dla sieci przesyłowych, wymiana sprzętu Huawei na mocy ustawy *Secure and Trusted Communications Networks Act*), a także wsparcie wojskowe Ukrainy, które deklaracja haska wprost uwzględniła w kalkulacji.

Normotwórcza rola Waszyngtonu polega jednak na czym innym: administracja USA wywiera presję na sojuszników, by kategorię 1,5% traktowali jako rzeczywiście nowe nakłady, a nie re-labeling istniejących wydatków. Atlantic Council postuluje, by NATO wzorując się na roli USA, powołało dedykowaną komórkę w Sekretariacie Generalnym monitorującą spójność narodowych interpretacji i identyfikującą dublowanie między komponentem 3,5% a 1,5%.[91]

Polska i flanka wschodnia: nadwyżkowe nakłady i luka gotowości cywilnej

Polska, Estonia, Łotwa i Litwa nie tyle zbliżają się do progów haskich, co je wyprzedzają , przynajmniej w warstwie ściśle militarnej. Dane Europejskiej Agencji Obrony za 2024 rok potwierdzają dominację regionu: Polska (3,8% PKB wg EDA), Estonia i Łotwa (po 3,3%), Litwa (3,1%), wobec Niemiec (2,1%), Francji i Włoch (po ok. 2%)[92]. Sekretarz Generalny Rutte otwarcie przyznał, że państwa flanki wschodniej są *„very close"* do spełnienia obu komponentów haskich, i wskazał je jako wzorzec dla pozostałych sojuszników.

Ten imponujący obraz ma jednak istotne pęknięcie po stronie cywilnej. Bertelsmann Stiftung Europe ocenia, że Polska, mimo militarnej przewagi: *„the integration of civil preparedness and societal involvement remains limited"*[93]. Przełomem legislacyjnym była dopiero ustawa o ochronie ludności i obronie cywilnej z grudnia 2024 roku, która ustanowiła minimalne finansowanie na poziomie 0,3% PKB i uruchomiła Program Ochrony Ludności i Obrony Cywilnej z alokacją 34 mld zł na lata 2025–2026. Polska jest zatem w unikalnej sytuacji: nakłady wojskowe z nadwyżką wypełniają próg haski, podczas gdy koszyk cywilny: gotowość społeczeństwa, schrony, zapasy strategiczne, system ochrony zdrowia, dopiero buduje pierwszą generację instytucji.

Z perspektywy haskiej metodologii oznacza to paradoks: kraj, który formalnie jest najbliżej spełnienia obu progów PKB, jednocześnie ma do pokonania największą odległość w najtrudniejszym do zmierzenia wymiarze, integracji obronności z gotowością społeczeństwa. Badanie ankietowe przeprowadzone w Polsce i Niemczech pokazuje zresztą, że gotowość deklaratywna bywa oderwana od systemowej: 61,6% Polaków wyraża gotowość osobistego udziału w obronie kraju, wyraźnie więcej niż 45,5% w Niemczech, lecz spójność instytucjonalna pomiędzy wojskiem a strukturami cywilnymi pozostaje achillesową piętą obu państw[94].

Wspólny mianownik: ryzyko „kreatywnej księgowości"

Przegląd interpretacji narodowych ujawnia strukturalny problem, który SIPRI, Janes i Carnegie zgodnie nazywają ryzykiem „kreatywnej księgowości": przy braku operacyjnej taksonomii i organu weryfikującego każde państwo może, i prawdopodobnie będzie, budować własną narrację o spełnieniu celu 1,5%, selektywnie dobierając pozycje z różnych portfeli resortowych[95]. Washington Times celnie podsumowuje: *„Critics warned that including security-related items could allow countries to meet targets on paper without enhancing military capability"*. Równocześnie nie należy ignorować pozytywnej dynamiki: po raz pierwszy od zakończenia zimnej wojny wszystkie główne sojusznicze gospodarki, w tym historycznie opieszałe Niemcy, podjęły wielomiliardowe zobowiązania infrastrukturalne i obronne z wiążącymi harmonogramami parlamentarnymi. Nawet jeśli część środków jest reklasyfikacją wydatków już planowanych, skala i prędkość zmian budżetowych w 2024–2025 roku nie mają precedensu od dziesięcioleci. Otwarte pytanie brzmi, czy wola polityczna szybkich sojuszników zdoła ustanowić standard rozliczalności zanim wolniejsi znajdą sposoby, by go ominąć[96].

3.3 Zasady finansowania wydatków 1,5%

Deklaracja haska ustanowiła nowy cel wydatków, ale nie stworzyła do niego instrumentów finansowych. NATO nie posiada wspólnego mechanizmu dotacyjnego ani funduszu, z którego sojusznicy mogliby czerpać środki na wydatki w kategorii 1,5% PKB. Zobowiązanie ma charakter czysto fiskalny: każde państwo ma samodzielnie zaplanować, sfinansować i raportować wydatki z własnych zasobów publicznych lub prywatnych, a następnie przedstawić NATO roczny plan wskazujący wiarygodną i przyrostową ścieżkę dochodzenia do celu.

Architektura finansowa zobowiązania wyraża się w kilku zasadach formalnych. Po pierwsze, cel sformułowano jako pułap górny, a nie minimum: sojusznicy „account for up to 1,5% of GDP" – co oznacza, że 1,5% to wartość maksymalna, do której mogą być zaliczane wydatki niemilitarne, nie zaś kwota wymagana jako nieprzekraczalny dolny próg. Po drugie, sojusznicy zobowiązali się do składania corocznych planów krajowych. Po trzecie, przewidziano przegląd trajektorii i bilansu wydatków w 2029 roku, z uwzględnieniem ówczesnego środowiska strategicznego i zaktualizowanych NATO Capability Targets[97].

Finansowanie komponentu 1,5% powinno obejmować pełny cykl życia zdolności odpornościowej: projektowanie, budowę lub zakup, wdrożenie, utrzymanie, testowanie, ćwiczenia, aktualizację danych, audyt oraz odtworzenie zdolności po zakłóceniu. Ograniczenie finansowania wyłącznie do nakładów inwestycyjnych zwiększa ryzyko powstania zasobów, które istnieją formalnie, ale nie są utrzymywane w gotowości operacyjnej.

Mechanizm raportowania oparty jest na dotychczasowej metodologii kasowej NATO, która od początku lat 50. XX wieku stosowana jest do liczenia wydatków obronnych w kategorii 2%, a od 2025 roku również 3,5%. Metodologia ta obejmuje płatności faktycznie dokonane lub zaplanowane przez rząd centralny (z wyłączeniem władz regionalnych i samorządowych) na potrzeby własnych sił zbrojnych, sił innych sojuszników lub całego Sojuszu. Kluczowe ograniczenie: istniejącą definicja NATO Defence Expenditure odnosi się wyłącznie do komponentu militarnego. Strona internetowa NATO poświęcona wydatkom obronnym zawiera szczegółową taksonomię kwalifikowalności dla kategorii 3,5%, natomiast analogiczna listy, definicji ani kryteriów dla kategorii 1,5% nie opublikowała.

Jedynym pierwotnym mechanizmem weryfikacyjnym są zatem plany krajowe. Pierwotna propozycja Sekretariatu NATO zakłada zobowiązanie do rocznych przyrostów wydatków o 0,2 punktu procentowego aż do osiągnięcia docelowego poziomu – co nadawałoby planowaniu krajowemu mierzalne, weryfikowalne kroki. Propozycja ta została odrzucona w trakcie negocjacji przed szczytem haskim, gdy część rządów sojuszniczych sprzeciwiła się mechanizmowi, który „przyparłby ich do muru". W efekcie deklaracja wymaga jedynie „wiarygodnej i przyrostowej ścieżki" – kryterium ocenianego przez samych sojuszników i ich pełnomocników w NATO[98]. Ambasador USA przy NATO Matthew Whitaker zasygnalizował po szczycie, że Waszyngton będzie oczekiwał od sojuszników „większej czujności we wzajemnym rozliczaniu się z roku na rok"[99], jednak ani konkretny mechanizm, ani sankcje za niespełnienie kroków pośrednich nie zostały włączone do deklaracji haskiej.

W 2025 roku wszyscy sojusznicy po raz pierwszy od dziesięcioleci osiągnęli lub przekroczyli próg 2% PKB, a europejscy członkowie i Kanada łącznie przeznaczyli na obronność ponad 574 mld USD (w cenach z 2021 r.), zwiększając wydatki o 20% rok do roku[100]. Ten postęp stanowi silny argument na rzecz skuteczności systemu politycznej presji bez formalnych sankcji, ale sceptycy wskazują, że akces ten nastąpił po ośmiu latach opóźnień względem celu Walii z 2014 roku. Pytanie, czy ta sama dynamika zadziała dla znacznie bardziej złożonej i trudniejszej do weryfikacji kategorii 1,5%, pozostaje otwarte.

3.4 Zasady wydatkowania środków kwalifikowanych do 1,5% PKB

Katalog wydatków kwalifikowanych do kategorii 1,5% PKB został w deklaracji haskiej celowo pozostawiony otwarty. Kluczowe sformułowanie brzmi: sojusznicy będą „przeznaczać do 1,5% PKB rocznie **inter alia** na ochronę naszej infrastruktury krytycznej, obronę naszych sieci, zapewnienie gotowości cywilnej i odporności, wyzwolenie innowacji oraz wzmocnienie naszej bazy przemysłowo-obronnej". Łacińskie inter alia – „między innymi" – oznacza w praktyce, że żaden z wymienionych obszarów nie jest ani wyczerpującym, ani wyłącznym katalogiem. Deklaracja nie zawiera definicji żadnego z pięciu obszarów, nie wskazuje dolnych progów alokacji dla poszczególnych kategorii ani nie precyzuje, czy wydatki raz zaliczone do 3,5% mogą być równocześnie raportowane jako część 1,5%.

Z perspektywy metodologicznej szczytu haskiego jest to ewidentna luka architektoniczna. Janes trafnie zauważyło, że deklaracja haska jest „najkrótszym oświadczeniem przyjętym na tym poziomie spotkania NATO"[101], a polityczna elastyczność, która umożliwiła konsensus trzydziestu dwóch rządów, automatycznie staje się przestrzenią interpretacyjną dla każdego

Tabela 1. Kwalifikowane obszary wydatków z podziałem na oryginalną terminologię deklaracji

Nr	Kategoria	Brzmienie oryginalne (j. angielski)
1	Ochrona infrastruktury krytycznej	protect our critical infrastructure
2	Obrona sieci	defend our networks
3	Gotowość cywilna i odporność	ensure our civil preparedness and resilience
4	Innowacje	unleash innovation
5	Baza przemysłowo-obronna	strengthen our defence industrial base

z nich z osobna. Łącznie 1,5% PKB sojuszniczego to ok. 825 mld USD rocznie – zasoby porównywalne z rocznym budżetem obronnym USA[102]. Sposób ich wydatkowania będzie mieć trwałe konsekwencje dla zdolności kolektywnych NATO, tymczasem wspólnych reguł ich definiowania wciąż nie ma.

Bertelsmann Stiftung Europe, w najgruntowniejszej jak dotąd analizie konsekwencji deklaracji haskiej dla wydatków militarnych, diagnozuje te sytuacje jako kategorie „konceptualnie szeroka, funkcjonalnie nieokreślona i otwarta na narodową interpretację"[103]. SIPRI również stwierdza wprost, że „nadal nie jest jasne, co kwalifikuje się do dodatkowego 1,5%", wskazując na ryzyko, że wydatki na „rozwijanie bazy przemysłowo-obronnej" lub infrastrukturę obronną mogłyby również z powodzeniem spaść do kategorii rdzenia militarnego 3,5%[104]. Brak delimitacji między dwoma komponentami celowo pozostawia sojusznikom swobodę, ale również pole do oportunistycznej reklasyfikacji.

Atlantic Council w analizie opublikowanej w lutym 2026 roku, kilka miesięcy przed szczytem w Ankarze, podsumował ten stan jednym zdaniem: „poza ogólnymi kategoriami wymienionymi w komunikacie NATO nie przedstawiło żadnych dalszych szczegółów dotyczących tego, jakie elementy krajowego PKB powinny być uwzględniane w rozliczeniu 1,5%". Oba dokumenty, Bertelsmann i Atlantic Council, wskazują na identyczną przyczynę: inaczej niż 3,5%, które są kalibrowane przez NATO Defence Planning Process i powiązane z konkretnymi celami zdolnościowymi (Capability Targets), kategoria 1,5% nie ma analogicznej struktury planistycznej ani mechanizmu weryfikacji zdolnościowej.

Różnice interpretacyjne ujawnione w ciągu kilku miesięcy po szczycie haskim potwierdzają tę diagnozę. Państwa południowoeuropejskie argumentowały na rzecz włączenia do katalogu 1,5% zdolności reagowania na klęski żywiołowe, powołując się na agendę bezpieczeństwa klimatycznego NATO. Niemcy skoncentrowały debatę krajową na inwestycjach infrastrukturalnych, wskazując na swoją rolę logistycznego hubu wschodniej flanki oraz na sięgające setek miliardów euro, latami zaniedbane zaległości drogowe i kolejowe. Państwa nordyckie i bałtyckie, zwykle wskazywane jako wzorzec całospołecznego podejścia do odporności („whole-of-society approach"), napotkały odwrotny problem: przy rozumieniu obronności jako wysiłku całego społeczeństwa trudno wskazać, co można z niego faktycznie wykluczyć.

Ambasador Whitaker w briefingu dla prasy przed szczytem haskim powiedział: „to nie jest worek, do którego każdy może po prostu wrzucać dodatkowe wydatki. To kluczowe rzeczy takie jak infrastruktura umożliwiająca mobilność wojskową. Możemy mieć najlepsze czołgi na świecie [...] ale jeśli nie można tych czołgów dostarczyć na linie frontu, bo drogi lub mosty lub kolej nie mogą udźwignąć ich wagi i tonażu, to są one bezużyteczne"[105]. Kilka miesięcy później, we wrześniu 2025 roku, Washington Times cytowało Whitakera jako stwierdzającego, że nowe wydatki obronne nie powinny obejmować „mostów, które nie mają strategicznej wartości wojskowej"[106]. Przywoływany już przykład mostu między Sycylią a kontynentalnymi Włochami w Mesynie stał się zatem przypadkiem granicznym, który wyznaczył nowy standard debaty: infrastruktura dual-use wlicza się do 1,5% pod warunkiem wykazania strategicznej wartości wojskowej, a nie tylko formalnego podwójnego zastosowania.

Podobne kontrowersje wzbudzały już wcześniejsze przypadki z obszaru celu 2%: koszty opieki nad dziećmi dla personelu wojskowego, wydatki krajowych brygad pozarniczych oraz emerytury pracowników cywilnych resortów obrony były przez niektórych sojuszników zaliczane do wydatków obronnych NATO, mimo że ich związek z „potrzebami sił zbrojnych" był wysoce wątpliwy. Według Bertelsmann Stiftung niektórych z tych pozycji „bardziej stosownie byłoby przypisać do przyszłej kategorii 1,5%, co w praktyce oznacza, że problem nie zniknie, a jedynie przesunie się między kategoriami bez żadnego sumarycznego wzmocnienia zdolności Sojuszu[107].

Na poziomie makroekonomicznym skala wyzwania jest zróżnicowana. Polska przeznaczyła w 2025 roku blisko 5% PKB na obronność w sensie militarnym, czyni ją liderem NATO pod względem obciążenia obronnego w relacji do PKB[108]. Dla krajów takich jak Włochy, Portugalia czy Hiszpania, które muszą zwiększać wydatki odpowiednio o 211%, 226% i 249%, sama arytmetyka budżetowa sprawia, że ochrona cywilna czy innowacje obronne są jedynymi obszarami, gdzie można szybko pokazać postęp bez dramatycznych efektów na wydatki socjalne. Tworzy to asymetryczną logikę, w której kraje najmocniej zagrożone są już bliskie spełnienia obu celów, zaś kraje najdalej od progu mają największe bodźce do szerokiej interpretacji katalogu 1,5%.

SIPRI w raporcie z kwietnia 2026 roku przestrzega, że niezbieżne lub niespójnie zdefiniowane dane o wydatkach mogą „zniekształcić oceny bilansu sił i potencjalnie kształtować percepcję zagrożeń oraz rozwój zdolności w oparciu o poziomy wydatków, które niedokładnie odzwierciedlają zdolności operacyjne”[109]. Jest to ostrzeżenie o długofalowych konsekwencjach instytucjonalnych: jeżeli 1,5% stanie się przede wszystkim kategorią budżetową, a nie zdolnościami, NATO będzie planować kolektywną obronność na podstawie danych, które mierzą aktywność finansową rządów, nie zaś rzeczywisty stan odporności ich społeczeństw.

Zasadą wydatkowania środków kwalifikowanych do komponentu 1,5% powinno być powiązanie każdego większego programu z miernikiem efektu odpornościowego. Miernik ten powinien wskazywać, czy wydatek zwiększa dostępność zasobu, skraca czas reakcji, poprawia ciągłość działania, wzmacnia ochronę ludności, podnosi odporność infrastruktury lub umożliwia weryfikację gotowości.

3.5 Ryzyka wdrożeniowe i rekomendacje

Brak operacyjnej taksonomii i mechanizmu weryfikacji nie jest jedynie problemem metodologicznym. Bertelsmann Stiftung Europe identyfikuje trzy ryzyka strategiczne wynikające wprost z obecnej architektury celu 1,5%, które, jeśli zostaną niezaadresowane przed przeglądem w 2029 roku, mogą trwale podważyć wiarygodność całego zobowiązania haskiego[110].

Pierwsze ryzyko to kreatywna księgowość. Bez jasnych definicji sojusznicy są silnie zmotywowani do zaliczania do kategorii 1,5% wydatków, które są już zaplanowane w krajowych budżetach pod innymi nagłówkami. Bertelsmann wprost ocenia, że „ten problem już teraz podważa wiarygodność obecnego celu 2%”. Przy kategorii 1,5% przestrzen interpretacyjna jest strukturalnie szersza, bo obejmuje nie tylko ministerstwo obrony, lecz cały aparat cywilny państwa.

Drugie ryzyko to oportunistyczna priorytetyzacja. Presja na szybkie osiągnięcie wymiernego poziomu wydatków może sprawić, że państwa będą skupiać inwestycje nie tam, gdzie są faktyczne luki odporności, lecz tam, gdzie dostępne są gotowe zdolności przesyłowe i procedury administracyjne[111]. Niemcy dostarczają tu empirycznej ilustracji: Sondervermögen, specjalny fundusz obronny w wysokości 100 mld EUR, uruchomiony po inwazji Rosji na Ukrainę w 2022 roku, zakończył się na koniec 2026 roku bez jasnej strategii następczej[112], a SIPRI wskazywało już w 2022 roku, że „zamówienia publiczne są notoryczne z powodu przewlekłości, przez co wydanie [funduszu] w ciągu trzech lat może mieć ograniczoną wartość dla adresowania trwałych luk zdolnościowych Bundeswehry”[113]. Nowy, jeszcze większy fundusz, SVIK (500 mld EUR na infrastrukturę) tworzy analogiczne ryzyko w kategorii 1,5%: wydatki będą kształtować się według tego, co można zamówić i zrealizować w dostępnych ramach czasowych, a nie według tego, czego Sojusz rzeczywiście potrzebuje.

Trzecie ryzyko to fragmentacja współpracy transgranicznej. Odporność cywilna jest z natury transgraniczna: sieci energetyczne, infrastruktura transportowa, łańcuchy dostaw farmaceutycznych i łańcuchy zaopatrzenia wojskowego przekraczają granice państwowe. Jeżeli każde państwo będzie definiować i realizować 1,5% w narodowych silosach, szanse na rzeczywiste efekty synergii (np. wspólne zaopatrzenie, interoperacyjność systemów, zintegrowane planowanie ewakuacji) zostaną zaprzepaszczone[114]. Bertelsmann przestrzega: „niejasne i nieskoordynowane priorytety inwestycyjne utrudniają rozwój współpracy transgranicznej niezbędnej dla podniesienia ogólnej gotowości obronnej Europy".

Łączny efekt tych trzech ryzyk może być odwrotny do zamierzonego. Jeżeli wzrost wydatków w kategorii niemilitarnej nie przekłada się na mierzalne polepszenie zdolności obronnych i odstraszających Europy, cała inicjatywa może, w średnim terminie, przynieść skutki odwrotne do zamierzonych, podważając zaufanie, podsycając rozczarowanie polityczne i obciążając relacje transatlantyckie"[115]. Istotnym ryzykiem wdrożeniowym jest wykazywanie zasobów odpornościowych bez potwierdzenia ich realnej gotowości. Dotyczy to w szczególności obiektów ochrony ludności, miejsc czasowego pobytu, infrastruktury krytycznej, systemów łączności, rezerw oraz usług publicznych, które mogą figurować w ewidencjach, lecz w momencie kryzysu okazać się niedostępne, niesprawne lub niemożliwe do uruchomienia w wymaganym czasie.

Rym Momtaz z Carnegie Endowment for International Peace trafnie podsumowuje ten paradoks: „Polska, państwa bałtyckie i nordyckie już osiągają cel lub mają plan osiągnięcia go w ciągu kilku lat – i to jest dowód, że jest to możliwe. [...] Głównym problemem nie jest to, że cel 5% jest zbyt ambitny lub nieosiągalny. Ryzyko polega na tym, że do 2035 roku może być za późno." [116]

Heritage Foundation idzie jeszcze dalej, sugerując, że analiza obronna powinna skupiać się na 3,5% na rdzeń obronny, a nie na łącznych 5% obejmujących powiązane wydatki infrastrukturalne, co odzwierciedla amerykański sceptycyzm wobec samej kategorii 1,5% jako pola analitycznego, jeśli ma ona zostać pozbawiona standardów kwalifikowalności[117]. Stanowisko to wskazuje na głębszy problem: jeśli nawet kluczowy sojusznik transatlantycki traktuje 1,5% jako marginalny komponent zbiorczego wskaźnika, a nie jako autonomiczny cel zdolnościowy, wola polityczna wypracowania taksonomii i mechanizmu weryfikacji będzie trudna do zmobilizowania.

Na te ryzyka analitycy wskazują zgodnie kilka kierunków rekomendacyjnych, których wdrożenie powinno poprzedzać przegląd w 2029 r. Pierwsza i centralnie ulokowana rekomendacja, sformułowana przez Bertelsmann Stiftung, to ustanowienie przez NATO odrębnego procesu planistycznego dla odpornosci, NATO Resilience Planning Process, jako samodzielnej ścieżki planowania, równoległy do, ale odrębny od istniejącego NATO Defence Planning Process[118]. Taki proces zapewniałby sojusznikom wspólną podstawę do oceny i rozwijania zdolności gotowości cywilnej, wyznaczając mierzalne punkty odniesienia, monitorując postępy, identyfikując luki zdolnościowe i ułatwiając skoordynowane działanie. Bertelsmann podkreśla, że NATO Resilience Planning Process „stanowiłby wiarygodne ramy dla wdrażania celu wydatkow 1,5% na gotowość cywilną".

Atlantic Council w swoich sześciu wytycznych dla operacjonalizacji 1,5%, opublikowanych w lutym 2026 roku, kilka miesięcy przed szczytem w Ankarze, proponuje powierzenie Allied Command Transformation opracowania szczegółowych wskazówek kwalifikowalności, implementowanych następnie w Kwaterze Głównej NATO przy wsparciu Asystenta Sekretarza Generalnego i wkładzie stałych przedstawicieli narodowych[119]. Atlantic Council wskazuje również na potrzebę włączenia do katalogu wydatków sektora prywatnego wzmacniającego obronność oraz ochrony łańcuchów dostaw zgodnie z NATO Defense-Critical Supply Chain Security Roadmap i Updated Defence Production Action Plan[120].

Uzupełniająca rekomendacja Bertelsmann Stiftung dotyczy poziomu unijnego: rozszerzenia mechanizmu Union Civil Protection Mechanism (UCPM) jako instrumentu koordynacji EU-NATO, który obejmowałby również Turcję jako członka NATO spoza UE oraz Ukrainę jako łącze między organizacjami[121]. Jest to rekomendacja o ważnym wymiarze instytucjonalnym: gotowość cywilna nie jest możliwa do zbudowania wyłącznie przez struktury wojskowe, wymaga współpracy agencji cywilnych, samorządów, organizacji pozarządowych i sektora prywatnego, a UCPM jest jedynym istniejącym międzynarodowym mechanizmem koordynacji tych podmiotów.

Na poziomie unijnym Instytut Europejski Universita Bocconi rekomenduje instrument miękki: porozumienia intencyjne pomiędzy Komisją Europejską a państwami członkowskimi w ramach programu SAFE, które formalnie obowiązywałyby państwa do tego, że pożyczki SAFE „będą uzupełniać, a nie zastępować krajowe budżety obronne”[122]. Bez takiego mechanizmu państwa zadłużone lub objęte w Unii procedurą nadmiernego deficytu mogą użyć SAFE jako narzędzia do zamrożenia krajowych budżetów obronnych, zaliczając równocześnie finansowane z niego zakupy do celu NATO, osiągając wskaźnik PKB na papierze bez faktycznego wzrostu wydatków.

Wspólnym mianownikiem wszystkich tych rekomendacji jest jeden postulat: cel 1,5% musi być powiązany z konkretną listą zdolności, nie tylko z listą kategorii. Bez zdolnościowej kotwicy zarówno cała debata o katalogach wydatków, jak i krytyka kreatywnej księgowości pozostają dyskusjami o formie, nie o treści. Carnegie Endowment, Bertelsmann Stiftung i Atlantic Council zgodnie stwierdzają, że okno decyzyjne, zanim sojusznicy „utrwalą” swoje interpretacje w wieloletnich planach budżetowych, jest krótkie, a przegląd 2029 roku powinien być traktowany nie jako raport z wykonania, lecz jako pierwszy punkt kontrolny zdolności kolektywnych zbudowanych za środki przypisane do 1,5%.

3.6 Zasady wydatkowania 1,5% PKB w Polsce

Po ustaleniach szczytu NATO w Hadze, kluczowym wyzwaniem stała się tzw. „funkcjonalna niejasność” celów cywilnych. Aby uniknąć ryzyka rozmycia tych środków i zarzutów o „kreatywną księgowość” na forum Sojuszu, polska metodyka wydatkowania 1,5% PKB musi opierać się na rygorystycznych kryteriach. Poniższe zasady, wywodzące się z rekomendacji wiodących ośrodków analitycznych oraz założeń strategii pozamilitarnych państwa, stanowią fundament narodowego mechanizmu sprawozdawczego:

Dodatkowość (additionality)

Środki z puli 1,5% PKB nie mogą pełnić funkcji mechanizmu łatania luk w samorządowych czy krajowych budżetach cywilnych. Raporty eksperckie jednoznacznie wskazują, że bez zasady dodatkowości państwa będą miały pokusę sztucznego zaliczania standardowych wydatków infrastrukturalnych czy administracyjnych w poczet wymogów NATO. Wydatek kwalifikowany musi tworzyć nową wartość bezpośrednio zwiększającą bezpieczeństwo państwa.

Trwały efekt odpornościowy

Gotowość cywilna to zdolność państwa do przetrwania długotrwałego szoku (konfliktu zbrojnego, blackoutu, wojny hybrydowej). Dlatego środki te nie mogą być przeznaczane na bieżącą konsumpcję czy krótkotrwałe programy osłonowe. Muszą być traktowane jako strategiczne inwestycje wieloletnie (np. budowa redundantnych sieci energetycznych, magazynów rezerw strategicznych), które trwale podnoszą próg odstraszania przeciwnika[123].

Pierwszeństwo ochrony życia cywilów

Załamanie struktur społecznych uniemożliwia siłom zbrojnym prowadzenie skutecznych działań operacyjnych. Zgodnie z wytycznymi NATO, utrzymanie ciągłości funkcjonowania administracji i społeczeństwa to rdzeń *civil preparedness*. Inwestycje muszą więc w pierwszej kolejności gwarantować fizyczne bezpieczeństwo ludności poprzez rozbudowę systemów schronów, bezpiecznej łączności oraz szlaków ewakuacyjnych.

Podwójne zastosowanie (Dual-use)

Aby utrzymać długofalowe poparcie społeczne dla tak wysokich nakładów finansowych, inwestycje z puli 1,5% nie mogą „stać puste" w czasie pokoju. Model *dual-use* gwarantuje optymalizację kosztów, infrastruktura (np. wzmocnione szpitale, drogi o podwyższonej nośności, huby logistyczne) służy na co dzień gospodarce, a w czasie kryzysu płynnie przejmuje funkcje wsparcia logistyki wojskowej i obrony cywilnej[124].

Transparentność i mierzalność

Brak sztywnego, natowskiego katalogu wydatków dla puli 1,5% PKB wymusza na państwach członkowskich samodzielne udowodnienie wkładu w bezpieczeństwo Sojuszu. Przyjęcie twardych wskaźników i transparentnego audytu jest niezbędne, aby Polska mogła na arenie międzynarodowej bezspornie wykazać, że jej wydatki na odporność realnie budują zdolności przetrwania wschodniej flanki, a nie są jedynie deklaracją polityczną. Wspólnym elementem przywołanych definicji jest traktowanie odporności jako zdolności praktycznej, a nie wyłącznie deklaratywnej. Obejmuje ona przygotowanie, utrzymanie, użycie i odtworzenie zasobów, ale również możliwość sprawdzenia, czy zasoby te są dostępne, działają zgodnie z przeznaczeniem i mogą zostać uruchomione w warunkach rzeczywistego zakłócenia.

CZĘŚĆ II

Od alokacji do sektorów: priorytety wydatkowe i przemysł

Część I uzasadniła, dlaczego komponent 1,5% PKB jest konieczny, wskazując skalę i hybrydowy charakter zagrożeń oraz lukę definicyjną w sposobie, w jaki NATO i państwa członkowskie traktują odporność cywilną. Część II odpowiada na pytania następne i bardziej praktyczne: na co te środki przeznaczyć, ile skierować na poszczególne obszary oraz z jakich źródeł sfinansować nakłady, by uniknąć obciążenia wyłącznie budżetu państwa. Punktem wyjścia jest matryca alokacyjna, porządkująca wydatki według siedmiu priorytetów strategicznych, a następnie mapa instrumentów finansowania. Kolejne rozdziały rozwijają wybrane priorytety w pogłębione analizy sektorowe.

Zaproponowana w niniejszej części architektura podziału środków z puli 1,5% PKB nie stanowi zamkniętego dogmatu budżetowego, lecz opartą na dowodach ramę analityczną. Przedstawiony podział procentowy został skonstruowany na bazie danych diagnostycznych: wyników audytów Najwyższej Izby Kontroli, raportów incydentów CERT Polska, wymogów implementacyjnych unijnych dyrektyw CER i NIS2 oraz rygorów natowskich Baseline Requirements for National Resilience. Stanowi on model wyjściowy, świadomie otwarty na rekalibrację w miarę dojrzewania metodologii rozliczania wydatków pozamilitarnych w ramach Sojuszu Północnoatlantyckiego oraz ewolucji krajowego otoczenia prawnego.

Celem tego zestawienia nie jest narzucenie sztywnych wskaźników księgowych, lecz dostarczenie decydentom spójnego i uzasadnionego źródłowo narzędzia do zarządzania priorytetami inwestycyjnymi. Kolejne rozdziały sektorowe nie omawiają wszystkich potencjalnych kategorii wydatkowych w równym stopniu. Zastosowano tu świadomy triaż strategiczny. Ograniczenie analizy na wybranych kierunkach wynika z trzech obiektywnych kryteriów:

Skali luki wyjściowej: Skupiamy się na obszarach, w których wieloletnie zaniedbania infrastrukturalne i legislacyjne wygenerowały największe ryzyko dla ciągłości funkcjonowania państwa.

Współczynnika dźwigni inwestycyjnej: Wyselekcjonowano sektory, w których alokacja kapitału przynosi najwyższą stopę zwrotu w postaci skokowego wzrostu bezpieczeństwa oraz generuje pożądane efekty gospodarcze (np. rozwój technologii dual-use).

Deficytu opracowań doktrynalnych: Priorytetyzujemy te dziedziny polityki publicznej, które dotychczas były marginalizowane w dyskursie eksperckim na rzecz klasycznych zdolności militarnych.

Z tych względów niektóre domeny – w szczególności infrastruktura schronowa i budowle ochronne oraz cyberbezpieczeństwo i ochrona infrastruktury krytycznej – zostały omówione w dokumencie w sposób nieproporcjonalnie szerszy i bardziej dogłębny. Asymetria ta jest w pełni celowa. Wymóg ochrony fizycznej ludności stanowi warunek przetrwania substancji demograficznej, wymagający obecnie najbardziej kapitałochłonnych interwencji po dekadach zapaści systemowej. Z kolei cyberprzestrzeń oraz infrastruktura krytyczna to domeny, w których państwo jest de facto w stanie ciągłego konfliktu podprogowego, co wymusza natychmiastowe, systemowe nakłady na technologie wczesnego ostrzegania, utrzymanie kadr i budowę suwerenności cyfrowej.

Dokonany wybór – obejmujący ponadto technologie kosmiczne, odporność systemu ochrony zdrowia oraz budowę krajowego przemysłu odpornościowego – jest wyrazem priorytetyzacji. Dokument nie pretenduje do encyklopedycznego ujęcia każdego z siedmiu wymogów odporności NATO ani każdej pozycji matrycy wydatkowej. Jego zadaniem jest wskazanie punktów ciężkości: tych precyzyjnych obszarów, w których w najbliższej dekadzie należy skoncentrować kapitał i uwagę państwa, aby 1,5% PKB przełożyło się na realną zdolność do absorpcji szoków kryzysowych. Pozostałe obszary zostały jedynie zasygnalizowane, pozostawiając ich pełną operacjonalizację odrębnym, specjalistycznym opracowaniom resortowym.

4 Struktura wydatków – proponowana alokacja

W kontekście makroekonomicznym Rzeczypospolitej Polskiej, której nominalne PKB w 2025 roku osiągnęło według pierwszych szacunków Głównego Urzędu Statystycznego wartość 3 912,7 mld zł, a prognozy agencji ratingowych i instytucji międzynarodowych (takich jak Fitch czy Bank Światowy) na lata 2026–2027 przewidują stabilny wzrost realny na poziomie 3,1%–3,6% oraz przekroczenie przez gospodarkę bariery 4 bilionów złotych, pula 1,5% PKB stanowi bezprecedensowy w historii kraju instrument stymulacji fiskalnej. Mówimy o kwocie oscylującej w granicach 60 miliardów złotych rocznie. Jest to potężny zastrzyk kapitału, który o ile zostanie zoptymalizowany pod kątem wskaźnika zwrotu z inwestycji w bezpieczeństwo (ROSI – Return on Security Investment), może nie tylko zabezpieczyć populację przed skutkami konfliktów kinetycznych i hybrydowych, ale również trwale zmodernizować polską gospodarkę.

Aby uniknąć ryzyka fragmentacji środków, powielania wyżej opisanej tzw. „kreatywnej księgowości" oraz oportunistycznego priorytetyzowania projektów pozbawionych wartości strategicznej, konieczne jest wdrożenie rygorystycznej matrycy alokacyjnej. Poniższa tabela prezentuje zoptymalizowaną strukturę wydatków w ramach komponentu 1,5% PKB, opartą na analizie luk zidentyfikowanych w audytach Najwyższej Izby Kontroli, raportach CERT Polska oraz wymogach dyrektyw europejskich i standardów NATO. W ramach zaproponowanej struktury wydatków można wyodrębnić również komponenty przekrojowe, które nie stanowią osobnej kategorii procentowej, lecz zwiększają skuteczność kilku wymienionych w tabeli priorytetów jednocześnie.

Tabela 2. Struktura wydatków – proponowana alokacja

Priorytet strategiczny	Udział w puli 1,5% PKB	Szacunkowa roczna wartość (przy PKB ok. 4 bln zł)
A. Schrony ochrony ludności	20%	~12,0 mld zł
B. Ochrona infrastruktury krytycznej	20%	~12,0 mld zł
C. Cyberbezpieczeństwo	15%	~9,0 mld zł
D. Gotowość cywilna i reagowanie kryzysowe	15%	~9,0 mld zł
E. Innowacje i technologie bezpieczeństwa	15%	~9,0 mld zł
F. Przemysł odpornościowy i łańcuchy dostaw	10%	~6,0 mld zł
G. Zarządzanie, audyt, rezerwy	5%	~3,0 mld zł

Poniższe sekcje stanowią wyczerpujące uzasadnienie dla zaproponowanego podziału, integrując najnowsze dane rynkowe, wskaźniki makroekonomiczne oraz uwarunkowania legislacyjne wynikające z nowej Ustawy o ochronie ludności i obronie cywilnej z 5 grudnia 2024 r.

Schrony ochrony ludności (20%)

Przeznaczenie jednej piątej całego budżetu odpornościowego, równowartości około 12 mld. złotych rocznie, na obiekty zbiorowej ochrony

stanowi fundamentalny krok w stronę odbudowy najbardziej zaniedbanego sektora bezpieczeństwa państwa. Decyzja ta jest podyktowana alarmującym stanem wyjściowym infrastruktury schronowej, zdiagnozowanym w raportach instytucji państwowych, a także olbrzymią kapitałochłonnością procesów inżynieryjnych i budowlanych.

Zniwelowanie luki i osiągnięcie wskaźników pokrycia porównywalnych z krajami skandynawskimi (gdzie miejsce w schronach ma nawet ok. 87% obywateli) wymaga wdrożenia w Polsce sieci składającej się dziesiątek tysięcy obiektów o odpowiedniej pojemności. To potężne wyzwanie ekonomiczne adresuje przyjęta 5 grudnia 2024 roku Ustawa o ochronie ludności i obronie cywilnej, która od 1 stycznia 2026 r. nakłada bezwzględny obowiązek projektowania miejsc doraźnego schronienia (MDS) w każdej nowo powstającej inwestycji wielorodzinnej i obiektach użyteczności publicznej. Ustawa precyzuje rygorystyczne wymagania metrażowe (1,5 m^2 na osobę, a 2 m^2 dla osoby na wózku inwalidzkim), normatywy wentylacyjne oraz wyposażenie sanitarne.

Alokacja 20% z 1,5% PKB pozwoli na powszechne zastosowanie modelu finansowania „dual-use" (podwójnego zastosowania). Środki te nie będą marnowane na budowę opuszczonych bunkrów, lecz zasilą fundusze samorządowe i państwowe z przeznaczeniem na pokrycie delta costs: kosztów wzmocnienia stropów, instalacji hermetycznych drzwi i specjalistycznej wentylacji w przestrzeniach, które w czasie pokoju będą funkcjonować jako garaże podziemne, magazyny komunalne, stacje metra i obiekty sportowe.

Ochrona infrastruktury krytycznej (20%)

Równoległy filar finansowy, stanowiący również 20% budżetu inwestycyjnego (kolejne ok. 12 mld zł), skoncentrowany jest na utrzymaniu ciągłości działania państwa poprzez ochronę infrastruktury krytycznej. Przydzielenie tak znaczących środków wynika bezpośrednio z potężnych obowiązków nałożonych na operatorów kluczowych systemów gospodarczych przez dyrektywę europejską CER (Dyrektywa 2022/2557 w sprawie odporności podmiotów krytycznych) oraz zaostrzający się reżim środowiska bezpieczeństwa międzynarodowego.

Proces legislacyjny w Polsce obarczony był opóźnieniami – nie dotrzymano unijnego terminu implementacji dyrektywy wyznaczonego na 17 października 2024 r., co wprowadziło system w fazę przejściową, wymagającą obecnie przyspieszonych i kapitałochłonnych działań dostosowawczych w ramach nowelizacji ustawy o zarządzaniu kryzysowym. Nowe ramy prawne znoszą dotychczasowe, wąskie rozumienie ochrony IK na rzecz holistycznego zarządzania ryzykiem. Objętych nowymi, rygorystycznymi wymogami zostało 15 strategicznych sektorów państwa, w tym tak szerokie domeny jak: produkcja, dystrybucja i uzdatnianie wody, zarządzanie usługami ICT, transport, wytwarzanie i dystrybucja chemikaliów, zaopatrzenie w żywność oraz, po raz pierwszy w tak ścisłym rygorze, finanse publiczne.

Holistyczne zarządzanie ryzykiem wymaga również bieżącej wiedzy o stanie infrastruktury technicznej, która warunkuje możliwość ochrony ludności i utrzymania usług publicznych. Do wydatków kwalifikowanych w tym priorytecie powinny należeć systemy monitorowania dostępności energii, wody, ogrzewania, wentylacji, łączności, parametrów środowiskowych oraz zdarzeń mogących wskazywać na awarię lub sabotaż infrastruktury. Dotyczy to zarówno operatorów infrastruktury krytycznej, jak i wybranych obiektów publicznych pełniących funkcje ochronne lub ewakuacyjne.

Podmioty, które uzyskają status Operatora Infrastruktury Krytycznej oraz Podmiotu Krytycznego, będą zmuszone do natychmiastowego wdrożenia kosztownych zintegrowanych systemów zarządzania bezpieczeństwem. Obejmują one m.in. drastyczne zaostrzenie reżimów w obszarze bezpieczeństwa fizycznego (budowa fizycznych barier, systemów antydronowych), bezpieczeństwa osobowego i teleinformatycznego. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (wdrażająca dyrektywę NIS2) zaostrza reżim nadzoru: na podmioty kluczowe nakłada obowiązek cyklicznych audytów bezpieczeństwa (pierwszy w ciągu 24 miesięcy od uzyskania statusu, kolejne nie rzadziej niż co trzy lata), wprowadza obowiązkowy system zarządzania bezpieczeństwem informacji oraz mechanizm weryfikacji dostawców ICT, w tym identyfikację dostawców wysokiego ryzyka. Niedostosowanie się do reżimu sankcjonowane jest przez organy właściwe do spraw cyberbezpieczeństwa wysokimi karami administracyjnymi – sięgającymi 10 mln euro

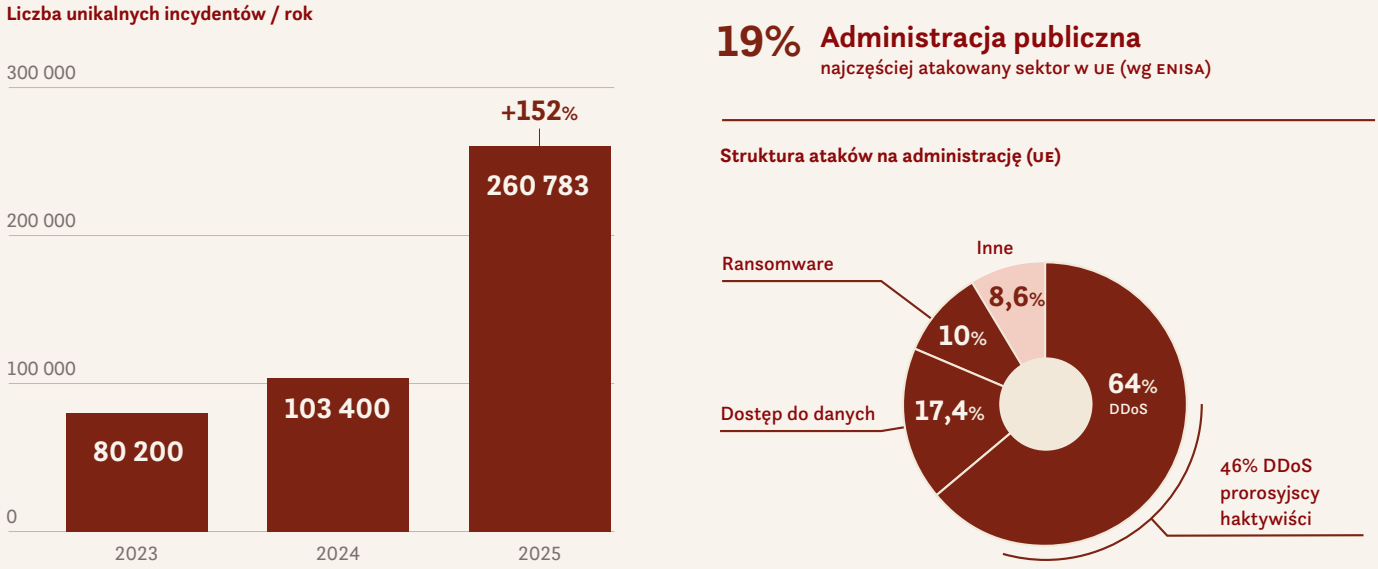
lub 2% rocznego przychodu dla podmiotów kluczowych, a w przypadku naruszeń powodujących bezpośrednie zagrożenie dla bezpieczeństwa państwa, porządku publicznego lub życia i zdrowia ludzi – nawet 100 mln zł. Z makroekonomicznego punktu widzenia środki alokowane w tym priorytecie posłużą do dofinansowania głębokiej przebudowy strukturalnej państwa, zgodnie z logiką, w której trwałość i bezpieczeństwo infrastruktury traktuje się łącznie. Inwestycje te obejmą rozbudowę redundancyjnych połączeń elektroenergetycznych, budowę rozproszonych źródeł energii odnawialnej wraz z magazynami energii zdolnymi do podtrzymania zasilania krytycznych węzłów w układzie wyspowym, a także wzmacnianie korytarzy transportowych. Tego rodzaju wydatki idealnie wpisują się w cel 1,5% PKB, z jednej strony utwardzają odporność sieci na sabotaż hybrydowy i ataki kinetyczne, z drugiej stymulują rozwój technologiczny i chronią konkurencyjność polskiego przemysłu w czasie pokoju.

Cyberbezpieczeństwo (15%)

Przeznaczenie 15% puli alokacyjnej (ok. 9 miliardów złotych rocznie) na cyberbezpieczeństwo jest wymuszone dynamicznie rosnącą skalą asymetrycznego konfliktu w domenach informatycznych. Sieci teleinformatyczne stały się głównym wektorem uderzeń na organy państwowe i infrastrukturę społeczną, co jednoznacznie udowadniają historycznie wysokie statystyki incydentów zanotowane na przestrzeni 2024 i 2025 roku. Raporty podsumowujące działalność CERT Polska za rok 2025 rzucają światło na lawinowy przyrost cyberzagrożeń. W ciągu całego 2025 roku analitycy zespołu otrzymali ponad 658 tysięcy zgłoszeń (wzrost o 10% r/r), które po merytorycznej weryfikacji przełożyły się na rejestrację 260 783 unikalnych incydentów cyberbezpieczeństwa. Stanowi to niewyobrażalny wręcz wzrost o 152% rok do roku w stosunku do wolumenu z roku 2024. Przytłaczająca większość, bo aż 97% zweryfikowanych zagrożeń z 2025 roku, stanowiły oszustwa komputerowe, ze szczególnym naciskiem na techniki phishingowe. Napastnicy zorganizowali wysoce sprofilowane kampanie uderzające w użytkowników popularnych portali e-commerce, a także instytucji publicznych i stacji informacyjnych. Równolegle z cyberprzestępczością pospolitą, diametralnie wzrosło zagrożenie ze strony grup typu APT (Advanced Persistent Threat), działających na zlecenie wrogich państw, wymierzonych w strategiczne organy polskiej administracji oraz podmioty naukowo-polityczne.

Na szczególną uwagę, uzasadniającą potężne zapotrzebowanie na kapitał, zasługuje ewolucja ataków z wykorzystaniem oprogramowania szyfrującego i wymuszającego okup (ransomware). W 2025 roku zarejestrowano 179 udanych lub wysoce krytycznych incydentów z użyciem takich narzędzi (wzrost z 147 w 2024 r. i 161 w 2023 r.), co w praktyce oznacza atak paraliżujący ważną strukturę korporacyjną lub instytucjonalną niemal co drugi dzień. Cyberprzestępcy z grup takich jak Qilin, LockBit, Beast, Makop czy RansomHub powszechnie stosują taktykę „podwójnego wymuszenia" (double extortion), która

Rysunek 3. Liczba cyberincydentów w Polsce



nie tylko blokuje systemy operacyjne firm, ale również polega na kradzieży wrażliwych danych i groźbie ich publikacji na czarnym rynku, co grozi podmiotom gospodarczym utratą reputacji i drastycznymi karami z tytułu naruszeń RODO. Zagrożenie mnożą dodatkowo krytyczne luki w oprogramowaniu powszechnego użytku oraz wykładniczy wzrost ataków zautomatyzowanych z użyciem sztucznej inteligencji, gdzie użycie AI drastycznie obniżyło barierę wejścia dla zorganizowanych grup przestępczych.

Alokacja 15% z budżetu umożliwi sfinansowanie infrastruktury defensywnej współmiernej do opisanej wyżej skali ataków. Niezbędne jest m.in. implementowanie na masową skalę rozwiązań z zakresu dyrektywy NIS2 oraz poszerzenie wydolności operacyjnej zespołów reagowania CSIRT na poziomie sektorowym i krajowym. O potencjale scentralizowanych inwestycji świadczą efekty działań CERT Polska: uruchomienie bezpłatnego numeru 8080 oraz wdrożenie niemal 800 wzorców smishingowych pozwoliło na zablokowanie blisko 1,88 miliona złośliwych wiadomości SMS w 2025 roku (o 27% więcej niż rok wcześniej). Systematycznie rozbudowywana Lista Ostrzeżeń uchroniła obywateli przed 140 milionami wejść na zainfekowane strony, a w samym tylko 2025 roku wpisano na nią 250 tysięcy szkodliwych domen (ok. 670 nowych adresów dziennie). Utrzymanie tego poziomu prewencji, rozbudowa suwerennych chmur obliczeniowych, testy penetracyjne oraz ciągłe audyty infrastruktury teleinformatycznej wymagają stałego i pewnego źródła finansowania.

Gotowość cywilna i reagowanie kryzysowe (15%)

Kolejne 15% budżetu (ok. 9 mld zł) ukierunkowane zostało na organizacyjny, sprzętowy i medyczny filar reagowania na masowe zdarzenia kryzysowe. Pula ta zasila instrumenty przewidziane we wdrożonym przez rząd RP „Programie Ochrony Ludności i Obrony Cywilnej na lata 2025–2026", którego przyjęcie w maju 2025 r. było fundamentalnym krokiem w operacjonalizacji Ustawy z 5 grudnia 2024 roku. Ramy finansowe dla gotowości cywilnej uzyskały bezprecedensowe oparcie w prawie – ustawowo zagwarantowano, że na ten cel przeznaczane będzie corocznie nie mniej niż 0,3% PKB, co przy obecnym PKB generuje stały strumień finansowy rzędu blisko 12 miliardów złotych z budżetu państwa (w 2025 r. rozdysponowano 16,7 mld zł, na 2026 r. założono 17,2 mld zł). Alokacja z pakietu NATO wzmacnia ten mechanizm o dodatkowe, wysokospecjalistyczne wektory modernizacyjne. Środki w ramach tego priorytetu będą wspierać funkcjonowanie Korpusu Obrony Cywilnej, nowej struktury grupującej personel odpowiedzialny za ratownictwo w czasie pokoju i przekształcany w scentralizowane jednostki obrony na wypadek wojny. Do głównych wydatków zalicza się: masowe zakupy sprzętu ratowniczego, doposażenie logistyczne jednostek wchodzących w skład Krajowego Systemu Ratowniczo-Gaśniczego (Państwowej Straży Pożarnej oraz Ochotniczych Straży Pożarnych), budowę Systemu Bezpiecznej Łączności Państwowej (m.in. powiadamianie poprzez europejski system EWS GALILEO) oraz dofinansowanie samorządów realizujących lokalne plany ewakuacji. W ramach tego priorytetu kwalifikowane powinny być także narzędzia umożliwiające szybkie wskazanie, ocenę i monitorowanie obiektów wykorzystywanych w lokalnych planach ewakuacji. Obejmuje to obiekty ochrony ludności, miejsca doraźnego schronienia, punkty zbiórki, miejsca czasowego pobytu oraz obiekty zakwaterowania ewakuowanych. Gotowość cywilna wymaga, aby samorząd i centrum zarządzania kryzysowego posiadały aktualną informację, które obiekty mogą przyjąć ludzi, jaką mają pojemność, jakie posiadają ograniczenia i czy zapewniają warunki bezpiecznego przebywania.

Istotną pozycję zajmują także programy szkoleniowe i edukacyjne dla obywateli (np. masowe kursy organizowane wspólnie z NGO, obejmujące docelowo ponad 100 tysięcy przeszkolonych osób z zakresu pierwszej pomocy i reagowania na alarmy). Organizacje pozarządowe otrzymały mocą ustawy nowe narzędzia współpracy, pozwalające im włączać się w system reagowania kryzysowego i ubiegać się o rządowe dofinansowania. Szczególnym wymiarem tej alokacji jest uodpornienie systemu ochrony zdrowia za sprawą koncepcji szpitali „dual-use" i procedury WAR-SOR. Placówki medyczne w świetle współczesnych doktryn zbrojnych przestają być wyłącznie obiektami leczniczymi, stając się strategicznymi węzłami oporu, ratowania życia i ewakuacji. Tradycyjne budownictwo szpitalne okazało się całkowicie nieprzydatne w obliczu ataków z powietrza. Nowe obiekty, takie jak zmodernizowany Szpital im. J. Biziela w Bydgoszczy, wytyczają innowacyjne standardy: przestrzenie

podziemne w krótkim czasie mogą zostać odizolowane hermetycznymi grodziami, tworząc niezależne od warunków zewnętrznych oddziały zabiegowe, punkty triażu masowego oraz sale dla poszkodowanych. 15-procentowa alokacja pozwoli na przyspieszoną adaptację kolejnych węzłów medycznych w Polsce do działania w warunkach przerwanych dostaw zasilania i braku bezpiecznej przestrzeni operacyjnej na wyższych kondygnacjach.

Innowacje i technologie bezpieczeństwa (15%)

Budowa suwerenności technologicznej w dobie niestabilnych sojuszy gospodarczych wymaga gigantycznych inwestycji w rodzimy sektor B+R (Badania i Rozwój). Alokacja 15% z budżetu bezpieczeństwa (ok. 9 mld zł) stymuluje zaawansowany przemysł deep-tech i jest bezpośrednią odpowiedzią na wezwanie NATO do „uwolnienia innowacji" w przemyśle odpornościowym. Środki polskie w tym segmencie działają z potężnym efektem dźwigni, gdyż są komplementarne z ogromnymi funduszami uruchomionymi z budżetów unijnych.

W 2026 roku szczególną wagę przywiązuje się do wdrażanego Funduszu Bezpieczeństwa i Obronności (FBiO), opartego o środki z Krajowego Planu Odbudowy. Polska, jako jedyne państwo w Unii Europejskiej, wynegocjowała wyodrębnienie z KPO kwoty ok. 22,5 miliarda złotych (5,3 mld euro) ściśle na cele militarne, bezpieczeństwa i odporności. Fundusz ten, dzielony po równo na samorządy i sektor prywatny, będzie zorientowany na produkcję technologii podwójnego zastosowania („dual-use"). Technologia dual-use obejmuje systemy komunikacji cyfrowej, platformy analizy danych czy układy zasilania rozproszonego (np. agregaty, mikrosieci inteligentne), które z sukcesem komercjalizują się na rynkach cywilnych, a w stanie wyższej konieczności płynnie włączane są w obieg wojskowy i zarządczy. Do tej kategorii należy zaliczyć również technologie integrujące sensorykę, telemetrię, analizę danych, lokalne przetwarzanie informacji, sztuczną inteligencję oraz bezpieczną komunikację na potrzeby zarządzania kryzysowego. Równolegle, w 2025 i 2026 roku polskie firmy obronne i technologiczne uzyskały dostęp do programu STEP (Strategic Technologies for Europe Platform), finansowanego za pośrednictwem Funduszy Europejskich dla Nowoczesnej Gospodarki (FENG), operujących potężnym budżetem prawie 40 mld zł. Synergia środków z tytułu natowskiego 1,5% PKB z europejskimi programami badawczymi ułatwi polskim podmiotom wypracowanie innowacyjnych patentów, m.in. w obszarze nowych materiałów i polimerów, drastycznie obniżających koszty i czas wznoszenia masowych budowli ochronnych (istotnych dla segmentu A), czy oprogramowania opartego na algorytmach sztucznej inteligencji, wykrywającego anomalie w infrastrukturze krytycznej zanim te doprowadzą do awarii sprzętowych. Własne zaplecze badawcze gwarantuje, że kluczowe kody źródłowe infrastruktury ratowniczej i energetycznej pozostaną całkowicie pod polską kontrolą, uniezależniając kraj od dostawców z państw trzecich.

Przemysł odpornościowy i łańcuchy dostaw (10%)

Zabezpieczenie 10% środków alokacji (ok. 6 mld zł) dla logistyki i rezerw państwowych służy redukcji ryzyk operacyjnych związanych z globalizacją łańcuchów produkcyjnych. Koncepcja odporności NATO jednoznacznie wskazuje na wymóg ciągłości zaopatrzenia gospodarki (przepływu żywności, zasobów medycznych, stabilności energetycznej) nawet w przypadku drastycznego zerwania szlaków handlowych przez akty sabotażu bądź wybuch wojny.

Środki z puli 1,5% PKB pozwolą na głęboką restrukturyzację systemu strategicznych rezerw (w szczególności zapasów leków niezbędnych dla ratowania życia ludności cywilnej, antybiotyków oraz materiałów opatrunkowych) na model zdecentralizowany. Finansowane będą procesy relokacji fabryk kluczowych komponentów półprzewodnikowych i substancji czynnych leków na terytorium RP (ang. near-shoring) oraz integracja cyfrowa systemów śledzenia terminów przydatności na rynkach hurtowych, co wyeliminuje patologie zarządzania na poziomie organów centralnych.

Zarządzanie, audyt, rezerwy (5%)

Zwieńczeniem architektury wydatkowej jest alokacja rzędu 5% (ok. 3 mld zł), która stanowi mechanizm zabezpieczający efektywność

wydatkowania pozostałych 95% funduszy. Doświadczenia z ewaluacji kryteriów NATO wielokrotnie dowodziły, że mgliste wytyczne co do kwalifikowalności wydatków pobocznych w obronności generują ogromne ryzyko „kreatywnej księgowości" i oportunizmu priorytetów ze strony państw członkowskich. Mechanizm ten został opisany m.in. w kontekście włoskich prób zaliczenia projektu cywilnego mostu na Sycylię do wydatków obronnych na etapie deklaracji inwestycyjnych związanych z celem 1,5%. Aby uchronić polski program przez podobnym rozmyciem kapitału, niezbędne jest sfinansowanie niezależnego centrum weryfikacji.

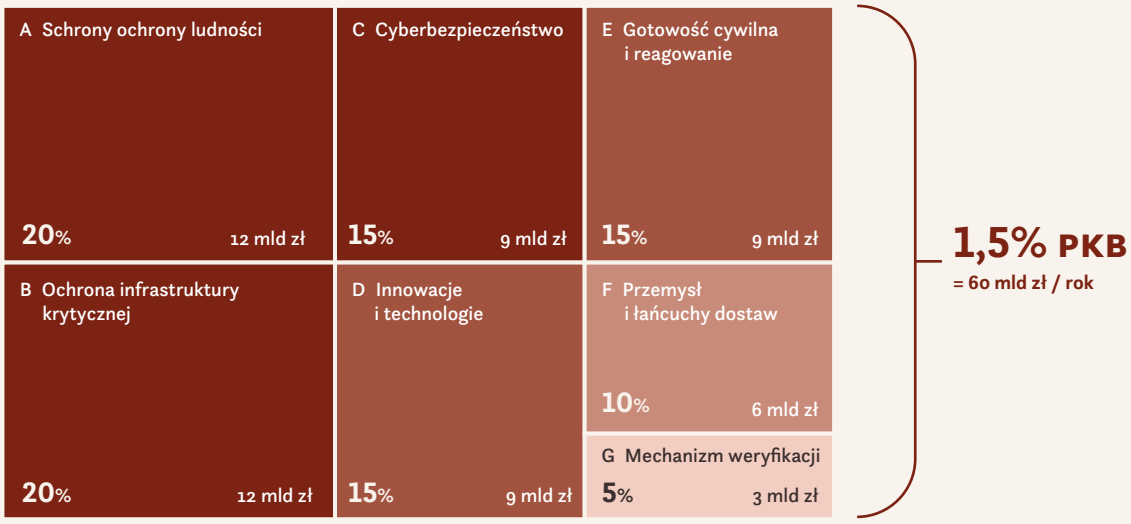
Niezależna weryfikacja powinna opierać się nie tylko na dokumentacji finansowej, lecz także na danych potwierdzających realną gotowość zasobów. Wydatki w tym priorytecie powinny więc obejmować mechanizmy raportowania, audytu, testów funkcjonalnych i utrzymywania aktualnych danych o dostępności oraz sprawności zasobów odpornościowych.

Wyodrębnienie 5% kwoty stanowi bufor na pokrycie gwałtownych zjawisk inflacyjnych w sektorze budowlanym, które mogą wystąpić wskutek uruchomienia setek nowych projektów infrastruktury ochronnej. Zaproponowana struktura wydatków harmonijnie splata militarne wymagania NATO z głęboką przebudową kluczowych obszarów administracji i gospodarki, udowadniając, że 1,5% PKB przeznaczone na odporność to najskuteczniejszy mechanizm unowocześnienia i ochrony zasobów Rzeczypospolitej Polskiej w erze zacierających się granic między wojną a pokojem.

Warunkiem skuteczności tej struktury jest powiązanie alokacji procentowej z mierzalnymi zdolnościami operacyjnymi. Każdy z priorytetów powinien wskazywać nie tylko rodzaj finansowanych inwestycji, lecz także sposób potwierdzenia, że dana inwestycja zwiększa odporność państwa: przez skrócenie czasu decyzji, zwiększenie dostępności zasobów, poprawę ciągłości działania, podniesienie bezpieczeństwa ludności, zwiększenie odporności infrastruktury albo umożliwienie audytu gotowości.

Rysunek 4. Struktura wydatków 1,5% PKB w Polsce

Podział puli odpornościowej (≈60 mld zł rocznie) na priorytety A–F i mechanizm weryfikacji



5 Dostępne źródła finansowania

Zobowiązanie haskie, nakładające na Polskę konieczność przeznaczenia do 1,5% PKB rocznie na niemilitarne wydatki z zakresu obronności i bezpieczeństwa, oznaczają strumień środków rzędu 50–60 mld zł rocznie, który musi być nie tylko wydatkowany, lecz również udokumentowany jako spełniający kryteria Sojuszu. Polska dysponuje już dziś portfelem instrumentów o łącznym potencjale przekraczającym 300 mld zł na lata 2025–2030, obejmującym środki krajowe, unijne i sojusznicze. Wyzwanie nie polega zatem na braku źródeł, lecz na ich koordynacji, przestrzeganiu zasady dodatkowości oraz zapobieżeniu klifowi finansowemu po wygaśnięciu zobowiązań z Krajowego Planu Odbudowy. Poniższy rozdział systematyzuje dostępne instrumenty w odniesieniu do siedmiu filarów odporności NATO (Baseline Requirements for National Resilience, BLR), zawiera tablice przeglądowe oraz formułuje rekomendacje dotyczące kolejności i zasad uruchamiania środków.

Przy ich dystrybucji należy przyjąć zasadę finansowania pełnego cyklu życia zdolności odpornościowej. Oznacza to, że koszt kwalifikowany nie powinien ograniczać się do budowy, zakupu lub modernizacji zasobu, lecz powinien obejmować również przygotowanie dokumentacji, cyfrową paszportyzację, integrację z systemami zarządzania kryzysowego, cyberbezpieczeństwo, szkolenia operatorów, testy funkcjonalne, serwis, aktualizację oraz utrzymanie gotowości w kolejnych latach.

Tabela 3. Mapa instrumentów finansowania w odniesieniu do siedmiu filarów odporności NATO (BLR)

Filar NATO (BLR)	Główne instrumenty krajowe	Kluczowe instrumenty unijne/sojusznicze
1. Ciągłość rządów	OLIOC, FBIO (telekomunikacja kryzysowa)	RESCEU, Horyzont Europa Klaster 3
2. Bezpieczeństwo energetyczne	KPO/REPOWEREU, FENIKS, RARS	EBI, CEF Energia, EDF (dual-use)
3. Przemieszczanie ludności	Tarcza Wschód, OLIOC, MSWiA/SG	FAMI, FBW (87 mln euro), RESCEU
4. Żywność i woda	OLIOC (ujęcia wody), RARS, FBIO	WPR/EFRROW, RESCEU stockpiles
5. Masowe ofiary	FBIO, KPO (zdrowie), RARS med.	EU4Health, RESCEU MedEvac, FENIKS
6. Łączność i cyber	Fundusz Cyberbezpieczeństwa, KPO, FBIO	EDF, DEP, Horyzont Europa Klaster 3
7. Transport	FENIKS, KPO/E, Tarcza Wschód, FBIO	CEF Transport, CEF Mob. Wojskowa, EBI

Źródło: opracowanie własne na podstawie danych programowych MFiPR, MSWiA, BGK i KE (maj 2026 r.).

5.1 Instrumenty finansowania

Fundamentem systemu finansowania odpornosci cywilnej jest obecnie **Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026** (Program OLIOC), przyjęty uchwałami Rady Ministrów z 27 maja 2025 r. na podstawie ustawy z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej[125]. Program dysponuje łączną alokacją 33,9 mld zł (16,7 mld zł w 2025 r. i 17,2 mld zł w 2026 r.), z czego ok. 80–90% trafia do samorządów terytorialnych za pośrednictwem urzędów wojewódzkich[126]. Ustawa ugruntowuje minimum 0,3% PKB rocznie jako ustawowy próg wydatków na zadania OLIOC, tworząc fiskalną kotwicę warunkującą zachowanie zasady dodatkowości po wygaśnięciu programu. Katalog kwalifikowanych wydatków obejmuje budowę i wyposażenie obiektów zbiorowej ochrony, awaryjne ujęcia wody i lokalne studnie, system łączności kryzysowej, zasoby logistyczne dla Korpusu Obrony Cywilnej oraz szkolenia i ćwiczenia ewakuacyjne. Program OLIOC odpowiada bezpośrednio na pięć z siedmiu filarów BLR i stanowi instrument natychmiastowo dostępny, bez potrzeby nowych regulacji.

Równie istotnym wehikułem jest **Fundusz Bezpieczeństwa i Obronności (FBiO)**, ustanowiony ustawą z 4 grudnia 2025 r. jako wyodrębniony komponent Krajowego Planu Odbudowy[127]. Ustawa weszła w życie w styczniu 2026 r., a pierwsze nabory wniosków planowane są na drugą połowę tego roku. Łączna pula środków wynosi 22,5 mld zł (5,3 mld euro), z podziałem na ok. 9,5 mld zł na infrastrukturę ochrony ludności (budowle ochronne, ujęcia wody, łączność kryzysowa), ok. 10 mld zł na infrastrukturę o podwójnym zastosowaniu (drogi, mosty, lądowiska), ok. 4 mld zł dla sektora obronno-przemysłowego oraz 2,46 mld zł na cyberbezpieczeństwo. Samorządy terytorialne korzystają z pożyczek nieoprocentowanych z możliwością częściowego umorzenia, spłacanych przez nawet 30 lat; przedsiębiorstwa i uczelnie mogą ubiegać się o wsparcie kapitałowe przez spółkę celową BGK[128].

Znaczna pula środków pochodzi ze **strumienia KPO poza FBiO**. Komponent G (REPOWEREU) dysponuje 12,14 mld zł dotacji i 99,09 mld zł pożyczek przeznaczonych na sieci dystrybucyjne, magazyny energii, morskie farmy wiatrowe i infrastrukturę wodną, wpisując się jako wiodący instrument dla Filaru 2. Komponent D (ochrona zdrowia) obejmuje 4,4 mld euro, a komponent E (mobilność) 28,4 mld zł. Termin kwalifikowalności wydatków z KPO upływa 31 sierpnia 2026 r., co stanowi pierwsze i najpoważniej wąskie gardło absorpcyjne całego systemu.[129]

Uzupełnieniem krajowych instrumentów programowych jest **Bank Gospodarstwa Krajowego (BGK)**, pełniący rolę agenta rozliczeniowego dla FBIO, emitujący obligacje Funduszu Wsparcia Sil Zbrojnych (zadłużenie ok. 113,1 mld zł na koniec 2025 r.) i udzielający gwarancji dla podmiotów sektora obronnego. W obszarze instrumentów innowacyjnych Polska posiada udokumentowaną ścieżkę emisji obligacji tematycznych: jako pierwsze państwo na świecie wyemitowała w 2016 r. zielone obligacje skarbowe. Emisja analogicznych obligacji odpornościowych, w formatach zgodnych z rozporządzeniem UE GB lub ICMA Green Bond Principles, pozostaje opcją dostępną bez konieczności uchwalania nowych przepisów.

Na poziomie samorządowym warto odnotować rosnącą dojrzałość modelu **partnerstwa publiczno-prywatnego (PPP)**. W 2025 r. podpisano 10 umów PPP o łącznej wartości 1,64 mld zł, w tym projekt Nowy Port 2030+ w Gdańsku (1,4 mld zł)[130]. Dla kategorii 1,5% NATO PPP jest szczególnie obiecujące w obszarze infrastruktury dual-use: schronów z funkcją komercyjną w czasie pokoju, obiektów logistycznych, portów i lądowisk.

Najistotniejszą nowością na mapie finansowania europejskiego jest program **SAFE (Security Action for Europe),** ustanowiony rozporządzeniem Rady UE 2025/1106 z 27 maja 2025 r. Polska otrzymała największą w Unii alokację: 43,7 mld euro (ok. 185–200 mld zł) w formie preferencyjnych pożyczek o terminie zapadalności do 2070 r. Chociaż SAFE jest klasyfikowany głównie

do filaru 3,5%, jego katalog obejmuje również mobilność wojskową, obronę cybernetyczną i infrastrukturę o znaczeniu obronnym, elementy bezpośrednio relewantne dla kategorii 1,5%. Pełne wykorzystanie tej alokacji zakładało pierwotnie przyjęcie ustawy, która ostatecznie została zawetowana przez Prezydenta RP. W odpowiedzi na tę sytuację rząd wdrożył alternatywną ścieżkę formalno-prawną, która neutralizuje skutki braku nowej legislacji ustawowej. W praktyce oznacza to przeniesienie ciężaru wdrożeniowego z poziomu ustawowego na instrumenty wykonawcze. Zamiast tworzyć nowe, dedykowane ramy prawne dla programu SAFE, Rada Ministrów opiera się na istniejących strukturach instytucjonalnych i obowiązującej ustawie o finansach publicznych. Środki te mogą być zoperacjonalizowane poprzez rozporządzenia oraz delegowanie zadań do wyspecjalizowanych podmiotów państwowych (np. wykorzystując Bank Gospodarstwa Krajowego lub Polski Fundusz Rozwoju w roli operatorów finansowych dla poszczególnych transz). Taki mechanizm pozwala na zawieranie umów o dofinansowanie, uruchamianie linii kredytowych i bezpośrednie kontraktowanie projektów cywilno-wojskowych bez konieczności uchwalania nowej ustawy, zapewniając zachowanie harmonogramów uzgodnionych z Komisją Europejską.

Europejski Fundusz Obronny (EDF) dysponuje budżetem 7,9 mld euro na lata 2021–2027. W 2025 r. otwarto nabory o łącznej wartości 1,065 mld euro. Polskie podmioty uczestniczą w niemal co drugim zatwierdzonym projekcie EDF[131], z silną pozycja w obszarach łączności satelitarnej, systemów bezzałogowych i elektroniki obronnej. EDF wpisuje się przede wszystkim w Filary 1 i 6, tworząc jednocześnie ścieżkę transferu innowacji cywilnych do sfery obronnej. Komplementarnie działa Program Cyfrowa Europa (DEP) oraz Klaster 3 programu Horyzont Europa poświęcony bezpieczeństwu cywilnemu (ok. 400 mln euro rocznie).

Program **rescEU** stanowi europejski mechanizm strategicznych rezerw reagowania kryzysowego, finansowany w całości z budżetu UE. Obejmuje rezerwy sprzętu medycznego, ratowniczego, środków gaśniczych oraz zdolności ewakuacji medycznej. W grudniu 2023 r. Komisja przyznała 690 mln euro na rozbudowę rezerw strategicznych CBRN w szesnastu państwach[132]. Ze względu na geograficzne położenie i dostępną infrastrukturę magazynową Polska jest wskazywana do pełnienia roli państwa goszczącego kolejny komponent rescEU w regionie.

Program **CEF Mobilność Wojskowa** sfinansuje modernizację infrastruktury transportowej o podwójnym zastosowaniu. W bieżącej perspektywie (1,74 mld euro na lata 2021–2027) Polska jest liderem w trzecim naborze z dwunastoma projektami na ponad 129 mln euro, obejmującymi m.in. wzmocnione mosty na autostradzie A2 oraz budowę drogi ekspresowej S12 (64,47 mln euro)[133]. Propozycja Komisji z lipca 2025 r. przewiduje dziesięciokrotne zwiększenie puli w perspektywie 2028–2034 do 17,6 mld euro. Pakiet łączony z planowanym systemem EMERS (European Military Mobility Enhanced Response System) stwarza potencjał finansowania infrastruktury podwójnego zastosowania, który Polska powinna aktywnie wykorzystać w negocjacjach nowej perspektywy budżetu UE.

5.2 Luki, zasada dodatkowości i wąskie gardła absorpcyjne

Pomimo imponującego portfela instrumentów analiza ujawnia trzy strukturalne luki. **Filar 3** (zarządzanie przemieszczaniem ludności) nie dysponuje dedykowanym wieloletnim programem krajowym poza Tarczą Wschód i unijnym Funduszem Bezpieczeństwa Wewnętrznego (87 mln euro dla Polski w perspektywie 2021–2027). Doświadczenie 2022 r., gdy Polska przyjęła ponad 1,5 mln uchodźców z Ukrainy bez żadnego instrumentu finansowania przygotowanego ex ante, ukazuje skalę ryzyka. **Filar 4** (bezpieczeństwo żywnościowe-wodne) nie posiada odpowiednika fińskiej Narodowej Agencji Dostaw Awaryjnych (NESA), finansowanej z opłaty w wysokości 1% wpływów z VAT i gwarantującej 6-miesięczne rezerwy żywności i paliwa. W Polsce Rządowa Agencja Rezerw Strategicznych opiera się na finansowaniu budżetowym bez trwałego źrodła zasilenia. **Filar 5** (masowe ofiary) posiada stosunkowo dobrze rozwinięte finansowanie szpitali ratunkowych z FENIKS i KPO, jednak zasoby medycznych rezerw strategicznych pozostają nieadekwatne do scenariuszy konfliktu wysokiej intensywności.

Do wskazanych luk należy dodać lukę gotowościową: ryzyko finansowania zasobów odpornościowych bez mechanizmu potwierdzania ich realnej dostępności, sprawności i możliwości użycia. Dotyczy to w szczególności obiektów ochrony ludności, miejsc czasowego pobytu, infrastruktury krytycznej, systemów łączności, zasobów energetycznych i rezerw. Zasób może zostać sfinansowany i ujęty w ewidencji, lecz bez aktualnych danych o jego stanie jego użyteczność w sytuacji kryzysowej pozostaje niepewna.

Atlantic Council i SIPRI w analizach z 2025 r. ostrzegają, że kategoria 1,5% stwarza ryzyko reklasyfikowania dotychczasowych wydatków sektorowych na drogi, szpitale czy sieci energetyczne zamiast faktycznego generowania nowych inwestycji odpornościowych[134]. Polska powinna przyjąć rok 2024 jako punkt referencyjny dla wydatków w sektorach budżetowych. Zapis w ustawie o finansach publicznych, ustalający minimum budżetowe dla OLIOC na poziomie 0,3% PKB jako niezależne od środków unijnych i pożyczek SAFE, stanowiłby kluczowe zabezpieczenie. Coroczne sprawozdanie Rady Ministrów do Sejmu z precyzyjną taksonomią wydatków i audytem NIK uzupełniałby tę architekturę.

Doświadczenia z wdrażaniem KPO i funduszy spójności wskazują na trzy nawracające bariery absorpcyjne. Po pierwsze, środki z Programu OLIOC dotarły na konta samorządów dopiero we wrześniu i październiku 2025 r., co wymuszało przesuwanie projektów i wzrost kosztów[135]. Po drugie, nie wszystkie z 2 500 gmin dysponują wystarczającym zapleczem kadrowym do przygotowania dokumentacji projektowej zgodnej z wymogami KPO i FBIO. Po trzecie, FBIO i OLIOC częściowo pokrywają się tematycznie, przy jednoczesnym braku mechanizmu zapobiegającego podwójnemu finansowaniu. Zasadne do rozważenia byłoby powołanie centrum kompetencji przy MFIPR lub BGK, pełniącego rolę jednego okienka dla samorządów poszukujących finansowania kategorii 1,5%.

Punktem porządkującym całą rozmowę może być zasada dodatkowości: publiczny pieniądz najlepiej służy tam, gdzie tworzy zdolność, której rynek sam by nie wytworzył, a nie tam, gdzie zastępuje nakłady powstające i tak. To wspólny test dla każdego mechanizmu opisanego dalej. Skalę możliwych korzyści dobrze ilustrują rynki dojrzałe: brytyjskie Ministerstwo Obrony odkupiło w 2025 r. ~36 tysięcy mieszkań służbowych za około 6 mld GBP, korzystając przez siedem lat z doradztwa rynkowego, od wycen po corporate finance, a w Stanach Zjednoczonych prywatni doradcy zarządzają ok. 600 mln stóp kwadratowych (ok 60 mln. m2) nieruchomości rządowych i wojskowych. Z analizy tych doświadczeń wyłaniają się cztery obszary, w których warto rozwinąć dzisiejsze ramy.

Pod pojęciem dual-use mieszczą się dwie różne funkcje, a ich świadome rozróżnienie pozwala precyzyjniej dobrać narzędzia. Pierwsza to

ochrona ludności: schronienie ludzi w sytuacji zagrożenia. Jej naturalnym miejscem są budynki, w których ludzie mieszkają i przebywają na co dzień: mieszkalnictwo, biura, obiekty użyteczności publicznej. Druga to konwersja obronno-gospodarcza: zdolność obiektu do przejęcia funkcji magazynowych, produkcyjnych czy logistycznych. Jej naturalnym miejscem są logistyka przy węzłach transportowych, przemysł i centra danych, które z natury dysponują nadmiarowością konstrukcyjną: wysokimi stropami, nośnymi posadzkami, otwartymi halami.

Rozdzielenie tych funkcji otwiera podwójną szansę. W mieszkalnictwie oraz w przypadku biur i obiektów użyteczności publicznej, by koszt już dziś ponoszony przełożył się na realnie wyższą ochronę, tam gdzie ludzie będą się schronić. W logistyce i przemyśle, by wykorzystać tanią i obronnie użyteczną zdolność konwersyjną, która dziś pozostaje poza zakresem zachęt. Chodzi zatem nie o przenoszenie ciężaru między sektorami, lecz o dopasowanie właściwego narzędzia do każdej z funkcji.

Obecne ramy w naturalny sposób kierują inwestora ku najniższemu dopuszczalnemu (i oczekiwanemu przez rynek) standardowi, nie z braku dobrej woli, lecz z ekonomii projektu, w której wyższa klasa ochrony oznacza wyższy koszt. Korzyść z wyjścia „ponad minimum" jest przy tym trwała: realna klasa ochronna to zdolność wpisana w konstrukcję na cały cykl życia budynku, na dekady, a nie na jeden cykl koniunkturalny.

Tu otwiera się jedna z największych szans. Mechanizm obowiązku już funkcjonuje: ustawa o ochronie ludności i obronie cywilnej określa minimalny standard i wyznacza kierunek projektowania i budowania obiektów w taki sposób, by uwzględniały walor ochrony ludności. Art. 106 ustawy o ochronie ludności i obronie cywilnej przewiduje bezpośrednie możliwości wsparcia, w tym dotacje, które przy mogą sięgnąć pełnego kosztu budowy czy adaptacji obiektu na potrzeby ochrony ludności. Naturalnym kolejnym krokiem jest mechanizm, w którym kapitał prywatny współfinansuje odporność, a publiczna złotówka działa jak dźwignia. Skalę takiego efektu dobrze pokazuje amerykański program MHPI, który przełożył 4 mld USD środków publicznych na 32 mld USD kapitału prywatnego i objął ok. 200 tys. mieszkań na ponad 150 bazach, w kontraktach sięgających 50 lat.

Warto przy tym rozróżnić, kto obiekt buduje, finansuje i utrzymuje, bo od tego zależy zarówno koszt publiczny, jak i realna gotowość. Na jednym biegunie państwo wznosi i utrzymuje aktywa stricte obronne samodzielnie: rozwiązanie czytelne, lecz kosztowne i obciążone ryzykiem, że obiekt rzadko używany na co dzień w decydującym momencie okaże się niesprawdzony. Na drugim biegunie obiekt powstaje czysto komercyjnie, poza zasięgiem polityki publicznej; w kryzysie jego operator i tak może zostać zobowiązany do udostępnienia przestrzeni, bez rekompensaty i bez pewności, że spełni ona funkcję ochronną. Między nimi mieści się rozwiązanie pośrednie, w wielu sytuacjach najkorzystniejsze: obiekt jest budowany i utrzymywany komercyjnie, więc na co dzień pracuje, jest serwisowany i sprawdzony, a dzięki temu w sytuacji zagrożenia rzeczywiście zadziała, inwestor zaś dokłada warstwę ochronno-obronną, która z perspektywy rynkowej nie ma dla niego wartości. Państwo pokrywa wyłącznie ten dodatkowy nakład: dotacją, ulgą, preferencją albo dostępem do gruntu trudno dostępnego w zwykłym trybie. Taki układ jest wzorcowym zastosowaniem zasady dodatkowości: publiczny pieniądz finansuje jedynie zdolność, której rynek sam by nie wytworzył, a nie budowę powstającą i tak. Jest też uczciwy wobec obu stron: zamiast przymusu bez wynagrodzenia pojawia się ułożona zawczasu wymiana – trwała zdolność ochronna w zamian za policzalną zachętę, w której inwestor nie dokłada do bezpieczeństwa publicznego, a państwo nie musi budować aktywów militarnych od zera.

Równolegle otwiera się szansa związana z majątkiem publicznym. Państwo i samorządy dysponują znaczącym, często doskonale zlokalizowanym zasobem – terenami powojskowymi, kolejowymi, logistycznymi, gruntami w centrach miast. Część tego zasobu, zarządzanego m.in. przez Agencję Mienia Wojskowego, mogłaby zarazem odpowiadać na odczuwalny deficyt zakwaterowania kadry. Pełniejsze jego wykorzystanie to jedna z najbardziej obiecujących ścieżek: przejście od decyzji projektowych ku zarządzaniu portfelowemu pozwala, by aktywa tworzyły wartość, a nie jedynie koszt utrzymania. Wzorce są sprawdzone: brytyjskie uwalnianie gruntów publicznych pod mieszkania i logistykę oraz szwedzkie wehikuły zarządzające majątkiem państwa dowodzą, że to droga przetarta, a nie eksperyment.

Tabela 4. Funkcje dual-use i kierunki rozwoju

Funkcja	Naturalne aktywa	Punkt wyjścia	Kierunek rozwoju
Ochrona ludności	Mieszkalnictwo, biura, obiekty publiczne	Obowiązek minimalnego schronienia (art. 94 ustawy o ochronie ludności i obronie cywilnej)	Zachęta do wyższej klasy ochrony tam, gdzie ludzie się schronią
Konwersja obronno-gospodarcza	Logistyka, przemysł, centra danych	Funkcja dotąd poza zakresem zachęt	Premiowanie taniej, użytecznej zdolności konwersyjnej
Finansowanie	Kapitał publiczny + prywatny (PPP)	Dotacja (art. 106 ustawy o ochronie ludności i obronie cywilnej)	Mechanizm dźwigni i kategoria inwestycyjna
Majątek publiczny	Tereny powojskowe, kolejowe, miejskie	Zarządzanie projektowe	Logika portfelowa; majątek tworzący wartość

Warto uwzględnić jeszcze jeden wymiar, który wykracza poza samą infrastrukturę. Klastry obronne rozwijają się najpełniej tam, gdzie towarzyszą im funkcje mieszkaniowe i usługowe: zakwaterowanie dla relokującej się kadry, zaplecze badawcze, usługi podnoszące standard życia. Szacuje się, że sektor obronny wraz z siłami zbrojnymi i zapleczem technicznym może do 2035 r. potrzebować rzędu 250 tys. nowych pracowników. Równoległe planowanie funkcji mieszkaniowej sprawia, że dobrze zaprojektowany klaster rzeczywiście tętni życiem. Rola samorządu jest tu istotna, ponieważ to on planuje przestrzeń i uzbraja tereny; rynek może te potrzeby zwymiarować i obsłużyć.

Wspólnym mianownikiem tych czterech obszarów jest stopniowe przejście od logiki zgodności ku logice zdolności. Zmiana ta nie wymaga mnożenia obowiązków, lecz mądrzejszego ułożenia narzędzi, którymi już dziś dysponujemy.

5.3 Propozycje działań

Na podstawie analizy instrumentów i doświadczeń nordyckich do rozważenia proponowana byłaby np. następująca sekwencja działań w trzech horyzontach czasowych.

W pierwszym etapie (do końca 2026 r.) kluczowe jest: maksymalne zaabsorbowanie środków KPO przed terminem kwalifikowalności; uruchomienie naborów FBIO z priorytetem dla projektów Filarów 1 i 6; aktywne włączenie się do programu RESCEU jako kraju goszczącego rezerwy strategiczne; aktywizacja polskich projektów CEF Mobilność Wojskowa pod nowa perspektywa finansowa 2028–2034 (17,6 mld euro); sfinalizowanie wydzielenia cywilno-wojskowego komponentu w krajowym planie SAFE.

W tym samym horyzoncie czasowym zasadne jest uruchomienie pilotażowego finansowania cyfrowej paszportyzacji i monitorowania gotowości wybranych zasobów odpornościowych, w szczególności obiektów ochrony ludności, miejsc czasowego zakwaterowania ewakuowanych oraz infrastruktury technicznej warunkującej ich użycie. Pilotaż powinien obejmować standard danych, minimalny zakres monitorowanych parametrów zgodnych z rozporządzeniami Ustawy o Ochronie Ludności i Obronie Cywilnej, integrację z centrami zarządzania kryzysowego, wymagania cyberbezpieczeństwa oraz mierniki efektu odpornościowego.

W drugim etapie (lata 2027–2028) niezbędne jest przyjęcie nowego rozwiązania (np. Funduszu Odpornosci Narodowej) jako trwałego instrumentu „post-KPO", zasilanego np. z opłat koncesyjnych operatorów infrastruktury krytycznej i wydzielonej części wpływów z VAT. Wzorcem jest fiński model NESA. Równolegle powinno nastąpić wprowadzenie ustawowego obowiązku budowy schronów dual-use w nowych inwestycjach budowlanych.

W trzecim etapie (perspektywa 2028–2030) priorytetem stają się aktywne negocjacje alokacji dla Polski w nowej perspektywie EDF i CEF oraz pełna integracja systemu OLIOC z systemem ochronnym na wzór szwedzki (Totalforsvaret), obejmującym sektory komercyjne, samorządy i organizacje społeczne.

Aby urzeczywistnić tak szeroki model obrony cywilnej, fundamentem staje się wdrożenie i rygorystyczne egzekwowanie ustawowego obowiązku budowy schronów o podwójnym przeznaczeniu we wszystkich nowych inwestycjach budowlanych. Włączenie prywatnych inwestorów w proces tworzenia infrastruktury ochronnej ma z założenia odciążyć sektor publiczny. Jednak realizacja tak ambitnego planu rozbudowy bazy obiektów zbiorowej ochrony (OZO) – nawet przy udziale podmiotów komercyjnych – nieuchronnie obnaża słabości i braki w obecnym modelu alokacji środków państwowych.

Należy pamiętać, że system finansowania zadań OLIOC został oparty na kilku mechanizmach, które mają zapewnić JST możliwość realizacji zadań: (1) ustawa OLOC gwarantuje minimalny poziom finansowania – 0,3% PKB rocznie – jest to stały element polityki budżetowej państwa, (2) program ochrony ludności na lata 2025–2026 i potem na każdy okres dwuletni określa priorytet oraz zakres inwestycji. W ramach tego programu OZO stanowią jedno z wielu zadań w ramach OLIOC. W ramach tego programu JST mogą otrzymywać dotacje celowe od MSWiA, których dysponentem w terenie jest wojewoda, (3) środki własne jednostek samorządu terytorialnego muszą być określone w budżetach i wieloletnich prognozach finansowych JST, (4) wsparcie rzeczowe i finansowe Rządowej Agencji Rezerw Strategicznych dla JST. W powszechnej ocenie samorządów, źródła te są drastycznie niewystarczające do osiągnięcia zakładanych poziomów dostępu do OZO, co będzie zmuszać gminy do zadłużania się na zasadach komercyjnych.Istnieje obawa, że wypłata środków z budżetu, takich jak dotacje celowe, pożyczki z FBIO – poza tym, że nie pokryje w całości wydatków na budowę OZO, będzie przekazywana z opóźnieniem albo po zakończeniu budowy, stosownie do płynności budżetu centralnego i FBIO. JST mogą w tym wypadku liczyć tylko na środki własne, które w zdecydowanej większości będą pochodziły z banków komercyjnych oprocentowane na poziomie komercyjnym oraz będą zwiększać zadłużenie JST.

W tym kontekście postulowane jest stworzenie ram dla uruchomienia obligacji JST na budowę OZO. Emisja obligacji OZO mogłaby zostać wsparta następującymi zmianami legislacyjnymi:

- wyłączeniem zysku z obligacji z opodatkowania podatkiem od zysków kapitałowych,
- wyłączeniem (tak jak w przypadku obligacji przychodowych) ze wskaźników zadłużenia JST w ramach ustawy o finansach publicznych,
- umożliwieniem spłaty obligacji środkami uzyskanymi z dotacji, budżetu centralnego.

W ten sposób JST uzyskałyby prefinansowanie finansowania z dostępnych obecnie mechanizmów wsparcia oraz możliwość sfinansowania wkładu własnego bez pogorszenia wskaźników zadłużenia, co przyczyniłoby się do szybszej i efektywniejszej realizacji projektów zmierzających do osiągnięcia zakładanych poziomów dostępności OZO.

Skala dual-use w Polsce najpełniej rozwinie się w oparciu o model łączący kapitał publiczny i prywatny. Punktowe dotacje mogą być jego uzupełnieniem, lecz to trwały mechanizm finansowania nadaje całości skalę. Poniższe kierunki ujęto opisowo, wskazując mechanikę i cel, a nie brzmienie przepisów, którego wypracowanie należy do strony publicznej. Porządkuje je prosty podział: na to, co może ustanowić państwo, oraz na to, co operacyjnie może wnieść rynek.

Uruchomienie proponowanych narzędzi dla samorządów stanowi fundament publiczny, jednak prawdziwy przełom wymaga zaangażowania drugiej strony tego równania – kapitału prywatnego. Aby przenieść ciężar finansowania z budżetu państwa na mechanizmy rynkowe, konieczne jest stworzenie płaszczyzny porozumienia między regulatorem a inwestorami komercyjnymi. Pierwszym i najważniejszym krokiem na tej drodze jest zmiana sposobu postrzegania samych inwestycji ochronnych. Rozpoznawalność dual-use jako klasy aktywów to kluczowy element całej koncepcji. Jednoznaczna, zdefiniowana kategoria obiektów o funkcji cywilno-obronnej pozwoli instytucjom finansowym i ubezpieczycielom w pełni uczestniczyć w ich finansowaniu. Zrozumiała kategoria inwestycyjna, mierzalne ryzyko i przewidywalne przepływy sprawiają, że dual-use zaczyna funkcjonować jak inne segmenty rynku nieruchomości, a pozostałe mechanizmy zyskują trwały punkt oparcia.

Sprawdzonej analogii dostarcza energetyka, w której państwo płaci nie tylko za zużytą energię, ale i za utrzymywaną w gotowości moc rezerwową. Tę samą logikę można z powodzeniem przenieść na odporność: państwo nabywa rezerwę bezpieczeństwa podobnie jak rezerwę mocy. Mechanizm taki najlepiej działa, gdy jest przewidywalny i znany inwestorowi przed decyzją

oraz stopniowany według klasy ochrony – im wyższa i trwalsza odporność, tym silniejsza zachęta. Tak skonstruowany, wzmacnia ochronę tam, gdzie ludzie się schronią w pierwszej kolejności, a jej koszt najtrudniej udźwignąć i jednocześnie uruchamia zdolność konwersyjną tam, gdzie jest ona najtańsza. Tak rozumiana płatność za gotowość jest zarazem offsetem dodatkowej warstwy ochronnej: rekompensuje inwestorowi nakład, który komercyjnie nie zwraca się sam, tak by utrzymywanie obiektu w pełnej sprawności, a więc jego realna zdolność w kryzysie, nie odbywało się jego kosztem.

Istotą tego kierunku jest profesjonalizacja, a nie prywatyzacja: własność publiczna i pełna kontrola państwa nad bezpieczeństwem pozostają nienaruszone. Narzędzia: długoterminowa dzierżawa, wyspecjalizowane wehikuły zarządcze, w wybranych przypadkach sprzedaż z leasingiem zwrotnym, pozwalają, by zasób zaczął służyć mieszkańcom i generować środki wracające na cele obronne i społeczne.

Skala możliwego zaangażowania jest realna: na rynkach dojrzałych portfele obronne o wartości około 14 mld USD bywają wyceniane i zarządzane przez doradców rynkowych przy zachowaniu pełnej kontroli publicznej. Powstaje w ten sposób obieg, w którym majątek państwa współfinansuje jego własną odporność.

To jeden z najskuteczniejszych, a zarazem najmniej kosztownych dla budżetu kierunków. Inwestycje o podwyższonej klasie ochrony mogłyby korzystać z przyspieszonych, przewidywalnych procedur planistycznych i budowlanych. Naturalnym narzędziem jest Zintegrowany Plan Inwestycyjny, który pozwala sprawnie ustalić warunki zabudowy, a przez umowę urbanistyczną, powiązać tę ścieżkę ze zobowiązaniem inwestora do dostarczenia realnej zdolności ochronnej w zamian za pewność planistyczną. Po stronie realizacyjnej tę samą logikę warto rozciągnąć na etap budowlany: pozwolenia na budowę (PnB) oraz odbiory techniczne obiektów dual-use powinny mieć priorytetową, terminową ścieżkę, wraz z uproszczonymi i przewidywalnymi uzgodnieniami z organami obrony cywilnej. Dziś długość i niepewność tych procedur obciąża najmocniej właśnie rozwiązania ambitniejsze i trwalsze, a więc działa odwrotnie do celu raportu. W tym samym trybie dostęp do gruntu trudno dostępnego w zwykłych warunkach może stanowić pozabudżetową formę offsetu, dla części inwestorów rekompensatę cenniejszą niż dotacja. Skrócenie i uprzewidywalnienie procedur działa jak zachęta, która nie obciąża budżetu, a oszczędza czas i kapitał obu stronom.

Rynek nie zastępuje państwa ani samorządu, lecz może być ich partnerem technicznym i wykonawczym. Wnosi metodykę przeglądu zasobu: systematyczną ocenę obiektów pod kątem kosztu i wykonalności adaptacji, która nadaje mapie potrzeb wymiar kosztowy. Wnosi sposób wyceny gotowości, ujęcie utrzymywanej dyspozycyjności w wartości aktywa. Wnosi wreszcie operacjonalizację zasady dodatkowości: praktyczne odróżnienie nakładu tworzącego nową zdolność od nakładu zastępującego inwestycję powstającą i tak. Doświadczenia międzynarodowe potwierdzają wartość takiej współpracy: outsourcing facility management baz wojskowych w Belgii (kontrakt rzędu 30 mln EUR) pozwolił skierować 61 żołnierzy do służby liniowej – czytelny dowód, że dobrze ułożona współpraca z rynkiem uwalnia zdolności po stronie publicznej i obniża koszt utrzymania obiektów, przy zachowaniu pełnej kontroli zamawiającego.

Punktem wyjścia dla całości tych działań jest powołanie Rady ds. Odpornosci jako organu koordynującego wydatkowanie i sprawozdawczość kategorii 1,5% NATO, skupiającego przedstawicieli kluczowych resortów, BGK, RARS oraz niezależnych ekspertów cywilnych. Doświadczenia Finlandii i Szwecji jednoznacznie wskazują, że skuteczność systemu finansowania odpornosci nie zależy od skali pojedynczych instrumentów, lecz od trwałości ram instytucjonalnych, przewidywalności finansowania i zaangażowania całego społeczeństwa. Polska dysponuje środkami i instrumentami; brakuje jej na razie trwałej architektury zarządzania nimi.

6 Strategia budowy i modernizacji schronów

Rozdział stanowi rozwinięcie Priorytetu A (20% alokacji) i określa kompleksową strategię tworzenia krajowej sieci schronów ochrony ludności cywilnej. Kluczowym elementem strategii jest koncepcja dual-use, zapewniająca efektywne ekonomicznie wykorzystanie infrastruktury zarówno w czasie pokoju, jak i w sytuacjach kryzysowych.

6.1 Schrony a prawo międzynarodowe

Budowa skutecznego systemu schronów dla ludności cywilnej wymaga przede wszystkim precyzyjnego rozumienia tego, czego prawo międzynarodowe od państw wymaga, a czego nie reguluje. Granica ta ma fundamentalne znaczenie praktyczne: określa, gdzie kończy się sfera zobowiązań traktatowych, a gdzie zaczyna autonomia ustawodawcy krajowego. W dziedzinie schronów cywilnych granica ta przebiega wyraźnie: prawo humanitarne chroni schrony jako kategorię obiektów i zapewnia im nietykalność w czasie konfliktu zbrojnego, ale nie ustanawia żadnych wiążących norm technicznych dotyczących ich konstrukcji, filtracji powietrza ani autonomii zasilania. Parametry te pozostają wyłączną prerogatywą państw.

Podstawowym aktem prawa humanitarnego w tej dziedzinie jest Protokół Dodatkowy I do Konwencji Genewskich z 1977 r.[136] („PD"), ratyfikowany przez Polskę w 1992 r. Art. 61 rozdziału VI poświęcony został obronie cywilnej, definiuje obronę cywilną przez katalog piętnastu zadań humanitarnych, wśród których wprost wymieniono „dostarczanie i organizowanie schronów". Definicja ta ma charakter zadaniowy, nie podmiotowy ani techniczny – protokół określa, co schrony mają zapewniać, a nie z jakich materiałów mają być zbudowane ani jaką odporność na nadciśnienie powinny wykazywać.

Art. 62 PD zobowiązuje strony konfliktu do poszanowania i ochrony „budynków i sprzętu używanych do celów obrony cywilnej". Art. 65 precyzuje, w jakich okolicznościach ochrona ta ustaje, a mianowicie wówczas, gdy chroniony obiekt lub organizacja dopuści się czynów wrogich wykraczających poza zakres humanitarnych zadań obrony cywilnej. Art. 66 wraz z Aneksem I ustanawia międzynarodowy znak rozpoznawczy obrony cywilnej: niebieski trójkąt równoboczny na pomarańczowym tle.

Dla planowania przestrzennego schronów kluczowa jest zasada rozróżnienia (principle of distinction), wyrażona w art. 48 i 51–52 PD. Nakazuje ona stronom konfliktu odróżnianie obiektów cywilnych od celów wojskowych i zakazuje atakowania tych pierwszych. Art. 51 ust. 7 wprost zakazuje wykorzystywania ludności cywilnej i obiektów cywilnych jako osłony dla operacji wojskowych. Konsekwencja praktyczna jest jednoznaczna: lokowanie schronów cywilnych w bezpośrednim sąsiedztwie obiektów wojskowych lub instalacji stanowiących prawowite cele ataku może doprowadzić do utraty przez nie ochrony prawnej. Planowanie przestrzenne schronów musi zatem uwzględniać normy prawa humanitarnego już na etapie wydawania decyzji lokalizacyjnych, a nie dopiero po ich wybudowaniu.

Podsumowując, Protokół Dodatkowy I tworzy solidną tarczę prawną dla schronów: zakazuje ich atakowania, niszczenia i zmiany przeznaczenia przez stronę przeciwną, ale nie zawiera ani jednej normy budowlanej. Wszystkie parametry techniczne: odporność na falę uderzeniową, skuteczność filtracji CBRN, długość autonomii zasilania i minimalny metraż na osobę, są domeną prawa krajowego. Luka ta, zamiast osłabiać system, odzwierciedla zasadę pomocniczości: szczegółowe rozwiązania techniczne zależą od zagrożeń regionalnych, klimatu, gęstości zaludnienia i możliwości budżetowych każdego państwa.

6.2 Ramy NATO i UE

NATO nie posiada jawnego Porozumienia Standaryzacyjnego (STANAG) poświęconego schronom dla ludności cywilnej. W publikowanych katalogach Organizacji Standaryzacyjnej NATO (NSO) dokumenty techniczne dotyczące schronów mieszczą się w literaturze wojskowej lub dotyczą efektów broni na konstrukcje w kontekście militarnym, nie zaś standardów ochrony ludności cywilnej. Oznacza to, że schrony cywilne są traktowane przez NATO na poziomie zobowiązań politycznych i doktrynalnych, nie normatywno-technicznych.

Podstawowym instrumentem NATO w tej dziedzinie są Siedem Fundamentalnych Wymogów Odporności Narodowej (*Seven Baseline Requirements for National Resilience*, BLR[137]), przyjętych po raz pierwszy na szczycie w Warszawie w 2016 r. Piąty filar tego pakietu obejmuje zdolność do zarządzania masowymi ofiarami i poważnymi kryzysami zdrowotnymi, a zatem pośrednio, wymaga istnienia sprawnego systemu schronów i ochrony ludności. Kolejne szczyty sukcesywnie rozwijały ten kierunek: Bruksela 2021 wzmocniła zobowiązania w ramach Strengthened Resilience Commitment, Madryt 2022 zintegrował planowanie odporności z procesem NDPP, a Waszyngton 2024 połączył planowanie cywilne z wojskowym. Polska, dążąc do zaliczenia wydatków schronowych do tej kategorii, powinna wypracować transparentną metodologię mapowania tych wydatków na odpowiednie filary BLR, zwłaszcza filar 5, co ułatwi sprawozdawczość wobec NATO i wzmocni wiarygodność deklarowanych kwot.

Unia Europejska nie dysponuje prawnie wiążącym instrumentem regulującym budowę schronów cywilnych. Dyrektywa o odporności podmiotów krytycznych (CER, 2022/2557), obejmująca 11 sektorów infrastruktury, dotyczy schronów jedynie pośrednio, przez wymogi odporności dla podmiotów krytycznych w sektorze ochrony zdrowia, takich jak szpitale[138]. UE pozostaje zatem na poziomie koordynacji i wydawania rekomendacji, a ciężar wdrożenia konkretnych standardów technicznych spoczywa na państwach członkowskich.

Strategia Unii ds. Gotowości, przyjęta 26 marca 2025 r., stanowi najważniejszy dotychczas dokument UE w tej dziedzinie. Wśród 30 działań priorytetowych szczególne znaczenie mają dwa: wezwanie do zapewnienia obywatelom 72-godzinnej samowystarczalności (minimum zaopatrzenia domowego w wodę, żywność i leki) oraz ustanowienie minimalnych kryteriów gotowości dla szpitali, szkół, sieci transportowych

i telekomunikacyjnych. Dokument nie określa wprost wymagań dla schronów publicznych, ale tworzy ogólny kontekst normatywny, w ramach którego 72-godzinna autonomia staje się minimalnym standardem europejskim i punktem odniesienia dla polskich rozporządzeń technicznych[139]. Intelektualnym zapleczem tej strategii jest wspomniany już raport *Safer Together* z 30 października 2024 r., przygotowany na zlecenie przewodniczącej Komisji Europejskiej Ursuli von der Leyen. Były prezydent Finlandii Sauli Niinistö, opierając się na fińskim doświadczeniu systemu ochrony ludności, rekomendował podejście all-hazards, w którym schrony są elementem zintegrowanego systemu obronności cywilnej, a nie wyizolowaną inwestycją infrastrukturalną. Raport stwierdził też, że 58% obywateli UE nie uważa się za dobrze przygotowanych na kryzys, i zaproponował przeznaczenie co najmniej 20% budżetu UE na bezpieczeństwo i gotowość kryzysową.[140]

6.3 Przykłady polityk publicznych Finlandii, Szwajcarii, Szwecji i Estonii

W braku wiążących standardów technicznych na poziomie NATO i UE jedynym praktycznym punktem odniesienia są rozwiązania krajowe. Cztery państwa europejskie oferują wzorce o szczególnej wartości diagnostycznej: Finlandia, która w ciągu dekad zbudowała najpełniejszy i najlepiej skodyfikowany system schronowy spośród demokracji zachodnich; Szwajcaria, która jako pierwsza wprowadziła zasadę miejsca schronienia dla każdego mieszkańca i konsekwentnie ją realizuje od ponad sześćdziesięciu lat; Szwecja, reaktywująca program schronowy po kilkunastoletniej przerwie; oraz Estonia – państwo frontowe, które od 2022 r. buduje system od zera i jest pod tym względem najbliższym porównaniem dla Polski.

W Finlandii podstawę prawną systemu schronowego stanowi *Pelastuslaki* – ustawa ratownicza z 2011 r. (379/2011). Jej przepisy §71–79 nakładają na inwestorów budynków mieszkalnych o powierzchni powyżej 1 200 m² brutto obowiązek wydzielenia schronu o powierzchni odpowiadającej co najmniej 2% powierzchni budynku. Dla budynków przemysłowych i magazynowych próg wynosi 1 500 m², a wymagany udział schronu – 1%. Szczegółowe parametry techniczne określa rozporządzenie Ministerstwa Spraw Wewnętrznych nr 506/2011, uzupełnione rozporządzeniem Rady Państwa nr 408/2011. Schrony klasy S1, dominujące w zabudowie miejskiej, muszą posiadać co najmniej dwa niezależne wzmocnione wyjścia, hermetyczną instalację filtrowentylacyjną CBRN zdolną do pracy bez zewnętrznego zasilania elektrycznego (napęd ręczny), filtry HEPA połączone z warstwą węgla aktywnego, automatyczne zawory nadciśnieniowe oraz wyposażenie zapewniające autonomię przez co najmniej 72 godziny od ogłoszenia gotowości przez władze. Filtry muszą spełniać wymogi eksploatacyjne w zakresie temperatur od –30°C do +70°C i być zaprojektowane na minimalny okres użytkowania wynoszący trzydzieści lat. System ten w ciągu kilku dziesięcioleci doprowadził do powstania ponad 50 000 schronów zapewniających miejsca ochronne dla ok. 4,8 mln osób – ok. 87% populacji kraju, a w Helsinkach ponad 130%.[141]

Szwajcarski model ochrony ludności oparty jest na zasadzie konstytuującej sformułowanej w prawie federalnym już w 1963 r.: każdy mieszkaniec ma mieć dostęp do miejsca schronienia. Obecna podstawa prawna to Federalna Ustawa o Ochronie Ludności i Obronie Cywilnej (BZG, SR 520.1) w wersji obowiązującej od 1 stycznia 2020 r. Inwestorzy budynków powyżej progu 38 izb mieszkalnych zobowiązani są do wybudowania schronu prywatnego (*Privater Schutzraum*, PRO); przy mniejszych budynkach uiszcza się opłatę zastępczą zasilającą fundusz budowy schronów publicznych. Schrony klasy PRO projektuje się

na nadciśnienie 1 bara (100 kPa), co odpowiada klasie S-1 przyjętej w polskim rozporządzeniu MSWiA z 2025 r. Wyposażenie obejmuje hermetyczne drzwi i zamknięcia, małe instalacje wentylacyjne z ręcznym napędem oraz filtry piaskowe i gazowe; obiekt musi być możliwy do przywrócenia do funkcji ochronnej w ciągu pięciu dni od wezwania, jeśli w czasie pokoju jest użytkowany jako piwnica lub parking. Łącznie Szwajcaria dysponuje ok. 360 000 schronów prywatnych i 5 100 publicznych – łącznie ok. 9 mln miejsc, czyli ok. 110% całej populacji.[142]

Szwecja, po kilkunastoletniej przerwie w aktywnej polityce schronowej, od 2022 r. systematycznie odbudowuje zdolności ochrony ludności. Podstawę prawną stanowią akty wydane pierwotnie przez SRV (Statens räddningsverk), utrzymane w mocy przez jego następcę MSB, a od 1 stycznia 2026 r. – przez nową agencję MCF (Swedish Civil Defence and Resilience Agency). Aktualnym dokumentem referencyjnym dla nowo budowanych schronów jest norma *Skyddsrum SR 15* z 2024 r. Szwecja dysponuje ok. 64 000 schronami (*skyddsrum*) o łącznej pojemności ok. 7 mln miejsc (81% populacji). W 2018 r. MSB rozdało wszystkim gospodarstwom domowym broszurę *Om krisen eller kriget kommer* („Jeśli nadejdzie kryzys lub wojna") – wzór komunikacji kryzysowej wart naśladowania[143].

Estonia, kraj o powierzchni i populacji zbliżonej do pojedynczych województw Polski, dostarcza szczególnie istotnej lekcji jako państwo frontowe, które po 24 lutego 2022 r. zdecydowało się zbudować system schronowy niemal od zera. W 2024 r. Riigikogu znowelizował ustawę o stanach nadzwyczajnych, nakładając obowiązek budowy schronów w nowych budynkach mieszkalnych i użyteczności publicznej powyżej 1 200 m^2 – próg identyczny z fińskim, z terminem wdrożenia od 1 lipca 2026 r. dla nowych inwestycji i od 1 lipca 2028 r. dla budynków istniejących. Cel polityczny zakłada wzrost pokrycia ludności ze śladowych 5–7% do 75% znających swoje miejsce schronienia w ciągu czterech lat[144].

6.4 Diagnoza potrzeb infrastruktury ochronnej w Polsce

Obecny stan infrastruktury ochronnej w Polsce stanowi jeden z najbardziej krytycznych punktów w architekturze bezpieczeństwa narodowego, będący wynikiem wieloletniej luki legislacyjnej oraz braku systematycznego finansowania, co w dobie rosnących zagrożeń geopolitycznych stawia państwo przed koniecznością natychmiastowej redefinicji priorytetów wydatkowych. Jak wskazują raporty Najwyższej Izby Kontroli[145], w kraju de facto nie funkcjonuje zorganizowany, spójny system budowli ochronnych, a te, które formalnie figurują w ewidencjach, w przeważającej mierze nie gwarantują realnego bezpieczeństwa. Z ogólnopolskiej inwentaryzacji przeprowadzonej przez Państwową Straż Pożarną na zlecenie MSWiA wynika, że choć zidentyfikowano blisko 62 tysiące obiektów o charakterze osłonowym, to zaledwie nieco ponad tysiąc z nich (ok. 1,6% ogółu badanych struktur) można uznać za budowle w pełni spełniające techniczne parametry schronu. Oznacza to, że w skali kraju profesjonalna ochrona zbiorowa jest dostępna dla niespełna ułamka populacji, co drastycznie odbiega od standardów państw takich jak Szwajcaria czy Finlandia.

Problem ten nie dotyczy wyłącznie liczby obiektów, lecz także braku aktualnej wiedzy o ich stanie technicznym, dostępności i gotowości do użycia. Obiekt ujęty w ewidencji nie musi być zasobem operacyjnie gotowym, jeżeli nie ma potwierdzonego dostępu do energii, wody, wentylacji, ogrzewania, łączności, sprawnych wejść, aktualnej pojemności oraz informacji o ograniczeniach użytkowania. Dlatego diagnoza potrzeb infrastruktury ochronnej powinna obejmować nie tylko inwentaryzację obiektów, lecz także mechanizm bieżącej weryfikacji ich statusu.

Ten krytyczny deficyt jest szczególnie alarmujący w dużych aglomeracjach miejskich, które w doktrynach wojskowych uznawane są za cele strategiczne. Audyty przeprowadzone w stolicy oraz innych centrach metropolitalnych wskazują na systemową zapaść: niemal żaden z nowoczesnych obiektów podziemnych, w tym parkingi pod wielkopowierzchniowymi biurowcami czy nowymi osiedlami deweloperskimi, nie spełnia norm technicznych przewidzianych przez Ministerstwo Obrony Narodowej dla ochrony przed skutkami użycia broni konwencjonalnej, wystąpieniem fali uderzeniowej czy skażeniami. Większość istniejącej bazy to obiekty z okresu zimnej wojny, które ze względu na brak konserwacji uległy degradacji fizycznej: są zdewastowane, pozbawione sprawnych systemów filtrowentylacyjnych (NBC), a często również zalane wodami gruntowymi lub odcięte od mediów. W konsekwencji zasoby te pełnią rolę wyłącznie statystyczną, nie oferując realnej ochrony w warunkach rzeczywistego kryzysu.

Problem potęguje tzw. „fikcja statystyczna" i chaos terminologiczny. W polskim porządku prawnym przez dekady brakowało ustawowej definicji schronu, co pozwalało na wliczanie do ewidencji tzw. miejsc doraźnego schronienia (MDS). Są to zazwyczaj piwnice, garaże podziemne lub tunele metra, które choć mogą chronić przed odłamkami, nie posiadają wzmocnionej konstrukcji odpornej na nadciśnienie, systemów autonomicznego zasilania ani systemu filtrowentylacji. Jak zauważa Rzecznik Praw Obywatelskich w swoich wystąpieniach do MSWiA[146], brak jasnych standardów technicznych doprowadził do sytuacji, w której obywatele nie mają wiedzy, gdzie faktycznie mogą szukać ratunku, a system aplikacji mobilnych (na czele z oficjalnym narzędziem MSWiA, platformą „Gdzie się ukryć" gdziesieukryc.pl), wskazuje miejsca, które w praktyce nie przeszły weryfikacji pod kątem odporności inżynieryjnej.

Kolejnym filarem diagnozy jest paraliż decyzyjny wynikający z rozproszenia kompetencji. Odpowiedzialność za utrzymanie infrastruktury jest obecnie rozmyta między samorządy, spółdzielnie mieszkaniowe i właścicieli prywatnych, przy całkowitym braku centralnego mechanizmu finansowania modernizacji. Gminy, obciążone wydatkami bieżącymi, nie są w stanie samodzielnie udźwignąć kosztów rewitalizacji schronów, których cena często przewyższa koszt budowy nowych obiektów. Z perspektywy ekonomicznej, luka ta tworzy barierę dla rozwoju budownictwa biorącego pod uwagę aspekt odporności, wg. doświadczeń fińskich budowa schronów pod budynkami mieszkalnymi podnosi koszty inwestycji od 2 do 5%, ale brak jest odpowiednich ulg podatkowych lub dotacji.

Skalę potrzeby da się dziś oszacować ilościowo. Analiza krajowa wyznacza minimalne zapotrzebowanie Polski na ok. 32 tys. budowli ochronnych (32 376), przy założeniu realnego zasięgu pieszego ok. 35 ha na obiekt, mniej niż połowa teoretycznego koła o promieniu 500 m (78,5 ha), ponieważ droga biegnie ulicami, nie w linii prostej. Średnia pojemność pojedynczego obiektu wypada wówczas na ok. 513 osób w rdzeniach największych miast, ok. 303 w miastach powiatowych i ok. 207 w gminnych[147]. Wniosek jest istotny dla doboru kategorii: nawet przy ambitnym podniesieniu celu pokrycia z ustawowych 25% do 50% ludności trzon programu pozostaje w paśmie schronu lekkiego, a najcięższe klasy dotyczą wyłącznie gęstych centrów wielkich miast. To empiryczny argument za tym, by kategorią bazową uczynić obiekt mały, tani i powtarzalny, a liczba 32 376 jest minimum wynikającym z obecnej zabudowy (dane GUS), więc wraz z urbanizacją obiektów będzie przybywać, a ich jednostkowe pojemności pozostaną niskie.

Wprowadzenie dedykowanej alokacji w wysokości 1,5% PKB na bezpieczeństwo i odporność ma na celu radykalne przełamanie tego impasu. Diagnoza potrzeb wskazuje, że środki te muszą zostać skierowane na fizyczną budowę oraz stworzenie sprawnego ekosystemu inżynierii odpornościowej. Należy jednak zaznaczyć, że polska branża budowlana wykazuje obecnie głęboki deficyt w zakresie zaawansowanych technologii ochronnych – brakuje krajowych producentów oferujących sprawdzone i certyfikowane rozwiązania, takie jak systemy filtrowentylacji (CBRN) o najwyższej wydajności. Masowa skala i krytyczna pilność potrzeb (budowa obiektów zbiorowej ochrony dla co najmniej 25% populacji w ciągu dekady) oznaczają, że system państwowy nie dysponuje marginesem czasu na ewolucyjne rozwijanie tych technologii od podstaw. Z perspektywy zarządzania ryzykiem, najbardziej racjonalnym modelem wdrożeniowym jest oparcie się na wieloletnim doświadczeniu państw posiadających dojrzałe systemy ochrony ludności, w szczególności Finlandii. Zastosowanie gotowych, przetestowanych rozwiązań od zagranicznych liderów rynku pozwala na natychmiastową

implementację najwyższych standardów bezpieczeństwa i ominięcie fazy kosztownych błędów projektowych, które nieodłącznie towarzyszą tworzeniu nowych gałęzi przemysłu. W średnim i długim terminie to właśnie współpraca technologiczna ze sprawdzonymi podmiotami zagranicznymi powinna stanowić fundament do stymulowania krajowego przemysłu poprzez licencjonowanie i transfer technologii, co pozwoli docelowo uniknąć pełnego uzależnienia od importu

Podsumowując, bez pilnej interwencji legislacyjnej w postaci ustawy o ochronie ludności oraz stabilnego fundamentu finansowego, polska infrastruktura ochronna pozostanie zbiorem przypadkowych obiektów o wątpliwej użyteczności. Stan obecny to nie tylko zaniedbanie techniczne, ale przede wszystkim ryzyko strategiczne: brak ochrony ludności cywilnej paraliżuje zdolność państwa do długotrwałego oporu i obniża morale społeczne. Inwestycja w nowoczesne schrony typu dual-use (np. wzmocnione garaże, obiekty sportowe[148], czy magazyny medyczne) jest jedynym ekonomicznie uzasadnionym sposobem na budowę realnej odporności kraju, gdzie infrastruktura służy obywatelom w czasie pokoju, a gwarantuje przeżycie w czasie wojny. Wszystkie przywołane dane z kontroli NIK oraz analiz MSWiA zbiegają się w jednej konkluzji: Polska potrzebuje natychmiastowego przejścia od fazy inwentaryzacji do fazy masowych inwestycji strukturalnych, wspieranych przez mechanizm 1,5% PKB.

6.5 Polskie ramy prawne: od próżni regulacyjnej do kompleksowej kaskady legislacyjnej

Polska przez ponad trzydzieści lat po 1989 r. funkcjonowała bez ustawowej definicji schronu, ukrycia i budowli ochronnej. Ustawa z 21 listopada 1967 r. o powszechnym obowiązku obrony zawierała jedynie ramowe przepisy o zadaniach obrony cywilnej; uchylenie jej bez odpowiednich przepisów przejściowych przez ustawę o obronie Ojczyzny z 11 marca 2022 r. wytworzyło dwuletnią próżnię regulacyjną. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907), która weszła w życie 1 stycznia 2025 r., a następnie została istotnie znowelizowana ustawą z dnia 17 kwietnia 2026 r., stanowi pierwszą w historii III Rzeczypospolitej kompleksową regulację tej dziedziny. Ustawa wprowadza trójstopniową klasyfikację obiektów zbiorowej ochrony: schron (najwyższy standard ochrony, odporność na fale uderzeniowe i filtracja CBRN), ukrycie (ochrona przed odłamkami i efektami pośrednimi) oraz miejsce doraźnego schronienia (MDS – ochrona minimalna, tymczasowo przystosowane obiekty budowlane o najniższym standardzie ochrony). Odrębną, wprowadzoną nowelizacją z 2026 r. kategorią są punkty schronienia – miejsca w obiektach budowlanych lub w innych lokalizacjach, zapewniające podstawową ochronę przed nagłymi zjawiskami pogodowymi i skutkami użycia konwencjonalnych środków rażenia, w szczególności odłamkami. Obowiązek realizacji zadań z zakresu ochrony ludności i obrony cywilnej ustawa powierza przede wszystkim jednostkom samorządu terytorialnego, statuując ochronę ludności zadaniem własnym JST, a organy JST – organami ochrony ludności i zapewniając im jednocześnie wsparcie z budżetu państwa – coroczne wydatki na ten cel nie mogą być niższe niż 0,3% PKB, a środki te trafiają do samorządów w formie dotacji celowych. Definiując pojęcie „obrony cywilnej", w art. 2 ust. 2 ustawa wprost odesłała do definicji obrony cywilnej z art. 61 lit. a Protokołu Dodatkowego I, czym zakotwicza polskie prawo krajowe w reżimie prawa humanitarnego[149].

Klasyfikacja obiektów zbiorowej ochrony powinna zostać uzupełniona o standard danych

opisujących ich gotowość operacyjną. W praktyce oznacza to potrzebę cyfrowego paszportu obiektu, obejmującego co najmniej: typ obiektu, lokalizację, pojemność, właściciela lub administratora, dostępność wejść, stan podstawowych instalacji, dostęp do mediów, wymagania techniczne, ograniczenia użytkowania, datę ostatniej weryfikacji oraz status gotowości. Taki standard umożliwia porównywanie obiektów, aktualizowanie danych przez administratorów oraz raportowanie gotowości do właściwych struktur zarządzania kryzysowego.

Kaskadę wykonawczą tworzą cztery rozporządzenia MSWiA, wydane w 2025 r. Rozporządzenie z 21 lutego 2025 r. (Dz.U. 2025 poz. 235) określa kryteria uznawania obiektów za budowle ochronne i wprowadza sześciostopniową klasyfikację klas odporności[150]. Rozporządzenie z 9 lipca 2025 r. (Dz.U. 2025 poz. 932) reguluje wymagania techniczne dla miejsc doraźnego schronienia, w tym minimalną powierzchnię 1,5 m^2 na osobę, 2 m^2 dla osób poruszających się na wózkach oraz minimalne wymiary pomieszczenia[151]. Najważniejszym pod względem technicznym jest rozporządzenie MSWiA z 4 listopada 2025 r. (Dz.U. 2025 poz. 1548), które po raz pierwszy w historii polskiego prawa budowlanego ustala kompletne parametry konstrukcyjne budowli ochronnych – klasy odporności, wartości Pso, wymagania dotyczące filtracji i zasilania[152].

Wynikiem tej transformacji legislacyjnej jest wniosek, który powinien wybrzmieć wyraźnie w każdej dyskusji o finansowaniu schronów w ramach 1,5% PKB: Polska dysponuje dziś kompletną strukturą prawną, dorównującą lub przewyższającą ramy regulacyjne Estonii i Szwecji. Luka, którą kraj musi teraz wypełnić, ma charakter wyłącznie inwestycyjny i wykonawczy – chodzi o budowę dziesiątek tysięcy schronów i ukryć tam, gdzie dotychczas nie istniały żadne. To uzasadnia skalę i pilność planowanej alokacji budżetowej.

Rozporządzenie MSWiA z 4 listopada 2025 r. ustanawia sześć klas odporności budowli ochronnych, pogrupowanych w dwie rodziny: klasę U (ukrycia, trzy podklasy) i klasę S (schrony właściwe, trzy podklasy). Ukrycia klasy U-1 zapewniają jedynie ochronę przed odłamkami i ostrzałem małokalibrowym – odpowiadają typowym MDS w istniejących budynkach. Klasy U-3 wymagają już odporności na nadciśnienie Pso ≥ 60 kPa. Schrony klasy S-1 projektowane są na Pso ≥ 100 kPa przy czasie trwania fazy dodatniej t+ ≥ 100 ms, odporność na wstrząs ≥ 12,5 g oraz co najmniej 1000-krotne osłabienie promieniowania gamma. Parametr S-1 jest bezpośrednio porównywalny ze szwajcarskim standardem PRO (1 bar = 100 kPa), co świadczy o tym, że polska regulacja świadomie czerpie z najbardziej dojrzałych wzorców europejskich. Klasy S-2 (Pso ≥ 200 kPa, osłabienie γ ≥ 1500×) i S-3 (Pso ≥ 300 kPa) przewidziane są dla obiektów strategicznych, węzłów dowodzenia i obiektów o szczególnym znaczeniu dla ciągłości funkcjonowania państwa.

Poniższa tabela zestawia klasy odporności, wymagania dotyczące filtracji CBRN, autonomię i normę powierzchniową w ujęciu porównawczym.

Tabela 5. Klasy odporności, wymagania dotyczące filtracji CBRN, autonomia i norma powierzchniowa w ujęciu porównawczym

Kategoria	Pso (kPa)	Filtracja CBRN/NBC	Autonomia	m^2/os.	Wzorzec
MDS / U-1	Brak wymogu Pso (ochrona przed odłamkami)	Brak filtracji	–	1,5	PL (Dz.U. 2025 poz. 932)
U-3	≥ 60 kPa	Filtracja podstawowa	48 h	–	PL (Dz.U. 2025 poz. 1548)
S-1 / PRO	≥ 100 kPa	HEPA + węgiel aktywny, ręczna korba	72 h+	0,75–1,0	PL, FIN, CH
S-2	≥ 200 kPa	Pełna filtracja NBC, 1500x osłabienie γ	72 h+	–	PL (Dz.U. 2025 poz. 1548)
S-3	≥ 300 kPa	Pełna filtracja NBC, podwyższona klasa	96 h+	–	PL (obiekty specjalne)

Źródło: opracowanie własne na podstawie Dz.U. 2025 poz. 1548 i poz. 932 oraz danych fińskich (Pelastuslaki 379/2011, Decree 506/2011) i szwajcarskich (BZG SR 520.1, BABS).

Przy całej dojrzałości technicznej tej regulacji pozostaje w niej luka o charakterze systemowym: przepis precyzyjnie definiuje sześć kategorii i przypisuje im twarde parametry (nadciśnienie, krotność osłabienia gamma, odporność na wstrząs, autonomię), ale nie zawiera reguły, która mówiłaby, jaką kategorię zastosować w danej sytuacji. Rozporządzenie odwołuje się do doboru jedynie pośrednio, liczbę osób określa organ ochrony ludności, a obliczeniowy czynnik rażenia uwzględnia się, „jeżeli takie wymaganie określono", lecz żaden akt nie wyprowadza z tych danych kategorii. Skutek jest podwójny i w obu wariantach niekorzystny: albo dobór staje się uznaniowy (każdy organ i inwestor przyjmuje własną logikę, system traci porównywalność), albo paraliżujący (z ostrożności przyjmuje się najwyższą klasę „na wszelki wypadek", co winduje koszty i spowalnia program). Nowelizacja z 17 kwietnia 2026 r. dołożyła przy tym kolejną, najlżejszą warstwę: punkty schronienia, nie dodając reguły doboru, więc liczba warstw rośnie, a brakujące ogniwo pozostaje to samo. Polska zbudowała najlepszy w regionie słownik budowli ochronnych, lecz bez gramatyki, która pozwala ułożyć z liter zdanie[153].

Systemy filtracji CBRN/NBC we wszystkich omawianych wzorcach – Finlandii, Szwajcarii i Polsce, oparte są na tej samej zasadzie inżynierskiej: filtry HEPA połączone z węglem aktywnym eliminują cząstki biologiczne, chronią przed skażeniem radiologicznym i absorbują substancje chemiczne. Polska norma 48-godzinnej autonomii jest niższa od fińskiej 72-godzinnej i szwajcarskiej siedmiodniowej. Argument za harmonizacją z fińskim standardem 72 h jest zbieżność z rekomendacją EU Preparedness Union Strategy 2025 oraz fakt, że Polska, jako kraj frontowy NATO, powinna projektować system na scenariusze, w których przywrócenie normalnego funkcjonowania po ataku może trwać dłużej niż dwie doby.

Odrębnym wymiarem standardów technicznych jest dostępność schronów dla osób ze szczególnymi potrzebami. Rozporządzenie z 9 lipca 2025 r. wprowadza wymagania dla MDS (drzwi o minimalnej szerokości, rampy, dostosowane sanitariaty), wpisując się w ramy Europejskiego Aktu o Dostępności (dyrektywa 2019/882) transponowanego do polskiego prawa w lipcu 2024 r. Budowa systemu schronowego masowej skali daje historyczną szansę wbudowania dostępności jako standardu od początku projektowania, co powinno zostać uwzględnione w kryteriach przetargów realizowanych w ramach 20% alokacji z puli 1,5% PKB.

Konsekwencją tej logiki jest również propozycja, reformatorska, wymagająca zmiany rozporządzenia i traktowana tu jako głos do debaty inżynierskiej, nie jako stan obecny, by klasa oznaczała cały pakiet wymagań, a nie wyłącznie nadciśnienie. Dziś polski schron S-1 dźwiga pełny ciężar najwyższej klasy (REI 240, ≥ 1000-krotna osłona gamma, rozbudowany program socjalno-medyczny, pełna autonomia), przez co jest tak drogi, że nikt nie zbuduje go dobrowolnie tam, gdzie wolno postawić ukrycie. Ponieważ prawo nakłada obowiązek budowy „budowli ochronnej" (najtańszą jest ukrycie), a reguły doboru brak, racjonalny inwestor wybierze najtańsze U-1, które dziś niewiele różni się od miejsca doraźnego schronienia. Bez korekty powstaną więc tysiące najtańszych obiektów nazwanych „systemem ochrony ludności", w którym zabraknie schronów z prawdziwego zdarzenia. Propozycja porządkująca jest dwojaka: (1) zamiast trzech klas ukryć – jedno ukrycie o odporności S-1, lecz bez hermetyzacji CBRN, tak by jedyną cechą odróżniającą ukrycie od schronu była hermetyzacja; (2) „odchudzenie" masowego S-1 (REI 120, ok. 500-krotna osłona gamma, program minimalny) do odpowiednika fińskiego S1, przy świadomym uznaniu, że rezygnuje się z części ochrony radiacyjnej i ogniowej w zamian za masowość[154].

6.6 Lokalizacja

Schron nieosiągalny w czasie alarmu nie pełni żadnej funkcji ochronnej. Z pozoru oczywista teza ma fundamentalne konsekwencje planistyczne: decyzje o lokalizacji budowli ochronnych muszą być podejmowane nie w logice inwestycyjnej (gdzie łatwiej zbudować), lecz w logice operacyjnej (gdzie ludzie będą w chwili zagrożenia i ile czasu mają, by dotrzeć do schronienia). Oba parametry, miejsce przebywania ludzi oraz czas reakcji od alarmu, są regionalnie zróżnicowane i zależą od rodzaju zagrożenia: atak rakietowy wymaga minut, powódź – godzin, pandemii – dni.

Polskie prawo jest pod tym względem wyjątkowo precyzyjne na tle Europy. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych określa, że odległość od budowli ochronnej do miejsca przebywania ludności nie może przekraczać 500 m w granicach administracyjnych miast i 1 000 m poza tymi granicami. Odległość mierzy się nie w linii prostej, lecz wzdłuż przewidywanych dróg poruszania się ludności, co odpowiada realnym warunkom ewakuacyjnym. Zapis ten zawiera także ważne wyjątki – obszary zagrożone powodzią z prawdopodobieństwem ≥10% oraz strefy w bezpośrednim sąsiedztwie dużych budowli hydrotechnicznych są wyłączone z obowiązku, co chroni przed paradoksem lokalizowania schronu w miejscu będącym samym w sobie zagrożeniem[155]. Przy średnim tempie marszu osoby dorosłej wynoszącym 4–5 km/h norma 500 m odpowiada ok. 6–8 minutom marszu, zaś norma 1000 m – ok. 12–15 minutom. Z uwzględnieniem czasu identyfikacji najbliższego wejścia, ruchu w tłumie, osób o ograniczonej mobilności oraz trudnych warunków terenowych w scenariuszu kryzysowym, przelicznik ten odpowiada orientacyjnym standardom 10 minut w mieście i 20 minut poza nim, stosowanym w międzynarodowej debacie planistycznej jako benchmark dostępności infrastruktury ochronnej. Norma ta nie jest jednak twardym standardem NATO ani UE, żadne porozumienie standaryzacyjne Sojuszu ani żadna wiążąca dyrektywa UE nie określa maksymalnego czasu pieszego dojścia do schronu. Polski ustawodawca zoperacjonalizował ją jako wewnętrzkrajową normę metryczną, potwierdzając jej słuszność również w przepisach o budynkach użyteczności publicznej: rozporządzenie Rady Ministrów z 31 lipca 2025 r. zwalnia budynek z obowiązku posiadania własnej budowli ochronnej właśnie wtedy, gdy w promieniu 500 m istnieje inny schron wystarczający do ochrony użytkowników[156].

Na tle państw, które zbudowały dojrzałe systemy schronowe, model polski wyróżnia się tym, że norma dostępności jest explicite wyrażona w prawie. Finlandia i Szwajcaria – kraje o najwyższym pokryciu populacji, realizują cel przestrzennej bliskości innymi metodami. Fiński ustawodawca od 1958 roku stosuje logikę „budynek jako jednostka": ustawa ratownicza Pelastuslaki nakłada obowiązek budowy schronu w ramach każdej nieruchomości powyżej progu 1 200 m² powierzchni użytkowej. W praktyce oznacza to, że mieszkańcy osiedli miejskich i osób zamieszkujących w budynkach wielorodzinnych mają schron w tym samym budynku lub w sąsiednim. Jednocześnie system fiński explicite rezygnuje z norm wiejskich: dla obszarów słabo zaludnionych, zabudowy jednorodzinnej nie przewidziano schronów, a mieszkańcom zalecane jest szukanie ochrony w najbardziej trwałych częściach budynku lub ewakuacji[157]. Wyniki badań przestrzennych wskazują, że mimo braku normy metrycznej pokrycie populacji fińskiej wynosi ok. 87%, przy czym w Helsinkach odsetek ten przekracza 100% dzięki stacjom metra zaadaptowanym na potrzeby ochrony ludności[158]. Szwajcaria osiągnęła ponad 110% pokrycia inną drogą. Federalna Ustawa o Ochronie Ludności i Obronie Cywilnej stanowi, że każda mieszkanka i każdy mieszkaniec ma mieć pełnowartościowe miejsce schronowe „w pobliżu miejsca zamieszkania". Zasadę tę realizuje się przez obowiązek budowy schronu prywatnego w każdym nowym budynku powyżej progu 38 izb mieszkalnych

oraz przez system gminnego przypisania (każda gmina opracowuje plan wskazujący, który schron służy danym mieszkańcom za schronienie w razie alarmu – plany te ujawniane są dopiero w sytuacji zagrożenia)[159]. Skuteczność tego systemu potwierdzają dane BABS: 9 milionów miejsc schronowych w ok. 370 000 schronach prywatnych i publicznych[160]. Szwecja przyjmuje zasadę otwartego dostępu bez przypisania: instruuje obywateli, że nie są przypisani do żadnego konkretnego schronu i powinni korzystać z najbliższego dostępnego. Podejście to zakłada wysoką świadomość obywatelską i infrastrukturę informacyjną (stale aktualizowana mapa schronów) zamiast administracyjnego przypisania[161]. Norma szwedzka nie określa odległości, a dostępność ok. 64 tys. schronów z orientacyjną liczbą 7 mln miejsc daje ponad 65% pokrycia społeczeństwa[162]. Najbardziej radykalny wariant podejścia lokalizacyjnego stosuje Izrael. System nie operuje normą odległości, lecz normą czasu: od chwili uruchomienia alarmu mieszkaniec musi dotrzeć do ochrony zanim nadleci rakieta. W obszarze położonym w sąsiedztwie Strefy Gazy czas ten wynosi 15 sekund, w rejonie Tel Awiwu – 90 sekund. Żadna sieć schrony publicznych nie jest w stanie zagwarantować dostępności w takim przedziale czasowym. Konsekwencją jest wprowadzenie w 1992 r. obowiązku mamad (merhav mugan dirati) – zabezpieczonego pokoju ochronnego w każdym nowym mieszkaniu[163]. Lekcja izraelska, również dla Polski, mogłaby być następująca: norma czasu dojścia powinna być pochodną parametru czasu ostrzegania dla danego regionu, a nie stałą wartością ogólnokrajową. Wschodnie powiaty Polski, położone w bezpośrednim sąsiedztwie granicy, wymagają surowszego reżimu dostępności niż aglomeracje centralne.

Tabela 6. Podejścia do normy dostępności

Państwo	Norma dostępności	Pokrycie populacji	Obszary wiejskie
Polska	500 m (miasto) / 1000 m (poza miastem)	~4% (stan 2024); cel: 50% miast / 25% wsi	MDS + ewakuacja
Finlandia	brak normy metrycznej; schron przy każdym budynku ≥1 200 m²	~87% (4,8 mln miejsc)	Brak schronów; ewakuacja
Szwajcaria	„w pobliżu miejsca zamieszkania”	>100% (9 mln miejsc)	Schrony lokalne, opłata zastępcza
Szwecja	Brak normy; „najbliższy dostępny”	~67% (7 mln miejsc)	Brak celów wiejskich
Izrael	norma czasu, nie odległości	>90% (mamad/miklat)	Mamad w każdym budynku

Źródło: opracowanie własne na podstawie danych rządowych.

Tabela obok zestawia porównawczo podejścia do normy dostępności w pięciu państwach.

6.7 Model dual-use – wykorzystanie w czasie pokoju

Każda instalacja infrastrukturalna ma dwie główne składowe kosztu: koszty kapitałowe – capex, czyli nakład początkowy na budowę, oraz koszty operacyjne – opex, czyli koszt ciągłej eksploatacji i utrzymania. Tradycyjny model schronu jako obiektu „dostępnego tylko w razie alarmu” powoduje, że opex jest czystym wydatkiem bez żadnego przychodu kompensacyjnego: schron zużywa prąd na klimatyzację, wymaga przeglądów, napraw, ochrony przed wilgocią i weryfikacji sprzętu, a przez 99,9% czasu stoi pusty. Ten model jest ekonomicznie nietrwały na dłuższą metę, dowodem jest przywoływany już raport NIK z 2024 r., który stwierdził, że brak użytkowania cywilnego był jednym z głównych czynników prowadzących do degradacji technicznej polskich schronów.

Ustawa o ochronie ludności i obronie cywilnej posługuje się w art. 92 ust. 5 pojęciem „obiektów o podwójnej funkcji” (obiektów dual-use), nie definiując przedmiotowego terminu. Tym samym, mając na względzie, że zarówno ustawa, jak i inne przepisy krajowe nie zawierają definicji legalnej „dual-use”, zasadne jest odwołanie się do ustawodawstwa unijnego, w tym do Rozporządzenia 2021/821, na podstawie którego można wyinterpretować, że „dual-use” to standard technologiczny i prawny określający produkty, usługi i wiedzę, które dzięki swojej

innowacyjności i wszechstronności służą zarówno rozwojowi gospodarki cywilnej, jak i wzmocnieniu bezpieczeństwa państwa. Choć Rozporządzenie 2021/821 nie odnosi się bezpośrednio do infrastruktury budowlanej, wyraża ono istotę pojęcia „dual-use", polegającą na tym, że ten sam zasób może służyć jednocześnie celom cywilnym i obronnym. Przeniesienie powyższego na grunt budownictwa ochronnego oznacza, że obiekt o podwójnej funkcji pełni na co dzień swoją funkcję użytkową, a w razie zagrożenia zostaje przekształcony tak, aby mógł pełnić funkcję ochronną.

Nie przesądzając, jakie funkcje użytkowe mogą być łączone z funkcją ochronną, polski ustawodawca nie wprowadził żadnych ograniczeń co do przeznaczenia obiektów o podwójnej funkcji. W modelu dual-use może być zatem zrealizowany zarówno obiekt oświatowy, jak i sportowy, kulturalny, medyczny czy administracyjny. O tym, czy budowa lub modernizacja danego obiektu wpisuje się w model dual-use, decydują wyłącznie potrzeby organów ochrony ludności (w szczególności władz samorządowych) oraz możliwości projektowe przewidziane dla konkretnej inwestycji, przede wszystkim warunki techniczne dotyczące projektowania obiektów budowlanych, określone w przepisach wykonawczych.

Finlandia pokazuje, w jak bardzo dojrzałej formie idea ta może być zrealizowana. Całkowity koszt fińskiej infrastruktury schronowej szacuje się na ok. 4,4 mld EUR, lecz kluczowe jest to, że większość tej kwoty poniosły prywatne podmioty, nie budżet państwa. Mechanizm jest prosty: prawo budowlane nakłada obowiązek budowy schronu przy każdym nowym obiekcie powyżej 1 200 m^2 powierzchni, lecz jednocześnie zezwala na jego pełne użytkowanie komercyjne w czasie pokoju pod warunkiem przywrócenia do funkcji schronu w ciągu 72 godzin od ogłoszenia gotowości. Deweloper ma zatem motywację: schron przytępia koszty budowy, bo przestrzeń podziemna i tak często byłaby budowana jako garaż lub magazyn, a dodatkowy koszt wzmocnienia konstrukcji rozkłada się na dziesięciolecia eksploatacji. W tym sensie dual-use nie jest kompromisem między ochroną a komercją – jest rozwiązaniem, w którym jedno warunkuje i finansuje drugie[164].

Szwajcaria wypracowała równolegle mechanizm radzenia sobie z obiektami, które, z uwagi na małą powierzchnię lub specyficzne przeznaczenie, nie mogą budować schronu we własnym zakresie: jest nim Ersatzbeitrag, tj. opłata zastępcza wpłacana do gminnego funduszu budowy schronów publicznych. Stawka wynosi 1400 CHF na każde niewybudowane miejsce schronowe i zasila w całości pułap inwestycji w większe, wielofunkcyjne obiekty publiczne. Logika jest systemowa: zamiast obarczania każdego podmiotu trudnym do wypełnienia zobowiązaniem, opłata tworzy zasób finansowy pozwalający gminie budować schrony o większej skali i lepszych możliwościach komercyjnych. Dla polskiej praktyki ten model jest bezpośrednią inspiracją w projektowaniu systemu finansowania schronów w gminach wiejskich i małomiejskich[165].

Szacunki kosztów dla polskich warunków wskazują na znaczące różnice między kategoriami budowli ochronnych: miejsce w MDS (miejscu doraźnego schronienia, np. zaadaptowanej piwnicy) kosztuje maks. ok. 2000 PLN, podczas gdy miejsce w schronie klasy S-1 to wydatek rzędu 10 000–15 000 PLN[166]. Przy założeniu, że Polska potrzebuje ok. 7–9 mln nowych miejsc schronowych, by osiągnąć docelowe pokrycie 50% ludności miejskiej, łączny CAPEX waha się od ok. 20 do nawet powyżej 100 mld PLN – bez dual-use. Model dual-use obniża efektywny koszt netto dla budżetu publicznego, bo część nakładu jest pokrywana przez przychody z eksploatacji lub przez inwestorów prywatnych budujących przestrzeń komercyjną, która zarazem pełni funkcję schronu.

Zasadność ekonomiczna wdrażania koncepcji podwójnego zastosowania (dual-use) w architekturze schronowej znajduje jednoznaczne potwierdzenie w analizie nakładów inwestycyjnych (CAPEX). Adaptacja infrastruktury użyteczności publicznej – na przykład poprzez lokalizację schronów pod obiektami sportowymi (boiskami) czy parkingami podziemnymi, pozwala zredukować jednostkowy wydatek inwestycyjny do poziomu około 16 000 PLN w przeliczeniu na miejsce schronowe. Z kolei w tradycyjnym modelu budowy dedykowanych schronów wolnostojących, całkowity koszt utworzenia jednego miejsca waha się w przedziale od 20 000 PLN do nawet 30 000 PLN. Wynika z tego, że podejście dual-use generuje oszczędności kapitałowe rzędu 20–45% na każdym wybudowanym miejscu, znacząco obniżając również późniejsze koszty operacyjne (OPEX) dzięki komercyjnej lub społecznej eksploatacji obiektu w czasie pokoju. Biorąc pod uwagę zapotrzebowanie rzędu kilku milionów miejsc,

zintegrowane projektowanie infrastruktury staje się kluczowym mechanizmem optymalizacji wydatków publicznych w ramach funduszu 1,5% PKB.

Najłatwiej adaptowaną kategorią dual-use są piwnice budynków mieszkalnych. Ustawa o ochronie ludności i obronie cywilnej z 5 grudnia 2024 r. nakazuje, by nowe budynki wielorodzinne i obiekty użyteczności publicznej były projektowane w sposób umożliwiający organizację MDS, a kondygnacje podziemne i garaże, dostosowane do tej funkcji w momencie składania wniosku o pozwolenie na budowę po 31 grudnia 2025 r.

Wymagania adaptacyjne są relatywnie skromne w porównaniu z wymogami pełnoprawnego schronu: MDS musi zapewnić minimalną powierzchnię 1,5 m² na osobę, wysokość co najmniej 2 m, wentylację gwarantującą odpowiednią zawartość tlenu przez 48 godzin, dwie drogi ewakuacji oraz oznakowanie międzynarodowym znakiem ochrony cywilnej. Standardowe wyposażenie techniczne garażu: wentylacja mechaniczna, oświetlenie awaryjne, hydranty pożarowe, po uzupełnieniu o awaryjny generator i zabezpieczenia drzwi wejściowych tworzy fundament MDS za stosunkowo niską cenę dodatkową[167].

Szczególną rolę odgrywa w tym kontekście sieć metra. Doświadczenia ukraińskie z 2022 r. pokazały, że stacje metra kijowskiego są jedynymi obiektami w przestrzeni miejskiej zdolnymi do absorpcji dziesiątek tysięcy mieszkańców jednocześnie: głęboko pod ziemią, z niezależną wentylacją i zasilaniem, z infrastrukturą sanitarną i łącznością[168]. Helsinki realizowało ten model przez dekady: stacje i tunele metra helsińskiego są formalnie sklasyfikowane jako schrony skalne klasy K i ujęte w planowaniu schronowym aglomeracji[169]. Podobnie działają podziemne hale sportowe i baseny, zintegrowane z tunelami miejskimi – Itäkeskus Swimming Hall (1995) pełni funkcję schronu dla 6 200 osób przy jednoczesnym użytkowaniu jako popularny obiekt rekreacyjny. Warszawskie metro I i II linii, chociaż zaprojektowane w czasach kiedy wymagania schronowe nie były priorytetem, ma jedynie potencjał do certyfikacji części przyszłych stacji jako MDS, tym bardziej że polska ustawa o ochronie ludności wprost wskazuje stacje metra i tunele kolejowe jako wymagające odrębnych wymogów schronowych.

Fiński model dual-use sięga dalej niż garaże: obejmuje pełną integrację funkcji schronowej z obiektami kulturalnymi i sportowymi na poziomie prawa budowlanego i planowania przestrzennego. Podziemne centrum Merihaka w Helsinkach było od początku projektowane jako schron skalny klasy K, a komercyjne użytkowanie jest sposobem jego finansowania i utrzymania. Kluczem do tego modelu jest zasada: funkcja ochronna jest „pierwotną" definicją obiektu; funkcja komercyjna jest wtórna i obniża koszt netto ochrony[170].

Szwajcarskie wielkie schrony publiczne (Grossschutzanlagen) stosują analogiczną logikę. Schrony regionalne w Zurichu, Berna i Genewie pełnią na co dzień funkcje sal konferencyjnych, archiwów kantonalnych, centrum logistycznego lub magazynu komunalnego; niektóre są udostępniane jako przestrzenie wystawiennicze. Warunkiem jest gotowość do pełnego przejścia na funkcję schronu w ciągu pięciu dni, co oznacza m.in. usunięcie wyposażenia tymczasowego, rozmieszczenie łóżek piętrowych i aktywację systemu filtracji. System szwajcarski prowadzi coroczne ćwiczenia gotowości, w trakcie których właściciele schronów mają obowiązek udowodnienia, że dual-use nie zdegradował gotowości operacyjnej, i opłacają kary za nieprzestrzeganie tego wymogu[171].

Izraelski system dual-use przyjmuje odmiennie skalowany kształt: mamam (merkhav mugan mosadi, przestrzeń ochronna obiektu użyteczności publicznej) jest obowiązkowym elementem każdego centrum handlowego, szkoły, biurowca i obiektu sportowego. W czasie pokoju mamam pełni funkcję sali zebrań, magazynu, punktu pierwszej pomocy lub sali konferencyjnej. Wymogi techniczne (beton zbrojony o odpowiedniej grubości, drzwi hermetyczne, wentylacja NBC) są zapisane w prawie budowlanym i sprawdzane przy każdym odbiorze. Izraelski model jest najdalej idącą egzemplifikacją tezy, że dual-use może stać się normą architektoniczną, a nie wyjątkiem[172].

Dla polskiego kontekstu kluczową implikacją jest pytanie o akceptację społeczną. Badania prowadzone w Finlandii i Szwecji konsekwentnie pokazują, że wysoki poziom społecznego poparcia dla systemów schronowych jest bezpośrednio związany z ich widocznością i użytecznością w czasie pokoju: Finowie pływają w schronach, ćwiczą w schronach, chodzą do pracy przez tunele. Schron jest dla nich nie abstrakcją „dystopijnego państwa", lecz częścią życia codziennego.

W Polsce, gdzie schrony przez trzydzieści lat były porzucone i zdegradowane, odbudowa zaufania społecznego wymaga właśnie tej widoczności. Inwestycja w dual-use jest zatem nie tylko ekonomiczną racjonalizacją wydatku, lecz także strategiczną komunikacją: „ta infrastruktura służy Wam na co dzień".

Trzecim filarem modelu dual-use są magazyny komunalne i strategiczne rezerwy materiałowe. Logika jest zbieżna z poprzednimi kategoriami: przestrzeń podziemna, która i tak byłaby wykorzystana do składowania, może być przy stosunkowo małych nakładach dodatkowych, przygotowana do przyjęcia ludności cywilnej w warunkach kryzysu. Finlandia jest pod tym względem wzorcem: Urząd ds. Zaopatrzenia Awaryjnego (Huoltovarmuuskeskus, NESA) zarządza rezerwami strategicznymi: lekami, surowcami energetycznymi, żywnością i sprzętem medycznym, w sieci podziemnych magazynów rozmieszczonych w całym kraju, częściowo w tych samych schronach skalnych, które pełnią funkcję ochrony ludności. Rezerwy te są szacowane przez ekspertów na poziomie 3–6 miesięcy zużycia krajowego, choć szczegółowe dane są objęte tajemnicą państwową[173]. Polska dysponuje Rządową Agencją Rezerw Strategicznych (RARS) jako instytucją odpowiedzialną za rezerwy państwowe. Ustawa z 17 grudnia 2021 r. o rezerwach strategicznych definiuje kategorie objęte obowiązkiem magazynowania (ropa naftowa, gaz ziemny, paliwa płynne, żywność, leki, wyroby medyczne) i ustanawia RARS jako gestora tych rezerw. Istotna luka systemowa polega na tym, że infrastruktura magazynowa RARS i sieć budowli ochronnych funkcjonują do tej pory jako dwa odrębne systemy, bez formalnego powiązania. Zasada dual-use nakazuje tę synergię, lokalizacja magazynów rezerw strategicznych powinna być koordynowana z planami sieci schronów, tak by przynajmniej część rezerw żywnościowych i medycznych była składowana w obiektach posiadających zdolność ochrony ludności. Osiągnięcie tego celu wymaga zmiany ustawy o rezerwach strategicznych lub wydania rozporządzenia koordynacyjnego między MSWiA a Ministerstwem Aktywów Państwowych.

Przestrzeń o funkcji ochronnej najlepiej służy wtedy, gdy pracuje na co dzień, a w sytuacji zagrożenia przechodzi w tryb operacyjny. To zasada łącząca oś odpornościową raportu z gospodarnym zarządzaniem majątkiem. Efektywność dual-use wynika nie z pojedynczych realizacji, lecz ze skali i powtarzalności. Model działa najpełniej, gdy obejmuje portfele aktywów i całe segmenty rynku. W praktyce rozkłada się on na dwie ścieżki o odmiennych ryzykach i kosztach, a ich świadome rozróżnienie ułatwia trafne decyzje.

Najtańszym momentem na wbudowanie funkcji ochronnej i konwertowalności jest etap projektowy. Pomocne jest oddzielne policzenie kosztu samej konwertowalności od kosztu budowy podstawowej, pozwala to decydentowi dostrzec rzeczywistą, niewielką cenę odporności, zamiast łączyć ją z kosztem całej inwestycji. Wzorcowy jest model fiński, oparty na koncepcji bezpieczeństwa zintegrowanego i powszechnych schronach: deweloper ponosi rzędu 2% kosztu budowy, przestrzeń ochronna w czasie pokoju służy jako parking lub magazyn, a gotowość do konwersji wynosi ok. 72 godzin, bez bezpośredniej dotacji. Co istotne, to realne schrony, a nie minimum doraźne: dowód, że powszechność i wysoką klasę ochrony da się pogodzić, gdy koszt jednostkowy jest niski, a przestrzeń użytkowana codziennie. Zauważalnym zjawiskiem stają się rynkowe oczekiwania wobec przestrzeni komercyjnych w zakresie przystosowania ich do funkcji ochronnych. Integracja tych potrzeb z codziennym użytkowaniem pozwala na optymalizację kosztów jednostkowych, co weryfikują rozwiązania z innych systemów prawnych, takie jak izraelski mamad czy singapurski Civil Defence Shelter Act.

Ten sam zestaw kompetencji: ocena techniczna, kosztorys, przegląd zasobu, można skierować na istniejący majątek państwa i samorządów. Różnica wobec ścieżki pierwszej jest jakościowa: nie projektujemy konwertowalności od zera, lecz odzyskujemy i przekwalifikujemy to, co już istnieje. Szczególnie obiecujące są nieruchomości doskonale zlokalizowane, a wykorzystywane poniżej potencjału: naziemne parkingi w centrach miast, place składowe, nieczynne działki przy węzłach komunikacyjnych. Najrzadszym zasobem miasta nie jest grunt jako taki, lecz dobra lokalizacja, a tu można ją uwolnić: uporządkowanie i zagęszczenie funkcji tworzy wartość, z której da się sfinansować wbudowaną warstwę odpornościową. Uruchomienie tej ścieżki nie wymaga zmian własnościowych, lecz uporządkowanego procesu: inwentaryzacji i wyceny zasobu, oceny technicznej, wyboru modelu zarządczego, i dopiero wówczas wejścia kapitału. Kolejność ma znaczenie. Rzetelna mapa i metodyka czynią każdą transakcję powtarzalną i szybką, zamiast negocjowanej od zera. We wszystkich modelach

kontrola nad standardami bezpieczeństwa, dostępem i przeznaczeniem pozostaje po stronie publicznej: kapitał prywatny wchodzi w rolę właściciela finansowego i wykonawcy, a gospodarzem misji pozostaje państwo.

Przełożenie wniosków analitycznych na praktyczny program wdrożeniowy opiera się na pięciu kluczowych kierunkach, z których trzy mają charakter ściśle regulacyjny i nie generują bezpośrednich obciążeń dla budżetu państwa. Fundamentalnym krokiem, warunkującym skuteczność pozostałych działań, jest formalne zdefiniowanie infrastruktury podwójnego zastosowania (dual-use) jako odrębnej klasy aktywów inwestycyjnych, co otworzy sektorowi obronnemu dostęp do kapitału instytucjonalnego oraz rynków ubezpieczeniowych. Stanowi to podstawę do szerokiego rozwinięcia projektów w formule partnerstwa publiczno-prywatnego (PPP), obejmujących między innymi mieszkalnictwo wojskowe, infrastrukturę logistyczną oraz zarządzanie bazami, co pozwoli na efektywny transfer kompetencji i wykorzystanie dźwigni kapitału prywatnego. Równolegle niezbędne jest wprowadzenie stabilnego mechanizmu premiującego utrzymywaną klasę ochrony obiektów – zaprojektowanego na wzór płatności za moc rezerwową w sektorze energetycznym, jako istotnego uzupełnienia wsparcia z art. 106 ustawy o ochronie ludności i obronie cywilnej. Działania te muszą zostać wsparte programem profesjonalizacji zarządzania majątkiem publicznym, polegającym na przejściu do logiki portfelowej przy bezwzględnym zachowaniu własności i pełnej kontroli państwa, a także wdrożeniem szybkich i przewidywalnych ścieżek administracyjnych, zapewniających priorytetowe traktowanie projektów dual-use w procedurach budowlanych i planowaniu przestrzennym. Operacyjne uruchomienie tak zaprojektowanego modelu wymaga jednak podjęcia trzech rozstrzygających decyzji kierunkowych: zdefiniowania docelowego tempa budowy dojrzałego rynku (w perspektywie kilku lub kilkunastu lat), wypracowania precyzyjnego modelu współpracy z sektorem prywatnym, który skutecznie połączy rynkową efektywność z nadzorem publicznym, oraz wytypowania obszaru pierwszego projektu pilotażowego wraz z jednoznacznym wskazaniem jego gospodarza po stronie administracji państwowej.

Finansowanie programu dual-use wymaga kombinacji co najmniej trzech mechanizmów. Pierwszym jest obowiązek ustawowy, analogicznie do fińskiego modelu obowiązku budowlanego i szwajcarskiego modelu opłaty zastępczej: każda nowa inwestycja deweloperska powyżej progu powierzchniowego powinna być zobowiązana do zapewnienia schronu lub wpłaty opłaty zastępczej do gminnego funduszu schronowego. Polskie prawo budowlane stwarza ramy dla takiego rozwiązania, które wymaga jednak wdrożenia na poziomie rozporządzeń technicznych.

Drugim mechanizmem jest partnerstwo publiczno-prywatne. Polska posiada ustawę o PPP z 2008 r. i doświadczenia z infrastrukturą podziemną, lecz dotychczas model ten nie był stosowany dla schronów. Dual-use tworzy naturalne przesłanki dla PPP: podmiot prywatny finansuje i eksploatuje część komercyjną (garaż, siłownia, centrum handlowe), państwo lub samorząd ponosi dodatkowy koszt wzmocnień schronowych i kompensuje podmiotowi prywatnemu ograniczenia wynikające z konieczności zachowania gotowości operacyjnej. Model ten wymaga precyzyjnej wyceny kosztu dodatkowego schronu względem standardowej inwestycji i czytelnego mechanizmu kompensacyjnego, co jest zadaniem dla przyszłej regulacji. Kwalifikowalność tej części wydatku do kategorii 1,5% PKB NATO wymaga transparentnego klucza podziału: część komercyjna nie kwalifikuje się, część stricte schronowa – tak[174].

Trzecim mechanizmem są fundusze europejskie. Infrastruktura dual-use mogłaby stworzyć warunki do kumulowania źródeł finansowania z kilku instrumentów jednocześnie: Europejski Fundusz Obronny (B+R dla technologii budowli ochronnych), fundusze spójności EFRR 2021–2027 (infrastruktura odporna na zmiany klimatu i katastrofy), Program Horyzont Europa (klaster Civil Security for Society), a także rescEU jako mechanizm wspólnych rezerw zasobów ratowniczych. Polska powinna aktywnie lobbować za włączeniem infrastruktury schronowej dual-use do katalogu wydatków kwalifikowanych Funduszu Spójności w perspektywie 2028–2034, co wymagałoby zmiany rozporządzenia EFRR, ale jest ścieżką realistyczną w świetle kierunku wyznaczonego przez Strategię Gotowości UE z 2025 r. Z perspektywy NATO, model dual-use, przez obniżenie kosztu netto schronu poniesionego przez budżet publiczny, pozwala jednocześnie wykazywać większy nominalny wydatek kwalifikowany do 1,5% PKB, zachowując dyscyplinę fiskalną i maksymalizując efekt odpornościowy z każdej wydanej złotówki.

6.8 Cyfrowa paszportyzacja i monitoring gotowości obiektów ochrony ludności

Budowa i modernizacja infrastruktury ochronnej powinna zostać uzupełniona o cyfrową warstwę gotowości obiektów ochrony ludności. Warstwa ta obejmuje cyfrowe paszporty obiektów, aktualizację danych o ich stanie, monitorowanie podstawowych parametrów technicznych i środowiskowych oraz raportowanie statusu gotowości do właściwych struktur zarządzania kryzysowego.

Minimalny zakres takiego rozwiązania powinien obejmować informacje o lokalizacji, pojemności, funkcji obiektu, administratorze, dostępności wejść, stanie zasilania, dostępie do wody, ogrzewania lub chłodzenia, wentylacji, łączności, ograniczeniach użytkowania oraz dacie ostatniej weryfikacji. W przypadku obiektów wykorzystywanych w modelu dual-use szczególne znaczenie ma możliwość szybkiego potwierdzenia, czy obiekt może zostać przełączony z funkcji pokojowej do funkcji ochronnej.

Celem cyfrowej paszportyzacji i monitoringu nie jest zastąpienie inwestycji budowlanych, lecz zapewnienie, że finansowane obiekty pozostają realnie dostępne, sprawne i możliwe do użycia w sytuacji kryzysowej.

6.9 Obiekty czasowego zakwaterowania ewakuowanej ludności

System ochrony ludności powinien obejmować nie tylko schrony, ukrycia i miejsca doraźnego schronienia, lecz także obiekty czasowego pobytu oraz zakwaterowania ewakuowanej ludności. W praktyce mogą to być szkoły, hale sportowe, internaty, akademiki, remizy, obiekty administracyjne, komunalne, sportowe i inne budynki publiczne lub prywatne wskazane w planach ewakuacji.

Gotowość takich obiektów nie powinna być oceniana wyłącznie przez liczbę dostępnych miejsc. Kluczowe znaczenie mają dostęp do energii, wody, sanitariatów, ogrzewania lub chłodzenia, wentylacji, łączności, bezpieczeństwa, zaplecza logistycznego oraz możliwość utrzymania akceptowalnych warunków środowiskowych po przyjęciu ludzi. Wydatki na przygotowanie, wyposażenie, paszportyzację i monitorowanie takich obiektów powinny być traktowane jako część infrastruktury odpornościowej państwa.

6.10 Inwestycje ochronne a prawo zamówień publicznych

Omówienia wymaga również kwestia reżimu prawnego, w jakim realizowana będzie budowa i modernizacja budowli ochronnych z uwzględnieniem modelu dual-use. Co do zasady, zamówienie na roboty budowlane, obejmujące budowę lub modernizację obiektu budowlanego, realizowane są w reżimie zamówień publicznych, jeżeli udzielane są przez zamawiającego w rozumieniu ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.

W drodze nowelizacji ustawy o ochronie ludności i obronie cywilnej z 2026 r. ustawodawca wprowadził wyjątek od tej reguły, przewidując art. 157a ustawy. Analiza przedmiotowego przepisu prowadzi do wniosku, że wyłączenie spod reżimu prawa zamówień publicznych obejmuje zamówienia, które spełniają łącznie trzy przesłanki: (i) służą bezpośrednio realizacji zadań ochrony ludności i obrony cywilnej, (ii) przynależą do skonkretyzowanej grupy zamówień obejmujących infrastrukturę zapewniającą schronienie w budowlach ochronnych, systemy łączności, teleinformatyki oraz wykrywania zagrożeń, powiadamiania i alarmowania, a także infrastrukturę medyczną o podwójnym przeznaczeniu, oraz (iii) są finansowane lub dofinansowane w ramach limitu wydatków na potrzeby obronne, zgodnie z ustawą z dnia 11 marca 2022 r. o obronie Ojczyzny, w wysokości 0,15% produktu krajowego brutto.

Tym samym, brak jest ustawowych przesłanek do wyłączenia z reżimu prawa zamówień publicznych budowli ochronnych realizowanych z zastosowaniem modelu dual-use w rozumieniu art. 92 ust. 5 ustawy o ochronie ludności i obronie cywilnej. Oznacza to, że udzielając zamówienia na roboty budowlane polegające na budowie lub modernizacji obiektu o podwójnej funkcji, zamawiający zobligowany jest do zastosowania przepisów ustawy Prawo zamówień publicznych. Gdy jednak roboty budowlane obejmują budowę lub modernizację obiektu pełniącego wyłącznie funkcję ochronną, zamawiający nie udziela zamówienia w reżimie prawa zamówień publicznych.

Stosowanie przepisów ustawy Prawo zamówień publicznych gwarantuje zachowanie zasad uczciwej konkurencji i równego traktowania wykonawców – zarówno krajowych, jak i zagranicznych, w tym podmiotów z państw trzecich, z którymi Unia Europejska zawarła umowę o dostępie do rynku zamówień publicznych na zasadzie wzajemności i równości, w szczególności w ramach Porozumienia WTO w sprawie zamówień rządowych (GPA). W szerszej perspektywie objęcie budowli ochronnych reżimem prawa zamówień publicznych może przyczynić się do ukształtowania zupełnie nowego, konkurencyjnego segmentu rynku budowlanego w Polsce – potencjalnie atrakcyjnego dla szerokiego kręgu przedsiębiorców działających w tej branży.

7 Architektura bezpieczeństwa infrastruktury krytycznej i cyberprzestrzeni

7.1 Ochrona infrastruktury krytycznej – ramy prawne

7.1.1. Nowelizacja ustawy o zarządzaniu kryzysowym z 2026 roku

W warunkach rosnącego zagrożenia atakami hybrydowymi, sabotażem oraz działaniami skierowanymi przeciwko infrastrukturze państw NATO i Unii Europejskiej, zagadnienie ochrony infrastruktury krytycznej zyskało w Polsce wyraźnie na znaczeniu regulacyjnym i operacyjnym. Do czasu wejścia w życie nowelizacji z 2026 r. podstawę prawną ochrony infrastruktury krytycznej w Polsce stanowiła ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Ustawa ta nakładała na właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji oraz urządzeń infrastruktury krytycznej, obowiązek przygotowywania i wdrażania planów ochrony oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymanie funkcjonowania tej infrastruktury do czasu jej pełnego odtworzenia. Centralnym instrumentem programowym był Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), uchwalany przez Radę Ministrów w drodze uchwały. Koordynację na poziomie ogólnokrajowym sprawował dyrektor Rządowego Centrum Bezpieczeństwa (RCB). System ten, zaprojektowany w realiach 2007 r., nie uwzględniał w pełni ani skali zagrożeń hybrydowych, ani obowiązków wynikających z prawa unijnego.

29 maja 2026 r. Sejm RP uchwalił, uwzględniając poprawki Senatu, ustawę o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw. Zasadniczym jej celem jest implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych (dyrektywa CER – Critical Entities Resilience). Reforma ta wpisuje się jednocześnie w szerszy kontekst unijny: dyrektywa CER jest systemowo powiązana z dyrektywą NIS2 (2022/2555), której polskie wdrożenie realizuje nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC). Oba akty unijne dotyczą tych samych podmiotów i tworzą komplementarne reżimy – CER koncentruje się na odporności fizycznej i organizacyjnej, NIS2 na cyberbezpieczeństwie.

Ustawa z 29 maja 2026 r. dokonuje zasadniczego przesunięcia paradygmatu: od reaktywnej ochrony wybranych obiektów i instalacji do systemowego budowania odporności podmiotów świadczących usługi kluczowe. Zmiana ta ma kilka istotnych wymiarów.

Po pierwsze, znacznie poszerza katalog sektorów i podmiotów objętych regulacją, włączając dotychczas nieuregulowane obszary takie jak przestrzeń kosmiczna, administracja publiczna, gospodarka odpadami czy infrastruktura cyfrowa, a zarazem obejmuje ochroną etap inwestycyjny.

Po drugie, wprowadza dwustopniowy system identyfikacji i zróżnicowanych obowiązków: lżejszy reżim dla operatorów infrastruktury krytycznej i bardziej wymagający dla podmiotów krytycznych świadczących usługi kluczowe. Tworzy tym samym przestrzeń do proporcjonalnego stosowania przepisów bez nakładania jednolitych, nadmiernych obciążeń na wszystkich uczestników systemu.

Po trzecie, ustawa integruje w jednym akcie regulacje dotyczące odporności fizycznej i organizacyjnej z obowiązkami cyberbezpieczeństwa, zobowiązując podmioty krytyczne będące jednocześnie podmiotami kluczowymi w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa (KSC) do integracji odpowiedniej dokumentacji. Zapewnia tym samym spójność z wdrożeniem dyrektywy NIS2 w polskim porządku prawnym.

7.1.2. Dwa poziomy regulacji infrastruktury krytycznej

Kluczowe dla zrozumienia nowych przepisów jest rozróżnienie między dwoma kategoriami podmiotów, które odpowiada dwupoziomowej strukturze regulacji. Na poziomie ogólnym ustawa obejmuje wszystkich operatorów infrastruktury krytycznej ujętych w Narodowym Planie Ochrony Infrastruktury Krytycznej. Na poziomie szczegółowym wyodrębnia spośród nich węższą kategorię podmiotów krytycznych, wpisanych do odrębnego, niepublicznego wykazu prowadzonego przez właściwy organ. Logika tego podziału jest funkcjonalna: im bardziej zakłócenie działania danego podmiotu dotknęłoby ciągłość usług kluczowych, tym szerszy katalog obowiązków mu się przypisuje. Oba poziomy współistnieją – wpis do wykazu podmiotów krytycznych nie zwalnia z obowiązków wynikających ze statusu operatora infrastruktury krytycznej, lecz je uzupełnia.

Infrastruktura krytyczna zdefiniowana jest w ustawie jako obiekt, urządzenie, instalacja, sieć, system lub usługa – albo połączone ze sobą funkcjonalnie takie elementy – niezbędne do realizacji ważnych interesów państwa, zapewnienia funkcjonowania przedsiębiorstw, zaspokajania potrzeb obywateli oraz świadczenia usług kluczowych. Definicja jest szersza niż ta zawarta w poprzednim akcie prawnym: istotnym novum jest wyraźne powiązanie infrastruktury krytycznej z wymiarem świadczenia usług kluczowych, co rozszerza zakres regulacji na podmioty, które wcześniej mogły nie być identyfikowane jako operatorzy IK. Usługa kluczowa to usługa o istotnym znaczeniu dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony lub dobrobytu gospodarczego lub społecznego ludności, wskazana w przepisach wykonawczych do ustawy lub w decyzji właściwego organu. Powiązanie pojęcia infrastruktury krytycznej z pojęciem usługi kluczowej powoduje, że o kwalifikacji danego składnika majątkowego przesądza nie tyle jego fizyczny charakter, co funkcja, jaką pełni w łańcuchu świadczenia usługi.

Podmiot krytyczny to operator infrastruktury krytycznej wpisany do odrębnego wykazu podmiotów krytycznych. Wpis następuje w drodze decyzji właściwego organu, gdy operator prowadzi działalność w jednym z sektorów objętych ustawą, świadczy co najmniej jedną usługę kluczową, posiada infrastrukturę krytyczną na terytorium RP lub na polskich obszarach morskich, a potencjalny incydent dotykający tej infrastruktury miałby istotny skutek zakłócający dla świadczenia usługi kluczowej. Ocena istotności skutku zakłócającego uwzględnia m.in. liczbę użytkowników zależnych od usługi, jej geograficzny zasięg, znaczenie dla innych sektorów, straty gospodarcze, skutki społeczne oraz czas przywrócenia normalnego funkcjonowania. Wykaz podmiotów krytycznych jest dokumentem niejawnym. Na podmiotach krytycznych ciążą obowiązki znacznie szersze niż na pozostałych operatorach. Obejmują one w szczególności: przeprowadzenie oceny ryzyka uwzględniającej zagrożenia naturalne, technologiczne, terrorystyczne i hybrydowe; opracowanie i wdrożenie planu odporności zawierającego techniczne, organizacyjne i kadrowe środki ochrony;

zapewnienie ciągłości działania i gotowości do odtworzenia świadczenia usługi kluczowej; zgłaszanie incydentów mających istotny wpływ na świadczenie usługi kluczowej do właściwego organu w określonym terminie; prowadzenie weryfikacji pracowników i współpracowników mających dostęp do infrastruktury krytycznej; wyznaczenie punktu kontaktowego do komunikacji z organami. Podmioty krytyczne podlegają inspekcjom i kontrolom właściwych organów; za naruszenie obowiązków grożą administracyjne kary pieniężne.

Ustawa wprowadza również nową kategorię potencjalnej infrastruktury krytycznej, obejmującej obiekty, urządzenia, instalacje, sieci, systemy lub usługi na etapie projektowania lub budowy, które po zakończeniu inwestycji mogą spełniać kryteria kwalifikacji infrastruktury krytycznej. Objęcie regulacją etapu inwestycyjnego jest nowością w polskim porządku prawnym – dotychczasowe przepisy przewidywały obowiązki wyłącznie w odniesieniu do infrastruktury już funkcjonującej.

Ratio legis tej kategorii jest systemowe: wczesna identyfikacja obiektów o potencjalnym znaczeniu krytycznym pozwala na uwzględnienie wymogów bezpieczeństwa już na etapie projektowania, zanim powstaną kosztowne do zmiany rozwiązania architektoniczne czy technologiczne. Ustawa nakłada na inwestorów lub podmioty realizujące inwestycje w sektorach objętych ustawą obowiązek notyfikacji właściwego organu o zamiarze realizacji inwestycji mogącej spełnić kryteria kwalifikacji. Organ dokonuje wstępnej oceny, czy planowana inwestycja wpisuje się w definicję potencjalnej infrastruktury krytycznej i może w drodze decyzji nałożyć na inwestora określone wymagania dotyczące projektowania, wyboru technologii lub środków ochrony fizycznej. Wymagania te uwzględnia się następnie w dokumentacji projektowej i decyzjach administracyjnych wydawanych w toku procesu inwestycyjno-budowlanego.

Status potencjalnej infrastruktury krytycznej wygasa z chwilą oddania obiektu do użytkowania i dokonania właściwej kwalifikacji – obiekt albo uzyskuje status infrastruktury krytycznej i jest ujmowany w Narodowym Planie Ochrony Infrastruktury Krytycznej, albo zostaje wyłączony z regulacji. W razie zasadniczej zmiany zakresu lub charakteru inwestycji w toku jej realizacji inwestor jest obowiązany ponownie zawiadomić właściwy organ. Ustawa przewiduje ponadto mechanizm współpracy organu z inwestorem na etapie projektowania w formie konsultacji, co pozwala na wczesne uzgodnienie wymogów bezpieczeństwa bez blokowania procesu inwestycyjnego.

Praktyczne znaczenie nowej kategorii jest szczególnie istotne w przypadku wielkoskalowych projektów infrastrukturalnych – terminali LNG, gazociągów, farm wiatrowych na morzu, węzłów telekomunikacyjnych czy centrów przetwarzania danych – których kwalifikacja jako infrastruktury krytycznej po zakończeniu budowy byłaby oczywista, a których projektowanie bez uwzględnienia wymogów bezpieczeństwa generowałoby konieczność późniejszych, kosztownych adaptacji.

7.1.3. Zakres sektorowy

Ustawa określa w załączniku sektory, podsektory i kategorie podmiotów stanowiące punkt odniesienia dla identyfikacji zarówno infrastruktury krytycznej, jak i podmiotów krytycznych. Należą do nich:

1. energia (wydobywanie kopalin, energia elektryczna, ciepło, ropa i paliwa, gaz, wodór, energetyka jądrowa);
2. transport (lotniczy, kolejowy, wodny, publiczny, drogowy);
3. bankowość i infrastruktura rynków finansowych;
4. ochrona zdrowia;
5. zaopatrzenie w wodę pitną i jej dystrybucja oraz zbiorowe odprowadzanie ścieków;
6. infrastruktura cyfrowa;
7. administracja publiczna (podmioty publiczne i finanse publiczne);
8. przestrzeń kosmiczna;
9. produkcja, przetwarzanie i dystrybucja żywności;
10. zarządzanie usługami ICT (Information and Communication Technology);
11. produkcja, wytwarzanie i dystrybucja chemikaliów;
12. usługi pocztowe;
13. gospodarowanie odpadami.

Katalog ten jest znacznie szerszy od dotychczas obowiązującego i odpowiada zakresowi dyrektywy CER, wypełniając tym samym wyraźną lukę w regulacji sektorów takich jak administracja publiczna, przestrzeń kosmiczna czy gospodarka odpadami.

7.1.4. Dokumenty strategiczne

Ustawa zastępuje Narodowy Program Ochrony Infrastruktury Krytycznej dwoma nowymi instrumentami strategicznymi przyjmowanymi przez Radę Ministrów w drodze uchwały.

1. Krajowa Ocena Ryzyka (KOR) zastępuje dotychczasowy raport o zagrożeniach bezpieczeństwa narodowego. Obejmuje zagrożenia naturalne, hybrydowe, z zakresu cyberbezpieczeństwa oraz terrorystyczne, a w odniesieniu do podmiotów krytycznych uwzględnia dodatkowo zagrożenia antagonistyczne, wzajemne zależności między sektorami i wpływ zakłóceń u podmiotów z innych państw UE. Ustawa definiuje zagrożenie antagonistyczne jako rodzaj zagrożenia hybrydowego ukierunkowanego celowo i świadomie przeciwko usługom kluczowym i infrastrukturze krytycznej, niezależnie od motywacji – definicja obejmuje zarówno działania terrorystyczne, jak i sabotaż wywołany przez podmioty państwowe lub parapaństwowe. KOR aktualizowana jest nie rzadziej niż raz na trzy lata; projekt opracowuje dyrektor RCB. Na podstawie KOR dyrektor RCB przekazuje Komisji Europejskiej streszczenie istotnych elementów oceny w terminie 3 miesięcy od dnia jej przyjęcia.
2. Krajowa Strategia Odporności Podmiotów Krytycznych (KSOPK) określa cele strategiczne i priorytety w zakresie niezakłóconego funkcjonowania infrastruktury krytycznej, zakresy działań dla organów administracji rządowej, metody identyfikacji podmiotów krytycznych oraz koordynację między organami właściwymi a organami odpowiedzialnymi za cyberbezpieczeństwo. Strategia przyjmowana jest co trzy lata i poddawana trzydziestodniowym konsultacjom publicznym przed przekazaniem Komisji Europejskiej.

7.1.5. Identyfikacja infrastruktury krytycznej i obowiązki operatorów

Centralnym rejestrem jest niejawny wykaz infrastruktury krytycznej prowadzony przez dyrektora RCB. Kryteria kwalifikacji określa Rada Ministrów w drodze uchwały (dokument niejawny). Ustawa przesądza strukturę tych kryteriów: obejmują one kryteria sektorowe (progi zdolności do zapewnienia funkcjonowania administracji, przedsiębiorstw i potrzeb obywateli) oraz przekrojowe (skutki w ludziach, konieczność ewakuacji, skutki ekonomiczne i społeczne, wpływ międzynarodowy, unikatowość infrastruktury).

Organami uprawnionymi do wnioskowania o wpis są: właściwi ministrowie (wpis przy spełnieniu kryterium sektorowego łącznie z co najmniej jednym przekrojowym), właściwy miejscowo wojewoda (co najmniej jedno kryterium przekrojowe), Komisja Nadzoru Finansowego oraz Narodowy Bank Polski. Dyrektor RCB informuje właściciela lub posiadacza infrastruktury o wpisie i wynikających z niego obowiązkach w terminie 30 dni.

Odrębnie prowadzony jest wykaz potencjalnej infrastruktury krytycznej, dotyczący inwestycji na etapie projektowania lub budowy. Do inwestorów ujętych w tym wykazie stosuje się część przepisów o operatorach infrastruktury krytycznej, w szczególności w zakresie analizy zagrożeń i zarządzania bezpieczeństwem fizycznym.

Ustawa szczegółowo reguluje obowiązki operatorów wpisanych do wykazu infrastruktury krytycznej. Obejmują one:

1. analizę zagrożeń – prowadzoną na bieżąco, przy czym pierwsza analiza musi zostać przeprowadzona w terminie 6 miesięcy od dnia otrzymania informacji o wpisie;
2. wdrożenie rozwiązań ochronnych – w terminie 6 miesięcy od przeprowadzenia analizy, obejmujących bezpieczeństwo fizyczne (ochrona fizyczna lub zabezpieczenia techniczne, systemy kontroli dostępu), bezpieczeństwo techniczne, osobowe (pracownicy i dostawcy zewnętrzni), cyberbezpieczeństwo, bezpieczeństwo prawne, a także ciągłość działania i odtwarzanie, w tym utrzymywanie własnych systemów rezerwowych do czasu pełnego odtworzenia infrastruktury. Minimalne wymagania w każdym z tych zakresów określi Rada Ministrów w rozporządzeniu;
3. bieżącą współpracę z organami zarządzania kryzysowego, służbami i dyrektorem RCB – w zakresie przekazywania i odbierania informacji o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury;
4. niejawną dokumentację ochrony infrastruktury krytycznej – obejmującą opis infrastruktury, analizę zagrożeń, opis wdrożonych rozwiązań, zasoby rezerwowe, procedury

działania w sytuacji zagrożenia, procedury ciągłości działania i odtwarzania oraz zasady współpracy z organami. Operator składa oświadczenie o opracowaniu dokumentacji w terminie 15 miesięcy od dnia wpisu;
5. raporty o stanie ochrony – przekazywane do 31 marca każdego roku właściwemu ministrowi, wojewodzie lub KNF. Pierwsza edycja dotyczy roku 2027;
6. sprawdzanie pracowników – na stanowiskach umożliwiających dostęp do informacji o bezpieczeństwie infrastruktury operator ma prawo pozyskiwać dane z Krajowego Rejestru Karnego oraz, przy spełnieniu warunków proporcjonalności, żądać danych biometrycznych;
7. wyznaczenie koordynatora ochrony infrastruktury krytycznej – w terminie 30 dni od wpisu. Koordynator podlega bezpośrednio organowi zarządzającemu operatora i musi spełniać wymogi bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych.

Dodatkowym uprawnieniem operatorów jest możliwość stosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze (zagłuszanie sygnału radiowego), służących przede wszystkim do neutralizacji wrogich bezzałogowych statków powietrznych. Stosowanie tych urządzeń dopuszczalne jest wyłącznie w ściśle określonych sytuacjach i wymaga uprzedniej notyfikacji ministra właściwego do spraw wewnętrznych, Prezesa UKE oraz właściwego organu wojskowego zarządzającego częstotliwościami.

Podmioty krytyczne, jako szczególna kategoria operatorów infrastruktury krytycznej wpisanych do wykazu podmiotów krytycznych, podlegają dalej idącym wymaganiom wynikającym z implementacji dyrektywy CER. Centralnym obowiązkiem jest wdrożenie zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, obejmującego:
1. ocenę ryzyka przeprowadzaną nie rzadziej niż raz na dwa lata (uwzględniającą zagrożenia z KOR, zagrożenia antagonistyczne oraz zależności między sektorami);
2. odpowiednie i proporcjonalne rozwiązania organizacyjno-techniczne;
3. bieżącą współpracę z organami zarządzania kryzysowego;
4. gromadzenie informacji o zagrożeniach i incydentach;
5. zarządzanie incydentami oraz stosowanie środków zapobiegawczych i ograniczających skutki zakłóceń.

Pierwsza ocena ryzyka musi zostać przeprowadzona w terminie 9 miesięcy od dnia wpisu do wykazu podmiotów krytycznych.

Rozwiązania organizacyjno-techniczne obejmują m.in. polityki zarządzania ryzykiem, bezpieczeństwo fizyczne budynków i terenów, bezpieczeństwo osobowe, cyberbezpieczeństwo zgodne z wymogami dla podmiotów kluczowych z ustawy o KSC, ciągłość działania, zdolność do ochrony informacji niejawnych, szkolenia personelu oraz audyt i certyfikację. Podmiot wdraża te rozwiązania w terminie 3 miesięcy od przeprowadzenia oceny ryzyka.

Zgłaszanie incydentów istotnych – podmiot krytyczny zgłasza incydent niezwłocznie, nie później niż w terminie 24 godzin od jego wystąpienia lub wykrycia, do właściwego organu do spraw podmiotów krytycznych, dyrektora RCB, Szefa ABW oraz właściwego CSIRT poziomu krajowego. Pełne sprawozdanie z incydentu przekazywane jest w terminie 30 dni. Progi uznania incydentu za istotny określi Rada Ministrów w rozporządzeniu, w podziale na sektory i podsektory.

Audyt zintegrowanego systemu zarządzania bezpieczeństwem – przeprowadzany co najmniej raz na 3 lata, na własny koszt, przez niezależnych audytorów lub jednostkę certyfikującą spełniających wymogi dostępu do informacji niejawnych o klauzuli „poufne". Audytorzy nie mogą być osobami realizującymi lub które realizowały zadania z zakresu systemu bezpieczeństwa w podmiocie audytowanym w ciągu ostatnich 2 lat.

Bezpieczeństwo łańcucha dostaw – podmiot krytyczny identyfikuje dostawców krytycznych, prowadzi ich rejestr, przeprowadza ocenę ryzyka co najmniej raz w roku oraz opracowuje plany awaryjne na wypadek konieczności zastąpienia dostawcy krytycznego. Dostawca krytyczny zgłasza incydenty istotne i podlega audytowi za pośrednictwem podmiotu krytycznego.

Pełnomocnik bezpieczeństwa usługi kluczowej – wyznaczany w terminie 30 dni od wpisu do wykazu, podlegający bezpośrednio organowi zarządzającemu podmiotu, z obowiązkowym dostępem do informacji niejawnych o klauzuli „poufne".

7.1.6. Wdrożenie i nadzór

Ustawa wyznacza organy do spraw podmiotów krytycznych według kryterium sektorowego. Dla sektora energii elektrycznej i ciepła organem właściwym jest minister ds. energii; dla wydobycia kopalin, ropy i paliw, gazu, wodoru i energetyki jądrowej – minister ds. gospodarki surowcami energetycznymi. Sektor bankowości i infrastruktury rynków finansowych nadzoruje Komisja Nadzoru Finansowego. Infrastruktura cyfrowa i usługi ICT podlegają odpowiednio ministrowi ds. informatyzacji i Prezesowi UKE. Pozostałe sektory nadzorują właściwi ministrowie branżowi.

Organy do spraw podmiotów krytycznych prowadzą bieżącą analizę operatorów, identyfikują podmioty krytyczne i dokonują wpisów do wykazu, prowadzą kontrole i nakładają kary pieniężne.

Kontrole prowadzone są w siedzibach podmiotów, miejscach wykonywania działalności lub zdalnie. Osoba prowadząca kontrolę ma prawo do swobodnego wstępu na teren podmiotu, wglądu w dokumenty, sporządzania kopii, żądania wyjaśnień oraz przeprowadzania oględzin urządzeń i systemów informacyjnych. Po zakończeniu kontroli sporządzany jest protokół, od którego podmiot może wnieść zastrzeżenia w terminie 7 dni.

Pojedynczy Punkt Kontaktowy prowadzony jest przez dyrektora RCB. Do jego zadań należą: odbieranie i przekazywanie zgłoszeń incydentów istotnych między państwami UE, przekazywanie Komisji Europejskiej i unijnej Grupie ds. Odporności Podmiotów Krytycznych (CERG) sprawozdań co dwa lata oraz koordynacja współpracy z organami właściwymi do spraw cyberbezpieczeństwa. Pierwsze sprawozdanie Polska przekaże Komisji Europejskiej do 17 lipca 2028 r.

Dotychczasowy jednolity wykaz infrastruktury krytycznej pozostaje w mocy do czasu sporządzenia nowego wykazu. Plany ochrony infrastruktury krytycznej opracowane na podstawie przepisów dotychczasowych zachowują moc do czasu opracowania dokumentacji ochrony przez operatorów zgodnie z nowymi przepisami.

Kluczowe terminy wdrożenia przedstawiają się następująco:

Obowiązek	Termin
Rada Ministrów przyjmuje kryteria identyfikacji infrastruktury krytycznej	3 miesiące od wejścia w życie
Pierwsze wpisy podmiotów krytycznych do wykazu przez organy właściwe	9 miesięcy od wejścia w życie
Pierwsza analiza zagrożeń przez operatora infrastruktury krytycznej	6 miesięcy od wpisu do wykazu IK
Pierwsza ocena ryzyka przez podmiot krytyczny	9 miesięcy od wpisu do wykazu PK
Pierwsze sprawozdanie Pojedynczego Punktu Kontaktowego do komisji Europejskiej o incydentach istotnych	Do 17 lipca 2028 r.

Raport o stanie ochrony infrastruktury krytycznej operator sporządza po raz pierwszy za rok 2027.

Kluczowym wyzwaniem na etapie wdrożenia pozostaje terminowe przyjęcie aktów wykonawczych przez Radę Ministrów – w szczególności rozporządzeń określających minimalne wymagania bezpieczeństwa oraz progi istotności incydentów – od których w praktyce zależy operacyjna wykonalność nowych obowiązków przez podmioty objęte ustawą.

7.2 Cyberprzestrzeń i krajowy system cyberbezpieczeństwa

7.2.1. Krajowy system cyberbezpieczeństwa – architektura i zakres podmiotowy

Cyberprzestrzeń stanowi dziś kluczowy wymiar odporności państwa – równoważny pod względem strategicznym z przestrzenią fizyczną. Deklaracja Haska z 25 czerwca 2025 roku wyraźnie wskazuje „obronę naszych sieci" jako jedną z pięciu kategorii wydatków kwalifikowanych do puli 1,5% PKB, plasując cyberbezpieczeństwo obok ochrony infrastruktury krytycznej i gotowości cywilnej. Krajowy wymiar cyberbezpieczeństwa wyznacza przede wszystkim ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC), znowelizowana ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, wdrażająca dyrektywę NIS2 (UE 2022/2555).

Cel krajowego systemu cyberbezpieczeństwa, wyrażony w art. 3 ustawy KSC, to zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług przez podmioty kluczowe lub podmioty ważne, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych oraz zapewnienie obsługi incydentów. Sformułowanie „odpowiedni poziom bezpieczeństwa" jest wypadkową ryzyka, stanu techniki, wielkości podmiotu i skutków społeczno-gospodarczych ewentualnego zakłócenia.

Nowelizacja z 2026 roku dokonała fundamentalnej zmiany podmiotowej. W miejsce dotychczasowej kategorii „operatorów usług kluczowych" wprowadzono podział na podmioty kluczowe oraz podmioty ważne (art. 5 KSC w nowym brzmieniu). Szacuje się, że w związku z powyższym KSC będzie miało zastosowanie do kilkudziesięciu tysięcy podmiotów z aż 18 sektorów gospodarki.

7.2.2. Wymagane działania na rzecz osiągnięcia poziomu cyberbezpieczeństwa

KSC określa zwarty, hierarchicznie zorganizowany katalog obowiązków, których łączna realizacja ma doprowadzić podmioty kluczowe i ważne do wymaganego poziomu cyberbezpieczeństwa oraz utrzymania go. Obowiązki te grupują się w pięć wzajemnie uzupełniających się osi działania.

Pierwsza oś: System zarządzania bezpieczeństwem informacji (SZBI)

Fundamentem jest obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) w systemach informacyjnych wykorzystywanych w procesach wpływających na świadczenie usługi. Wymóg ten – sformułowany w art. 8 ust. 1 KSC w nowym brzmieniu – obejmuje 13 kategorii środków technicznych i organizacyjnych, proporcjonalnych do oszacowanego ryzyka oraz uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu i skutki społeczno-gospodarcze ewentualnych incydentów. Dla podmiotów ważnych będących podmiotami publicznymi ustawa przewiduje alternatywną ścieżkę – zamiast pełnych wymogów z art. 8 ust. 1 stosują one SZBI spełniający wymogi załącznika nr 4 do KSC. Rada Ministrów może ponadto rozporządzeniem określić szczegółowe wymagania SZBI dla poszczególnych rodzajów działalności, uwzględniając rekomendacje ENISA (art. 8a KSC).

Druga oś: Odpowiedzialność zarządcza i wymagania kadrowe

Nowelizacja z 2026 r. po raz pierwszy expressis verbis nakłada na kierownika podmiotu kluczowego lub ważnego osobistą odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa (art. 8c KSC). Kierownik jest zobowiązany m.in. do: (i) podejmowania decyzji

w zakresie wdrażania i nadzoru SZBI, (ii) planowania adekwatnych środków finansowych na realizację obowiązków cyberbezpieczeństwa, (iii) przydzielania i nadzoru zadań z zakresu cyberbezpieczeństwa oraz zapewnienia świadomości personelu co do wewnętrznych regulacji (art. 8d KSC). Kierownik podmiotu kluczowego lub ważnego musi ponadto co roku odbywać szkolenie z zakresu cyberbezpieczeństwa (art. 8e KSC). Osoba realizująca zadania z zakresu SZBI lub obsługi incydentów musi przedstawić zaświadczenie z KRK o niekaralności za przestępstwa przeciwko ochronie informacji (art. 8f KSC).

Trzecia oś: Zarządzanie incydentami i obowiązki raportowe

KSC reguluje cykl życia incydentu bezpieczeństwa komputerowego w sposób skodyfikowany i wielopoziomowy. Podmioty kluczowe i ważne są zobowiązane do:

a) zapewnienia pełnej obsługi incydentu (wykrywanie, rejestrowanie, analiza, klasyfikacja, priorytetyzacja, działania naprawcze i ograniczenie skutków);
b) zgłoszenia wczesnego ostrzeżenia o incydencie poważnym do właściwego CSIRT sektorowego niezwłocznie, nie później niż w ciągu 24 godzin od jego wykrycia (art. 11 ust. 1 pkt 4 KSC);
c) zgłoszenia pełnego raportu o incydencie poważnym do właściwego CSIRT sektorowego nie później niż w ciągu 72 godzin od jego wykrycia (art. 11 ust. 1 pkt 4a KSC);
d) przekazania sprawozdania końcowego z obsługi incydentu poważnego nie później niż w ciągu miesiąca od dnia zgłoszenia (art. 11 ust. 1 pkt 4c KSC);
e) informowania użytkowników o incydencie poważnym, jeśli ma on niekorzystny wpływ na świadczenie usług oraz w przypadku poważnego cyberzagrożenia – informowania ich o możliwych środkach zapobiegawczych (art. 11 ust. 2a-2b KSC).

Trójpoziomowa architektura CSIRT uzupełniona jest od nowelizacji z 2026 r. przez sieć CSIRT sektorowych. Wzmacnia to reakcję na poziomie sektora, co jest szczególnie istotne dla ochrony podmiotów kluczowych i ważnych.

Czwarta oś: Wewnętrzne struktury cyberbezpieczeństwa i audyt

Realizacja obowiązków wynikających z art. 8–12 KSC musi być oparta na odpowiednim zapleczu organizacyjnym. Podmiot kluczowy lub ważny jest zobowiązany do powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14 ust. 1 KSC). Struktury te muszą spełniać warunki organizacyjne i techniczne określone w rozporządzeniu Ministra Cyfryzacji.

Podmiot kluczowy jest zobowiązany do przeprowadzenia audytu bezpieczeństwa systemu informacyjnego co najmniej raz na trzy lata (art. 15 ust. 1 KSC). Niezależnie od powyższego, w określonych przypadkach organ właściwy do spraw cyberbezpieczeństwa może nakazać przeprowadzenie audytu zarówno podmiotom kluczowym jak i ważnym. Sprawozdanie z audytu jest udostępniane właściwym organom. Audyt stanowi kluczowy instrument weryfikacji osiągnięcia wymaganego poziomu cyberbezpieczeństwa i powinien być centralnym punktem raportowania w ramach mechanizmu wydatkowania 1,5% PKB do NATO.

Piąta oś: Wymiana informacji i certyfikacja cyberbezpieczeństwa

Ustawa KSC wprowadza (art. 8h KSC) formalne ramy dobrowolnej wymiany informacji pomiędzy określonymi podmiotami, CSIRT i organizacjami. Wymieniane informacje mogą dotyczyć m.in. cyberzagrożeń, podatności, technik czy oznak naruszenia integralności systemów informacyjnych. Platformy wymiany informacji stanowią efektywny kosztowo instrument podnoszenia zbiorowego poziomu bezpieczeństwa sektora.

Uzupełnieniem systemu obowiązków jest ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa, tworząca ramy krajowych schematów certyfikacji dla produktów ICT, usług ICT i procesów ICT – umożliwiająca weryfikację poziomu zabezpieczeń w łańcuchu dostaw technologicznych.

7.2.3. Rekomendacje inwestycyjne dla alokacji cyberbezpieczeństwa

Biorąc pod uwagę wymagania ustawy KSC i dokumentowane luki w polskim ekosystemie cyberbezpieczeństwa, priorytetowe kategorie wydatków w ramach alokacji cyberbezpieczeństwa powinny obejmować:

a) Budowę i wyposażenie CSIRT sektorowych (jako bezpośrednich adresatów zgłoszenia incydentów);
b) Dofinansowanie wdrożeń SZBI i audytów bezpieczeństwa dla podmiotów kluczowych i ważnych;
c) Inwestycje w platformy wymiany informacji o zagrożeniach,
d) Programy szkoleń z zakresu cyberbezpieczeństwa dla kadry zarządczej podmiotów kluczowych;
e) Zakup usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów publicznych nieposiadających własnych zdolności;
f) Certyfikacje produktów ICT stosowanych w infrastrukturze krytycznej w ramach krajowego systemu certyfikacji cyberbezpieczeństwa (jako instrument weryfikacji bezpieczeństwa łańcucha dostaw technologicznych).

7.3 Architektura cyberbezpieczeństwa, wykrywanie i reagowanie

7.3.1. Zasady projektowania architektury cyberbezpieczeństwa infrastruktury krytycznej

Alokacja 15% puli odpornościowej na cyberbezpieczeństwo przyniesie trwały efekt obronny wyłącznie wówczas, gdy środki te nie zostaną rozproszone na pojedyncze, punktowe rozwiązania techniczne, lecz wydatkowane w ramach spójnej dyscypliny architektonicznej. Skuteczna ochrona infrastruktury krytycznej nie wynika z zakupu pojedynczego systemu zabezpieczeń, lecz z warstwowego modelu obrony (*defense in depth*), w którym sprzęt, oprogramowanie, protokoły komunikacyjne oraz ramy zarządcze (*governance*) wspólnie utrzymują integralność systemu i ciągłość działania nawet po naruszeniu pojedynczego komponentu. Środki z komponentu 1,5% PKB powinny być zatem kwalifikowane nie według kryterium „zakupu narzędzia", lecz według ich wkładu w mierzalne parametry odporności: ograniczenie powierzchni ataku, głębokość segmentacji sieci, dokładność wykrywania anomalii, czas reakcji oraz czas odtworzenia funkcji systemowych.

Architektura bezpieczeństwa systemów infrastruktury krytycznej różni się fundamentalnie od architektury klasycznych sieci informatycznych. Systemy sterowania procesami fizycznymi – energetyką, wodociągami, ciepłownictwem, transportem – działają w reżimie czasu rzeczywistego, mają deterministyczne wymagania komunikacyjne i bezpośrednio oddziałują na procesy fizyczne. W tych środowiskach dostępność systemu, determinizm jego działania oraz bezpieczeństwo funkcjonalne (minimalizacja ryzyka szkód fizycznych) są często wymaganiami nadrzędnymi wobec klasycznej poufności danych. Każdy mechanizm zabezpieczający musi być więc dobierany tak, aby chronić system bez narażania sterowanego przezeń procesu fizycznego. To rozróżnienie ma bezpośrednie konsekwencje finansowe: bezkrytyczne przenoszenie rozwiązań rynku IT do środowisk przemysłowych prowadzi do kosztownych błędów wdrożeniowych, dlatego wydatki w tym priorytecie powinny opierać się na standardach dedykowanych systemom automatyki przemysłowej, w szczególności normie IEC 62443.[175]

Projektowana architektura powinna respektować zestaw utrwalonych zasad inżynierskich, które

jednocześnie wyznaczają katalog wydatków kwalifikowanych:

- Bezpieczeństwo wbudowane i domyślne (*security by design*, *security by default*) – ochrona jako element projektu systemu, a nie warstwa doklejana wtórnie.
- Segmentacja i izolacja stref (*security zones*) – logiczny i fizyczny podział sieci na strefy o zdefiniowanym poziomie zabezpieczenia (*security level*) dla poszczególnych zasobów, ograniczający ruch boczny atakującego.
- Architektura zerowego zaufania (*zero trust*) – brak dostępu bez uwierzytelnienia, minimalny niezbędny zakres uprawnień (*least privilege*) oraz cykliczna weryfikacja praw dostępu.
- Minimalizacja powierzchni ataku oraz rezygnacja z bezpieczeństwa opartego na niejawności rozwiązań (*security by obscurity*).
- Bezpieczna degradacja (*fail secure*) – kontrolowane przechodzenie systemu w stan bezpieczny w razie awarii.
- Logowanie i monitorowanie zapewniające dostępność danych do analizy śledczej incydentu (*forensic readiness*).

Punktem wyjścia dla każdej inwestycji powinna być analiza ryzyka oparta na zbudowaniu kontekstu bezpieczeństwa, stworzeniu modelu zagrożeń oraz przeprowadzeniu analizy zagrożeń i ryzyk (TARA – *Threat and Risk Analysis*), definiującej cele bezpieczeństwa dla danego systemu. Tylko takie podejście pozwala – przy zawsze ograniczonych zasobach – uniknąć wydatkowania środków na przeciwdziałanie zagrożeniom mało prawdopodobnym lub nieszkodliwym, koncentrując kapitał tam, gdzie ekspozycja jest realna. Ze względu na dynamiczny charakter cyberprzestrzeni analiza ta nie może być jednorazowa: zagrożenia i podatności ocenione jako marginalne w chwili oddania systemu do użytku z czasem stają się ryzykiem wymagającym aktualizacji zabezpieczeń. Architektura systemu powinna więc z założenia umożliwiać cykliczny monitoring stanu bezpieczeństwa, szybką identyfikację komponentów oraz sprawne instalowanie poprawek i łatanie zidentyfikowanych luk.

Projektant rozwiązań musi również uwzględnić wektory pozatechniczne. Bezpieczeństwo łańcucha dostaw i dostawców – opisane szczegółowo w dalszej części opracowania (mechanizm *Vendor Risk Management*, eliminacja dostawców wysokiego ryzyka, kryteria 5G Toolbox) – pozostaje jedną z najpoważniejszych podatności także na poziomie pojedynczych komponentów systemów sterowania; analogiczny rygor należy stosować w całej domenie infrastruktury krytycznej. Komplementarnie należy traktować bezpieczeństwo fizyczne jako potencjalny środek naruszenia cyberbezpieczeństwa oraz procedury bezpiecznego wycofywania i wymiany wyeksploatowanych komponentów, na których mogą pozostawać dane techniczne lub osobowe wykorzystywalne do ataku. Wreszcie – żaden mechanizm techniczny nie zastąpi świadomości cyberbezpieczeństwa użytkowników końcowych, budowanej poprzez szkolenia, weryfikację konfiguracji oraz certyfikację i akredytację systemów; nakłady na ten komponent ludzki powinny być traktowane jako pełnoprawny wydatek kwalifikowany. Nieocenionym, publicznie dostępnym wsparciem przy projektowaniu zabezpieczeń pozostają katalogi technik, taktyk i procedur (TTP) stosowanych przez atakujących, udostępniane m.in. przez MITRE ATT&CK, CISA oraz E-ISAC.[176]

7.3.2. Systemy wczesnego ostrzegania, wykrywania zagrożeń i reagowania (*TDR*)

Tradycyjne środki ochrony – zapory sieciowe i oprogramowanie antywirusowe – przestały być wystarczające wobec współczesnych, wyrafinowanych zagrożeń. Skalę tej zmiany ilustrują przywołane wcześniej dane CERT Polska. W tych warunkach drugą – obok architektury z sekcji 7.3.1 – niezbędną kategorią wydatków staje się budowa zdolności wykrywania zagrożeń i reagowania (TDR – *Threat Detection and Response*). TDR to proces identyfikacji złośliwych działań, zanim wykorzystają one podatność, oraz opracowania i wdrożenia adekwatnej reakcji. Wykracza on poza samo generowanie alertów, dostarczając zespołom bezpieczeństwa kontekstu, wglądu i narzędzi do szybkiego działania.

Architektura skutecznego systemu TDR opiera się na pięciu komponentach, które wyznaczają zakres inwestycji: ciągłym monitorowaniu sieci, punktów końcowych i środowisk chmurowych w czasie rzeczywistym; zaawansowanej analityce ustalającej bazowy poziom normalnej aktywności i wykrywającej od niego odstępstwa; integracji wywiadu o zagrożeniach (*threat intelligence*) z aktualnych źródeł globalnych; zautomatyzowanej reakcji pozwalającej blokować adresy, zatrzymywać zainfekowane procesy i izolować skompromitowane urządzenia; oraz na analizie

śledczej i raportowaniu incydentów, istotnym zarówno operacyjnie, jak i dla zgodności regulacyjnej. W praktyce wykorzystuje się cztery uzupełniające się metody detekcji:

- detekcja sygnaturowa – porównanie z bazą znanych sygnatur ataków; skuteczna wobec zagrożeń znanych, słaba wobec polimorficznych;
- detekcja anomalii – identyfikacja odstępstw od profilu bazowego; skuteczna wobec zagrożeń wewnętrznych i exploitów zero-day, lecz podatna na fałszywe alarmy;
- detekcja behawioralna – analiza zachowań użytkowników, aplikacji i systemów, wykrywająca eskalację uprawnień, ruch boczny i eksfiltrację danych;
- detekcja oparta na wywiadzie o zagrożeniach – wykorzystanie zewnętrznych wskaźników kompromitacji (złośliwe adresy, domeny, skróty plików) wzbogacających alerty o kontekst.

Wybór i kalibracja tych metod muszą odpowiadać profilowi zagrożeń infrastruktury krytycznej: zaawansowanemu złośliwemu oprogramowaniu i ransomware, zagrożeniom wewnętrznym, kampaniom phishingowym oraz exploitom zero-day. Ewolucję zagrożeń napędzają dziś rosnąca złożoność ataków (m.in. *malware* bezplikowy i techniki *living-off-the-land*), powiększająca się powierzchnia ataku (chmura, urządzenia IoT, praca zdalna) oraz presja czasu, wymuszająca wykrywanie i reakcję niemal w czasie rzeczywistym.

Wykrycie stanowi jednak dopiero połowę zadania. Skuteczna reakcja wymaga priorytetyzacji incydentów, zautomatyzowanego powstrzymywania zagrożeń, dostarczenia analitykom kontekstu i narzędzi oraz – co kluczowe – ciągłego doskonalenia procesów na podstawie analizy poincydentalnej. Z perspektywy wydatków kwalifikowanych oznacza to finansowanie nie tylko technologii, lecz także zdolności organizacyjnych: centrów operacji bezpieczeństwa (SOC), pełnej widoczności środowiska (chmura i *on-premises*), automatyzacji zadań rutynowych oraz inwestycji w szkolenie zespołów. Naturalnym beneficjentem tej alokacji jest poszerzanie wydolności operacyjnej zespołów reagowania CSIRT na poziomie sektorowym i krajowym, których efektywność potwierdzają liczby – od blokady niemal 1,88 mln złośliwych wiadomości po ochronę obywateli przed 140 mln wejść na zainfekowane strony.

7.3.3. Wykorzystanie sztucznej inteligencji w wykrywaniu zagrożeń

Skala i tempo współczesnych ataków, wykładniczy wzrost kampanii zautomatyzowanych z użyciem sztucznej inteligencji, drastycznie obniżający barierę wejścia dla grup przestępczych – sprawiają, że obrona oparta wyłącznie na pracy ludzkich analityków i regułach sygnaturowych przestaje nadążać. Odpowiedzią jest wkomponowanie sztucznej inteligencji w systemy TDR. Wykrywanie wspomagane AI analizuje duże wolumeny danych – logi, ruch sieciowy, zachowania użytkowników – w celu identyfikacji zagrożeń znanych i nieznanych, wychodząc poza podejście sygnaturowe ku szybszej i bardziej adaptacyjnej obronie opartej na uczeniu maszynowym, profilach behawioralnych i wykrywaniu anomalii w czasie rzeczywistym. Zastosowania obejmują bezpieczeństwo sieci (wykrywanie nietypowego ruchu), ochronę punktów końcowych, filtrowanie poczty (blokowanie phishingu), analizę zachowań użytkowników, bezpieczeństwo aplikacji oraz monitorowanie środowisk chmurowych pod kątem błędnych konfiguracji.

Podejście to stanowi operacyjne dopełnienie kierunku zarysowanego w bloku „Innowacje i technologie bezpieczeństwa", gdzie wskazano oprogramowanie wykrywające anomalie w infrastrukturze krytycznej, zanim doprowadzą one do awarii. Wdrażanie AI w obronie cybernetycznej wymaga jednak realistycznej oceny ograniczeń, które bezpośrednio wpływają na efektywność wydatkowania środków: potrzeby wysokiej jakości danych treningowych, ryzyka przeciążenia zespołów fałszywymi alarmami, konieczności poprawy interpretowalności modeli (warunkującej zaufanie i trafność decyzji), podatności samych modeli AI na ukierunkowane ataki oraz wyzwań związanych z utrzymaniem wydajności w złożonych środowiskach o dużym wolumenie danych. Z tych względów sztuczna inteligencja powinna być traktowana jako narzędzie wzmacniające, a nie zastępujące analityków. Spójnie z przyjętą w całym raporcie logiką suwerenności technologicznej, kluczowe modele, dane treningowe i kody źródłowe wykorzystywane w obronie infrastruktury krytycznej powinny pozostawać pod kontrolą krajową lub sojuszniczą, tak aby zdolność detekcyjna państwa nie stała się sama w sobie wektorem uzależnienia od dostawców z państw trzecich.

7.4 System Bezpiecznej Łączności Państwowej (SBŁP) i suwerenność cyfrowa

7.4.1. Cyfrowa suwerenność jako fundament bezpieczeństwa państwa

Raport Najwyższej Izby Kontroli (NIK) z 2025 r.[177] jednoznacznie obnażył głębokie opóźnienie oraz brak spójności w obszarze łączności krytycznej w Polsce. W dobie permanentnych zagrożeń hybrydowych oraz dynamicznie zmieniającej się sytuacji geopolitycznej na flance wschodniej NATO, budowa systemu łączności krytycznej przestała być jedynie projektem modernizacyjnym, a stała się bezwzględną koniecznością strategii bezpieczeństwa i odporności. Brak jednolitego standardu komunikacji służb mundurowych oraz administracji państwowej bezpośrednio rzutują na zdolność państwa do reagowania w sytuacjach kryzysowych.

Obecna sytuacja tworzy jednak unikalne „okno technologiczne", które Polska powinna wykorzystać. Zamiast inwestować miliardy w nadrabianie zaległości poprzez wdrażanie przestarzałego i przeznaczonego do komunikacji głosowej standardu TETRA, racjonalna strategia wymaga wykonania technologicznego przeskoku. Przyszłością łączności dla misji krytycznych jest szerokopasmowa technologia 5G PPDR (*Public Protection and Disaster Relief*), wspierana przez budowaną suwerenną infrastrukturę satelitarną UE – konstelację IRIS^2 i zintegrowana z istniejącymi już systemami starszych generacji (TETRA, DMR). Taka synergia nie tylko zapewni służbom ratunkowym i bezpieczeństwa odpowiedni transfer danych, wideo w czasie rzeczywistym, możliwość korzystania z dronów oraz odporność na cyberataki, ale przede wszystkim pozwoli na budowę niezależnych, długofalowych zdolności operacyjnych.

Próbą odpowiedzi na trwający od dekad paraliż jest wspomniana wcześniej Ustawa o ochronie ludności i obronie cywilnej uchwalona 5 grudnia 2024 r. [178]. Wprowadza ona do porządku prawnego pojęcie Systemu Bezpiecznej Łączności Państwowej (SBŁP), mającego obejmować: jawną (SBŁP-J) i niejawną (SBŁP-N) łączność stacjonarną, podsystem wideokonferencyjny (SBŁP-V), bezpieczną łączność mobilną (SBŁP-M), trankingową (SBŁP-T) oraz satelitarną (SBŁP-S). Ustawa stanowi również podstawę prawną dla finansowania systemu oraz powierza odpowiedzialność za jego nadzór ministrowi właściwemu do spraw wewnętrznych[179].

Kluczowym wyzwaniem w procesie wdrażania SBŁP jest zbalansowanie dotychczasowej, głębokiej zależności od technologii dostarczanych przez ograniczoną liczbę podmiotów. Choć rozwiązania te stanowią cenny element wsparcia, pełne bezpieczeństwo państwa frontowego wymaga budowy realnej suwerenności cyfrowej. Oparcie architektury bezpieczeństwa na rozwiązaniach europejskich i krajowych pozwala ograniczyć zależność infrastruktury krytycznej od wąskiej grupy dostawców i zwiększyć stopień suwerenności technologicznej państwa. Dla Polski, jako państwa flanki wschodniej, dywersyfikacja łańcucha dostaw ma przy tym znaczenie nie tylko gospodarcze, lecz także operacyjne, ogranicza ryzyko jednoczesnej utraty zdolności w razie zakłócenia po stronie pojedynczego dostawcy.

Skala tego przedsięwzięcia wymaga nowatorskiego i elastycznego podejścia do jego finansowania. Budżet SBŁP nie może obciążać jednego resortu; powinien opierać się na hybrydowym systemie finansowym. Sukces projektu leży w precyzyjnym montażu finansowym, łączącym:

- Fundusze krajowe: środki z Funduszu Ochrony Ludności, budżetu MSWiA oraz Ministerstwa Obrony Narodowej.
- Fundusze europejskie: unijny instrument „Łącząc Europę" (CEF Digital), Krajowy Plan Odbudowy (KPO) oraz programy powiązane z rozwojem konstelacji IRIS^2.

Niniejszy rozdział stanowi analizę architektury, wyzwań oraz ścieżki wdrożenia SBŁP jako fundamentu nowoczesnej doktryny obronnej i cyfrowej niepodległości Rzeczypospolitej.

Rysunek 5. Ogólnokrajowe cyfrowe systemu radiowe w Europie

Grafika: Raport NIK – s. 12 – https://www.nik.gov.pl/plik/id,30983,vp,34067.pdf

7.4.2. Budowa i utrzymanie Systemu Bezpiecznej Łączności Państwowej (SBŁP) jako fundamentu ciągłości dowodzenia

Według raportu Najwyższej Izby Kontroli z maja 2025 roku, system łączności radiowej w służbach podległych MSWiA nie funkcjonuje dziś właściwie, a jego niewydolność stanowi „istotne ryzyko dla bezpieczeństwa publicznego”[180]. Głównym problemem wykazanym podczas kontroli jest niekompatybilność systemów łączności wykorzystywanych przez Policję, Straż Pożarną, Straż Graniczną i Służbę Ochrony Państwa, wynikająca z braku jednolitego standardu cyfrowego[181]. Chociaż prace koncepcyjne dążące do stworzenia ogólnokrajowego cyfrowego systemu łączności radiowej dla służb i instytucji państwowych trwają od ponad 20 lat, cel ten pozostaje niezrealizowany, czego główną przyczynę stanowiły dotychczas brak dedykowanego mechanizmu finansowania oraz brak skutecznej koordynacji na poziomie centralnym[182]. Budowa spójnego Systemu Bezpiecznej Łączności Państwowej jest zatem konieczna do skoordynowanej działalności podległych służb.

W konsekwencji wieloletnich zaniedbań, poszczególne służby przez lata rozwijały własne systemy, w oparciu o niekompatybilne wzajemnie standardy, czego łączne koszty w latach 2016–2023 wyniosły blisko 435 mln zł[183]. Policja, jako jedyna formacja, realizuje budowę systemu w docelowym, promowanym przez MSWiA standardzie TETRA (SRP-T)[184]. Proces ten pozostaje jednak rozproszony i uzależniony od doraźnego finansowania. System działa obecnie w największych ośrodkach miejskich, jednak w skali kraju większość komend wciąż opiera się na łączności analogowej lub standardzie DMR (Digital Mobile Radio)[185]. W oparciu o ten standard, swój własny system wdrożyła już Straż Graniczna. Wybór ten, uzasadniony ekonomicznie, stworzył jednak barierę technologiczną uniemożliwiającą bezpośredni kontakt z policjantami korzystającymi z TETRY bez użycia specjalnych integratorów[186]. W międzyczasie Państwowa Straż Pożarna opracowała własną koncepcję migracji do systemu DMR, pozostającą w sprzeczności z rekomendacjami MSWiA, zaś Służba Ochrony Państwa wdrożyła i rozwinęła swój system w oparciu o standard NEXEDGE[187].

Niewydolność systemu łączności stwarza bezpośrednie zagrożenie dla życia i zdrowia obywateli oraz funkcjonariuszy, zwłaszcza w sytuacjach wymagających skoordynowanego działania wielu służb, takich jak klęski żywiołowe czy katastrofy drogowe[188]. Ponadto stosowanie przestarzałych systemów bez silnego szyfrowania naraża operacje służb na infiltrację ze strony grup przestępczych czy obcego wywiadu, a masowe wykorzystywanie prywatnych telefonów komórkowych pozwala na precyzyjne śledzenie lokalizacji funkcjonariuszy[189].

Jak wskazano powyżej ustawa o ochronie ludności i obronie cywilnej wprowadzająca SBŁP stanowi podstawę prawną dla finansowania systemu. Jednocześnie ustawa nie zabezpiecza środków konkretnie na budowę SBŁP. Zgodnie z art. 155 ust. 1., na finansowanie wszystkich zadań określonych w ustawie przeznaczone co

roku mają być środki w wysokości nie niższej niż 0,3% PKB. Połowa tej kwoty ma pochodzić z budżetu obronnego państwa, a reszta z budżetów MSWiA, wojewodów oraz Rządowej Agencji Rezerw Strategicznych[190]. Szczegółowy sposób wydatkowania funduszy określa Program Ochrony Ludności i Obrony Cywilnej, opracowywany na okres 4 lat i aktualizowany co 2 lata[191]. Wprowadzony mechanizm musi pokryć wszystkie potrzeby ochrony ludności, w tym kosztowną budowę schronów podziemnych, co może ograniczać fundusze dostępne bezpośrednio na rozwój łączności. Według założeń przedstawionych w ocenie skutków regulacji, łączny koszt rozwoju i utrzymania SBŁP może w ciągu 10 lat wynieść ponad 3,7 miliarda złotych[192].

7.4.3 Zapewnienie pełnej autonomii i odporności technologicznej

System radiokomunikacji TETRA (Terrestrial Trunked Radio) od lat stanowi standard komunikacji przeznaczony dla służb w państwach europejskich. Wprowadzony w latach 90., system oferuje funkcje takie jak grupowa komunikacja głosowa, wiadomości tekstowe, oraz transmisję danych[193]. TETRA została zaprojektowana z myślą o zapewnieniu niezawodnej i bezpiecznej łączności głosowej dla służb odpowiedzialnych za bezpieczeństwo publiczne, ratownictwo oraz zarządzanie kryzysowe. Jednak pomimo wysokiej niezawodności i odporności operacyjnej, możliwości transmisji danych w systemie TETRA są ograniczone w porównaniu z nowoczesnymi technologiami szerokopasmowymi.

W związku z rosnącym zapotrzebowaniem służb na przesyłanie obrazu, danych geolokalizacyjnych, materiałów wideo, wykorzystania dronów oraz innych informacji pochodzących z systemów teleinformatycznych, wiele państw europejskich rozpoczęło proces uzupełniania lub zastępowania sieci TETRA rozwiązaniami opartymi na technologiach LTE i 5G[194]. Przykładem takiej zmiany jest Finlandia, która dokonała zmiany systemu na szerokopasmowy Virve 2[195]. Oprócz podstawowych funkcji, takich jak komunikacja głosowa czy transmisja danych, Virve 2 wykorzystuje sieci 4G i 5G aby priorytetować połączenia, namierzać lokację użytkowników oraz dynamicznie alokować zasoby między ich grupami. W przyszłości pojawią się również usługi roamingu dla służb bezpieczeństwa publicznego, segmentacja sieci 5G oraz technologia Voice over New Radio (VoNR) (IBID). Inne kraje Europy Zachodniej i Północnej planują przeniesienie systemów na szerokopasmowe w latach 2028–2031[196].

Wzrost zapotrzebowania na systemy komunikacji szerokopasmowej, spowodował wzrost zapotrzebowania na europejskie rozwiązania w tym obszarze. Jednocześnie eksperci wskazują na brak jednolitego europejskiego rozwiązania zapewniającego bezpieczną komunikację transgraniczną podczas katastrof, pożarów, powodzi, zamachów terrorystycznych czy kryzysów hybrydowych. Komisja Europejska rozwija projekt European Critical Communication System (EUCCS), którego celem jest stworzenie europejskiej, bezpiecznej i interoperacyjnej infrastruktury komunikacyjnej dla służb bezpieczeństwa, ratownictwa i ochrony ludności[197]. EUCCS ma umożliwić służbom ratowniczym, organom ścigania

Tabela 7. Adopcja nowoczesnych rozwiązań łączności specjalnej w krajach Europy

Państwo	Ramy czasowe	Szczegóły dotyczące migracji i sieci
Hiszpania	2027	Cel osiągnięcia pełnej gotowości serwisowej sieci SIRDEE (misji krytycznej sieci szerokopasmowej).
Finlandia	do końca 2028	Zakończenie równoległego działania starej sieci TETRA i pełna migracja 50 000 użytkowników do usługi VIRVE 2.
Wielka Brytania	2028–2031	Migracja użytkowników PPDR (Public Protection & Disaster Relief) z systemów TETRA do ogólnokrajowych sieci 3GPP (ESN).
Francja	2028–2031	Planowe przeniesienie użytkowników na sieć RRF (Radio Network of the Future); cel to obsługa 300 000 użytkowników do 2028 r
Szwecja	2028–2031	Migracja użytkowników na sieć SWEN (wcześniej Rakel G2), która ma w pełni zastąpić system TETRA do 2030 roku.
Norwegia	do końca 2031	Planowane wycofanie z eksploatacji obecnej sieci Nødnett (TETRA) na rzecz nowej sieci Nytt Nødnett.
Dania	do 2034	Strategia ewolucji i zastąpienia sieci SINE (TETRA), która ma pozostać operacyjna do 2034 roku.
Szwajcaria	2035	Planowane osiągnięcie ogólnokrajowej gotowości serwisowej dla systemu MSK (bezpieczna mobilna łączność szerokopasmowa).
Rumunia	do 2035	Równoległe działanie sieci TETRA wraz z nową siecią szerokopasmową opartą na standardach 3GPP.
Niemcy	od 2026	Rozpoczęcie postępowań przetargowych na pierwszą fazę programu szerokopasmowego, w tym dedykowaną sieć rdzeniową 4G/5G.

Źródło: Public Safety Broadband Spending to Exceed $6.3 Billion by 2028, Says SNS Telecom & IT, MCXTEND, https://www.mcxtend.com/news/public-safety-broadband-spending-to-exceed-6-3-billion-by-2028-says-sns-telecom-it.

i innym służbom bezpieczeństwa prowadzenie działań operacyjnych niezależnie od granic państwowych, przy zachowaniu pełnej interoperacyjności oraz ciągłości komunikacji.

Założeniem inicjatywy jest integracja krajowych systemów komunikacji krytycznej w jednolity ekosystem oparty na standardach 3GPP Mission Critical Services (MCX), obejmujących usługi Mission Critical Push-to-Talk, Mission Critical Data oraz Mission Critical Video[198]. Dzięki temu możliwe będzie nie tylko prowadzenie komunikacji głosowej, ale również wymiana danych operacyjnych, materiałów wideo, informacji geoprzestrzennych oraz wspólnego obrazu sytuacji pomiędzy służbami różnych państw. W oficjalnych materiałach dotyczących projektu podkreśla się, że budowa europejskiego systemu komunikacji krytycznej ma ograniczać zależność od rozwiązań technologicznych pochodzących spoza UE oraz zwiększać odporność europejskiej infrastruktury bezpieczeństwa na zakłócenia geopolityczne, cybernetyczne i gospodarcze[199].

Projekt EUCCS powiązany jest z innym projektem unijnym, IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite)[200]. IRIS² zaprojektowany został jako odpowiedź na rosnące znaczenie odpornej łączności w sytuacjach kryzysowych oraz potrzebę ograniczenia zależności od nieeuropejskich systemów satelitarnych. Dzięki takiemu rozwiązaniu powstają europejskie, bezpieczne i odporne usługi łączności satelitarnej dla administracji publicznej, służb bezpieczeństwa, operatorów infrastruktury krytycznej, ochrony ludności, dyplomacji i obronności[201]. System będzie wspierał komunikację podczas katastrof naturalnych, awarii sieci naziemnych, kryzysów bezpieczeństwa oraz zagrożeń hybrydowych, zapewniając ciągłość działania państwa nawet w sytuacji uszkodzenia lub przeciążenia infrastruktury naziemnej. Program ma dostarczać szyfrowaną komunikację dla instytucji publicznych, służb ratowniczych oraz operatorów infrastruktury krytycznej, stanowiąc satelitarną warstwę bezpieczeństwa dla europejskich systemów komunikacji krytycznej.

7.4.4. 5G jako standard Łączności Krytycznej (*PPDR*) w Polsce

Kluczowym wnioskiem płynącym z analizy potencjału technologicznego nowych generacji sieci komórkowych – co szczegółowo dokumentuje raport Fundacji Digital Poland[202] – jest fakt, że technologia 5G wprowadza całkowicie nową jakość w obszarze bezpieczeństwa i odporności infrastruktury krytycznej, pozostając całkowicie nieporównywalną z rozwiązaniami starszych generacji. Standard 5G NR („New Radio") został od samych podstaw zaprojektowany i sformatowany z myślą o natywnej odporności na zaawansowane cyberataki oraz operacje o charakterze hybrydowym. W przeciwieństwie do systemów takich jak TETRA czy komercyjnych sieci 3GPP opartych o technologie wcześniejszych generacji, gdzie łaty bezpieczeństwa były implementowane wtórnie, w architekturze 5G ochrona danych i integralność sygnału stanowią fundament kodu źródłowego. Standard ten wprowadza zradykalizowane, zaawansowane mechanizmy kryptograficzne, w tym pełne szyfrowanie tożsamości użytkownika w sieci radiowej. Rozwiązanie to skutecznie eliminuje podatności na ataki z użyciem tzw. „IMSI-catcherów" – fałszywych stacji bazowych powszechnie stosowanych przez obce służby wywiadowcze do inwigilacji, przechwytywania ruchu oraz geolokalizacji terminali abonenckich. Dla państwa frontowego, jakim jest Polska, eliminacja tego typu zagrożeń radiowych na poziomie samej architektury sieciowej jest warunkiem bezwzględnym do budowy zaufanego środowiska komunikacyjnego.

Wdrożenie standardu 5G w formule PPDR rozwiązuje zarazem jeden z najbardziej palących problemów strukturalnych polskiego systemu bezpieczeństwa, jakim jest silosowość i brak technicznej kompatybilności systemów łączności poszczególnych formacji. Nowoczesna, jednolita sieć państwowa musi charakteryzować się uniwersalnością pozwalającą na jednoczesną i bezpieczną obsługę nie tylko formacji ratowniczych i porządkowych, takich jak Policja czy Państwowa Straż Pożarna. Struktura SBŁP oparta na 5G posiada wystarczającą pojemność i elastyczność, aby w ramach jednej, spójnej fizycznie infrastruktury połączyć skrajnie rozproszony ekosystem instytucjonalny kraju. Obejmuje to służby specjalne, kontrwywiad, Straż Graniczną, Krajową Administrację Skarbową (KAS), Służbę Więzienną oraz kluczowe ośrodki decyzyjne państwa, w tym Kancelarię Prezesa Rady Ministrów czy Belweder. Zastosowanie technologii tzw. plasterkowania sieci („network slicing") pozwala na logiczne odizolowanie pasm dla poszczególnych formacji wewnątrz jednej sieci, gwarantując każdemu podmiotowi pełną

autonomię, dedykowane parametry bezpieczeństwa oraz bezwzględny priorytet dostępu, eliminując ryzyko przeciążenia systemu nawet w warunkach głębokiego kryzysu kinetycznego czy klęski żywiołowej.

Współczesne pole walki informacyjnej oraz realia zarządzania kryzysowego redefiniują także same potrzeby w zakresie charakteru przesyłanych informacji. Klasyczna łączność głosowa, choć nadal istotna, staje się niewystarczająca wobec wyzwań XXI wieku. Służby mundurowe, ratunkowe i analityczne potrzebują natychmiastowego, mobilnego dostępu do strumieni danych o bardzo wysokiej przepustowości i minimalnych opóźnieniach („Ultra-Reliable Low-Latency Communication" – URLLC). Architektura 5G jako jedyna na rynku skutecznie integruje ekstremalną prędkość transferu z krytyczną, niemal stuprocentową niezawodnością transmisji. Umożliwia to realizację operacji w czasie rzeczywistym w oparciu o zaawansowane narzędzia wsparcia dowodzenia, takie jak bezpośredni podgląd z taktycznych bezzałogowych statków powietrznych (dronów), masowy strumieniowy przesył monitoringu miejskiego w jakości HD, dynamiczne mapowanie stref zagrożeń skażeniem chemicznym i radiologicznym, a także natychmiastową weryfikację telemetryczną i biometryczną na miejscu zdarzenia. Przejście na standard 5G PPDR nie sprowadza się zatem do wymiany sprzętu radiowego. Oznacza zmianę funkcji łączności państwowej: z kanału przekazu komunikatów głosowych w zintegrowany system wsparcia świadomości sytuacyjnej, umożliwiający przesył danych, obrazu i telemetrii w czasie rzeczywistym.

7.5 Finansowanie wykonawców zewnętrznych i ochrona łańcucha dostaw

Skuteczna realizacja i operacyjne wdrożenie SBŁP wymaga nie tylko precyzyjnego doboru technologii, ale przede wszystkim stworzenia stabilnego, a zarazem elastycznego mechanizmu finansowania oraz rygorystycznego zabezpieczenia wykonawczego. Architektura finansowa tego przedsięwzięcia musi sprostać kryteriom odporności na zawirowania makroekonomiczne oraz próby infiltracji łańcucha dostaw przez podmioty trzecie. Doświadczenia ostatnich 20 lat, wskazują, że brak dedykowanych i wieloletnich środków był jedną z głównych przyczyn fiaska wcześniejszych prób budowy jednolitej sieci. Nowa architektura finansowa, nakreślona przez ustawę o ochronie ludności i obronie cywilnej, ma na celu przełamanie tego impasu poprzez oparcie się na trzech filarach zabezpieczających ciągłość inwestycyjną.

Pierwszym i najważniejszym elementem tego modelu jest opisany wcześniej stały mechanizm ustawowy, gwarantujący przeznaczanie corocznie na zadania z zakresu ochrony ludności kwoty nie niższej niż 0,3% PKB. Kluczowym rozwiązaniem w tym obszarze jest tzw. solidarność budżetowa, polegająca na bezpośrednim zaangażowaniu środków Ministerstwa Obrony Narodowej. Połowa wspomnianej kwoty, czyli około 0,15% PKB, wydzielana jest corocznie z limitu wydatków na obronność kraju, co podkreśla strategiczny i militarny wymiar systemu. Pozostała część środków pochodzi z części budżetowej pozostającej w dyspozycji Ministra Spraw Wewnętrznych i Administracji oraz budżetów wojewodów.

Drugim filarem jest Fundusz Ochrony Ludności i Obrony Cywilnej (FOLIOC), będący państwowym funduszem celowym[203]. Przychody tego funduszu są zróżnicowane i obejmują m.in. wpływy z Agencji Mienia Wojskowego, środki z grzywien nakładanych w drodze mandatów karnych przez Państwową Straż Pożarną oraz darowizny

i zapisy. Istotnym elementem wzmacniającym ten mechanizm jest możliwość przekazywania na fundusz do 0,3% zysku netto przez spółki z udziałem Skarbu Państwa oraz jednostek samorządu terytorialnego[204]. Ponadto system przewiduje wsparcie dla samorządów w formie dotacji celowych z budżetu państwa, które mogą pokryć nawet do 100% kosztów inwestycji związanych z budową infrastruktury łączności na poziomie gminnym i powiatowym[205].

Trzecim strumieniem finansowania, traktowanym jako źródło dodatkowe i uzupełniające, są fundusze europejskie. Resort spraw wewnętrznych planuje rozwój SBŁP w pełnej synergii z architekturą unijną, w szczególności w kontekście Europejskiego Systemu Komunikacji Krytycznej (EUCCS). Ma to umożliwić wykorzystanie instrumentów takich jak unijny instrument „Łącząc Europę" (CEF Digital), Krajowy Plan Odbudowy (KPO) oraz programów powiązanych z rozwojem wieloorbitalnej konstelacji satelitarnej IRIS^2, zapewniającej autonomię strategiczną UE[206].

Sama dostępność środków nie gwarantuje jednak sukcesu bez głębokiej optymalizacji procedur zakupowych. Specyfika budowy systemu łączności krytycznej dla służb mundurowych i administracji publicznej w warunkach podwyższonego ryzyka geopolitycznego wymaga odejścia od standardowych, długotrwałych mechanizmów przetargowych. Dotychczasowe doświadczenia pokazują, że klasyczny reżim zakupów publicznych drastycznie wydłuża proces wdrożenia, narażając państwo na ryzyko technologicznego zestarzenia się komponentów jeszcze przed ich implementacją. Podstawowym instrumentem prawnym gwarantującym niezbędną elastyczność budżetową i operacyjną jest wyłączenie stosowania przepisów ustawy – Prawo zamówień publicznych wobec zamówień związanych z budową, utrzymaniem i rozwojem SBŁP. Zastosowanie klauzuli bezpieczeństwa państwa, analogicznie do procedur zakupu zaawansowanych systemów uzbrojenia, pozwala na skrócenie czasu kontraktowania zewnętrznych wykonawców o wiele miesięcy, umożliwia płynne przesuwanie środków w zależności od postępów prac oraz pozwala na prowadzenie poufnych negocjacji z certyfikowanymi podmiotami z pominięciem jawnych procedur, które mogłyby ujawnić słabe punkty projektowanej architektury teleinformatycznej. Rezygnacja z ram PZP nie oznacza przy tym osłabienia kontroli państwa, lecz umożliwia wdrożenie znacznie bardziej rygorystycznych procedur z zakresu cyberbezpieczeństwa i kontrwywiadu gospodarczego. Filozofia budowy SBŁP w oparciu o 5G umożliwia wykorzystanie istniejącej radiowej sieci dostępowej mobilnych operatorów komórkowych, co jest powszechnie stosowaną praktyką przez kraje, które rozpoczęły już realizację takich projektów. Ma ona na celu znaczącą (wieloletnią) optymalizację aspektu czasowego i kosztowego uruchomienia krytycznych usług sieci PPDR. Kryterium decydującym o możliwości realizacji takiego wariantu jest posiadanie przez operatorów komercyjnych sieci zbudowanej w oparciu o komponenty zaufanych dostawców gwarantujące możliwość realizacji usług z zachowaniem najwyższych standardów bezpieczeństwa w oparciu zarówno o kryteria techniczne jak i nietechniczne określone przez Komisję Europejską w 5G Toolbox[207]. W Polsce, na dzień dzisiejszy, nie wszyscy spełniają to kryterium, jednak kwestie te mają zostać uregulowane poprzez mechanizmy zaproponowane w przyjętej przez Parlament Nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa i określonej w niej procedurze weryfikacji oceny dostawców sprzętu i oprogramowania (ICT Supply Chain Risk Management) pozwalających na identyfikację i eliminację rozwiązań od tzw. dostawców wysokiego ryzyka (HRV) w systemach krytycznych, która zgodnie z treścią Sprawozdania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa powinna rozpocząć się jeszcze w 2026 roku[208].

Swoboda proceduralna pozwala na obligatoryjne zaimplementowanie restrykcyjnego mechanizmu *Vendor Risk Management* (VRM). Każdy zewnętrzny wykonawca oraz dostawca komponentów, zarówno w segmencie naziemnej sieci szerokopasmowej 5G PPDR, jak i w komponencie satelitarnym, musi podlegać drobiazgowej, wielostopniowej certyfikacji przez Agencję Bezpieczeństwa Wewnętrznego oraz Służbę Kontrwywiadu Wojskowego. W tym ujęciu kryterium najniższej ceny zostaje bezwzględnie zastąpione kryterium zaufania technologicznego i geopolitycznego, co automatycznie wyklucza z łańcucha dostaw podmioty z krajów podwyższonego ryzyka, w szczególności zależne od kapitału chińskiego lub rosyjskiego. Priorytet zyskują rodzime konsorcja oraz sprawdzeni partnerzy z Unii Europejskiej i państw sojuszniczych NATO, co wprost przekłada się na budowę realnej suwerenności cyfrowej i odporności całej flanki wschodniej.

8 Technologie kosmiczne dla odporności kraju i bezpieczeństwa ludności

8.1 Rosnące znaczenie technologii kosmicznych

Współczesna gospodarka opiera się na technologiach satelitarnych w stopniu, którego skala bywa niedoceniana. Poza powszechnie rozpoznawalnymi zastosowaniami, przekazem medialnym i nawigacją GNSS, sygnały satelitarne zapewniają synchronizację czasu o znaczeniu krytycznym dla rozproszonych systemów bankowych, teleinformatycznych, transportowych i energetycznych. Zobrazowania satelitarne wspierają rolnictwo, gospodarkę przestrzenną, monitoring środowiska i akcje ratunkowe, a dane orbitalne stanowią fundament prognoz pogody oraz badań atmosfery i klimatu. W tym kontekście suwerenność technologiczna w obszarze kosmicznym przestaje być kwestią prestiżu, a staje się jednym z filarów odporności państwa.

Znaczenie tych technologii ujawnia się ze szczególną wyrazistością w sytuacjach kryzysowych, zarówno naturalnych, jak i wywołanych przez człowieka. Polska dysponuje już własnymi doświadczeniami w tym zakresie. Podczas pożaru Puszczy Solskiej satelity systemu FIRMS (NASA) zarejestrowały pierwsze anomalie termiczne, a dane unijnego programu Copernicus umożliwiły szybką ocenę zasięgu ognia oraz monitorowanie chmury dymu zagrażającej mieszkańcom. W trakcie powodzi na Dolnym Śląsku we wrześniu 2024 roku Centrum Informacji Kryzysowej CBK PAN, we współpracy z Instytutem Meteorologii i Gospodarki Wodnej, dostarczało sztabom kryzysowym aktualizowane co kilka godzin mapy zasięgu zalania, dostępne już 40–50 minut po przelocie satelity.

Równie istotną rolę systemy satelitarne odgrywają w budowaniu odporności na zagrożenia generowane przez człowieka. Współczesna agresja nie ogranicza się do działań na linii frontu; obejmuje uderzenia w infrastrukturę w głębi terytorium państwa, prowadzone często poniżej progu otwartego konfliktu: od aktów sabotażu i podpaleń, przez cyberataki, po zakłócanie sygnałów GNSS i incydenty przygraniczne. Skuteczna odpowiedź wymaga zatem zdolności do obserwacji lokalizacji krytycznych z orbity oraz redundantnych, częściowo satelitarnych systemów łączności i nawigacji. Kluczowe pozostaje przy tym synergiczne wykorzystanie zasobów cywilnych i wojskowych: satelity wojskowe w czasie pokoju mogą dostarczać danych użytecznych w zarządzaniu kryzysowym i bieżącej działalności administracji, a infrastruktura cywilna stanowi naturalne wsparcie sił zbrojnych w razie potrzeby.

8.2 Konieczność suwerenności technologicznej w kosmosie

Satelitarne systemy międzynarodowe i sojusznicze już dziś dostarczają nam wielu informacji niezbędnych dla odporności kraju. Jednak całkowite uzależnienie od technologii zagranicznych rodzi zagrożenia jakich doświadczali Ukraińcy, kiedy firma SpaceX wyłączała im łączność w kluczowym momencie przed zaplanowanym atakiem. Oczywiście narodowe systemy powinny być włączone w systemy sojusznicze, co zwielokrotnia ich możliwości. Ale nie wolno zapominać, że w sytuacjach kryzysowych sojusznik może mieć inne priorytety. Musimy więc posiadać własne zasoby, które mogą działać także w sposób autonomiczny. Nie wystarczy jednak zakupić na własność sprzęt z zagranicy, gdyż niezależnie od stanu własności i podpisanych umów w czasie poważnych kryzysów dostawca może nam uniemożliwić korzystanie z tych zasobów. W szczególności dotyczy to satelitów obserwacyjnych i łącznościowych oraz obsługującej je infrastruktury naziemnej.

Polska wykonała już pierwsze kroki w tym kierunku. MON zakupił dwa satelity optyczne wysokiej rozdzielczości od francusko-niemieckiej firmy Airbus oraz trzy satelity radarowe od polskiego oddziału fińskiej firmy ICEYE. Jednak w trosce o budowę suwerennych kompetencji MON uruchomił też pierwsze zamówienia do polskich firm. W listopadzie 2025 na orbicie znalazły się trzy satelity obserwacyjne PIAST wykonane przez polskie konsorcjum kierowane przez Wojskową Akademię Techniczną. Platformy satelitarne dostarczył Creotech Instruments, teleskopy CBK PAN i ScanWay, napędy Instytut Lotnictwa sieci Łukasiewicz. Satelity dostarczają zobrazowania i zostały już przekazane użytkownikowi końcowemu, co dowodzi, że rodzimy sektor kosmiczny jest już w stanie zapewnić polską suwerenność w kosmosie. W tym roku na orbicie znajdą się też cztery satelity optyczne zamówione przez MON, a w kolejnych latach dołączą do nich cztery satelity CAMILA (trzy optyczne i jeden radarowy), wszystkie wykonane przez Creotech Instruments z wysokim udziałem polskich partnerów. Jak wspomniano wyżej, istotne jest zapewnienie synergicznego wykorzystania wszystkich tych satelitów dla zwiększenia odporności kraju.

8.3 Polski wkład w europejską infrastrukturę satelitarną

W listopadzie ubiegłego roku Polska zadeklarowała zwiększenie wkładu do Europejskiej Agencji Kosmicznej (ESA) do 545 mln EUR na programy technologiczne ESA w latach 2026–28 i 186 mln EUR na program naukowy i funkcjonowanie ESA w latach 2026–30. Pierwsza część tych środków wróci do kraju w postaci zamówień na realizację wybranych programów. Szczególne znaczenie mają tu dwa programy cywilne związane z odpornością. Program „*European Resilience from Space*" (ERS) służy budowie europejskich możliwości obserwacyjnych. W jego ramach powstaną prototypu satelitów, które po roku 2028 Komisja Europejska będzie kupować do unijnej konstelacji „*Earth Observation Governmental Service*" (EOGS). Z kolei „*ESA Programme Related to EU Secure Connectivity*" ma rozwijać prototypowe satelity i usługi dla rozwoju telekomunikacyjnej konstelacji unijnej IRIS² („*Infrastructure for Resilience, Interconnectivity and Security by Satellite*").

Kluczowe jest zapewnienie poparcia w ESA dla propozycji zgłaszanych przez polskie podmioty. Pozyskanie kontraktów na prototypowe satelity i usługi przekształciłoby polską składkę do ESA w inwestycję z wielokrotnym zwrotem w postaci zakupów unijnych, a przede wszystkim rozwinęłoby kompetencje niezbędne do rozwoju polskiej suwerenności technologicznej w kosmosie.

Opanowanie technologii budowy satelitów obserwacyjnych przez polski sektor kosmiczny jest powodem do dumy, ale nie wystarczy do osiągnięcia sukcesu na rynkach międzynarodowych. Silna konkurencja i niezwykle szybki rozwój technologii powodują, że firmy muszą intensywnie rozwijać swoje możliwości technologiczne i produkcyjne. Do tego niezbędne są granty rozwojowe przyznawane przez instytucje takie jak NCBR, ARP czy PARP, ale one mogą zapewnić jedynie rozwój technologii w początkowych fazach. Prawdziwą ekspansję zapewnić mogą jedynie duże zamówienia publiczne, gdyż państwo jest ciągle głównym klientem technologii kosmicznych. Taką politykę skutecznie stosowały Francja, Włochy i Niemcy dzięki czemu wypromowały krajowych czempionów (Airbus Pléiades, Thales Alenia Space, OHB), którzy zdominowali rynek europejski. Polska stoi przed szansą dołączenia do tej trójki a nawet skutecznej z nią rywalizacji na niektórych polach.

Wspomniane wyżej zamówienia MON i MRiT to dopiero pierwsze jaskółki nadchodzącej kosmicznej wiosny. Ich suma plus wkład do ESA to rocznie ok. 480 mln EUR, czyli zaledwie 1/94 z około 45 mld EUR stanowiących 5% budżetu, jakie Polska ma przeznaczać na obronność i odporność. Z tego zamówienia MON to ok. 230 mln EUR, a pozostałe to ok. 250 mln EUR rocznie. Potrzeby kraju są znacznie większe. Aby pokryć cały teren kraju i tereny przygraniczne codziennymi przelotami potrzebne jest kilkadziesiąt satelitów obserwacyjnych. Jeśli dodamy do tego wkład do systemów unijnych, w szczególności telekomunikacyjnych oraz koszt niezbędnej infrastruktury naziemnej do odbioru i przetwarzania danych to konieczne są inwestycje rzędu 1 mld EUR rocznie. Zauważmy, że stanowi to zaledwie drobny ułamek środków przeznaczanych na obronność i odporność, co przy rosnącym znaczeniu technologii kosmicznych ciągle nie jest kwotą wygórowaną.

Tabela 8. Porównanie wydatków na technologie kosmiczne

kraj	wkład do ESA [mld EUR]	zamówienia rządowe w kraju + program krajowy	zamówienia rządowe za granicą
Francja	1,30	2,70	
Niemcy	1,70	1,60	
Włochy	1,20	1,00	
Polska dziś	0,22	0,06	0,20
Polska – propozycja	0,40 → 0,60	0,60 → 0,90	0,00

Ambicje naszego kraju powinny jednak sięgać dalej niż tylko zaspokojenie własnych potrzeb. Sektor kosmiczny jest obecnie najszybciej po AI rozwijającą się gałęzią gospodarki na świecie. Zwiększenie poziomu inwestycji w ten sektor do 1,5 mld EUR rocznie, pozwoliłoby na dołączenie Polski do czołówki w usługach satelitarnych w Europie środkowo-wschodniej i wejście do pierwszej czwórki w Europie.

Powyższa propozycja została przedstawiona na tle aktualnych wydatków Polski i czołowych krajów UE. W polskich zamówieniach krajowych uwzględniono konstelacje Piast, Mikroglob i Camila, a w zagranicznych Airbus Pleyades i ICEYE MikroSAR, zaś sumy wydatków podzielono na 4 lata, bo tyle mniej więcej obejmuje zakres realizacji kontraktów. W zamówieniach rządowych innych krajów trudno wydzielić wydatki krajowe i zagraniczne, gdyż Airbus i TAS są firmami międzynarodowymi. Zamówienia rządowe krajów zawierają także projekty realizowane poprzez ESA na zasadzie umów bilateralnych.

Przedstawione powyżej kierunki inwestycji w technologie kosmiczne wykazują ścisłą synergię z priorytetami strategicznymi zdefiniowanymi w rozdziale 4. W obszarze ochrony infrastruktury krytycznej należy podkreślić podwójną funkcję systemów satelitarnych – z jednej strony dostarczają one narzędzi niezbędnych do monitorowania i zabezpieczania kluczowych zasobów państwa, a z drugiej same stanowią strategiczny komponent tej infrastruktury. Ponadto instalacje telekomunikacyjne operujące na orbicie znacząco podnoszą ogólny poziom cyberbezpieczeństwa państwa, gwarantując redundantne i wysoce niezawodne kanały łączności. Zdolności te bezpośrednio warunkują skuteczność działań w zakresie gotowości cywilnej i reagowania kryzysowego, gdzie niezależny dostęp do danych satelitarnych radykalnie optymalizuje procesy zarządzania w sytuacjach nadzwyczajnych. Omawiane rozwiązania stanowią przy tym modelowy przykład wdrażania innowacyjnych technologii bezpieczeństwa, stymulujących rozwój zaawansowanych kompetencji badawczo-rozwojowych. Zwieńczeniem tego wielowymiarowego znaczenia jest kwestia budowy suwerennego przemysłu odpornościowego – sektor kosmiczny, jako gałąź o znaczeniu absolutnie krytycznym dla bezpieczeństwa narodowego, wymaga bezwzględnego zabezpieczenia oraz systemowej dywersyfikacji własnych łańcuchów dostaw.

9 Odporność systemu ochrony zdrowia

System ochrony zdrowia należy do najbardziej krytycznych, a jednocześnie najsłabiej przygotowanych na kryzys sektorów infrastruktury państwa. Wskazują na to zarówno wieloletnie audyty krajowych instytucji kontrolnych, jak i doświadczenia z realnych konfliktów zbrojnych i katastrof ostatnich lat. Współczesny szpital jest budowany według logiki pokojowej: optymalizuje przepływ pacjentów w warunkach przewidywalnego obciążenia, minimalizuje koszty operacyjne, a całkowicie pomija scenariusze, w których placówka może stać się celem ataku lub mieć przerwane zewnętrzne łańcuchy dostaw energii, wody i materiałów medycznych. Każde bezpośrednie uderzenie skutkuje wyłączeniem placówki z użytku na czas nieokreślony. Brakuje również strategii relokacji chorych, która umożliwiłaby szybkie odciążenie zaatakowanych szpitali, oraz sieci obiektów zdolnych do działalności leczniczej w warunkach konfliktu lub katastrofy.

Skala i systemowy charakter tego problemu są dobrze udokumentowane. WHO dokumentuje w Ukrainie już ponad 3 000 zweryfikowanych ataków na infrastrukturę medyczną od czasu pełnoskalowej inwazji Rosji w lutym 2022 roku[209]. W samym 2024 roku odnotowano 487 ataków na placówki ochrony zdrowia w Ukrainie, czyli o 12% więcej niż rok wcześniej[210]. Analiza 617 ukraińskich placówek zdrowia przeprowadzona przez WHO Regional Office for Europe na potrzeby raportu „Underground shelters and services in hospitals" (2025) ujawniła, że zdecydowana większość obiektów nie posiadała ani bezpiecznych stref dla pacjentów i personelu, ani autonomicznych źródeł energii, ani minimalnych zapasów wody i gazów medycznych gwarantujących choćby krótkookresowa ciągłość działalności[211]. Polska doświadcza tego problemu we własnym, szczególnie dotkliwym wydaniu: systemy obrony cywilnej, w tym infrastruktura medyczna, były przez dziesięciolecia pozbawione finansowania i planowania. Przełomem legislacyjnym była dopiero ustawa z 5 grudnia 2024 roku o ochronie ludności i obronie cywilnej, która narzuciła szpitalom obowiązek posiadania budowli ochronnych.[212]

Niniejszy rozdział analizuje trzy wzajemnie powiązane wymiary tego wyzwania. Po pierwsze, przedstawia koncepcje szpitali podwójnego zastosowania, z propozycją WAR-SOR, jako architektonicznych ram projektowych dla polskich inwestycji medycznych. Po drugie, omawia strategie zachowania ciągłości opieki i relokacji pacjentów w warunkach kryzysu. Po trzecie, identyfikuje brakujące ogniwa w łańcuchu dostaw leków, cyberodporności szpitalnych systemów informatycznych i wsparcia psychologicznego dla personelu medycznego pracującego w warunkach stresu wojennego.

9.1 Koncepcja WAR-SOR: szpitale podwójnego zastosowania

Zasadnicze pytanie, na które stara się odpowiedzieć koncepcja WAR-SOR, nie brzmi: „jak zbudować szpital wojenny?", lecz: „jak sprawić, by istniejący lub nowo budowany szpital cywilny nie wypadł z użycia w momencie, gdy jest najbardziej potrzebny?". Odpowiedź leżąca u podstaw tej koncepcji jest jednocześnie architektoniczna i ekonomiczna: nie przez budowę odrębnych, kosztownych obiektów przeznaczonych wyłącznie na czas konfliktu, lecz przez zaprojektowanie lub modernizację szpitala w taki sposób, by jego strefa podziemna lub wzmocniona konstrukcyjnie pełniła użyteczne funkcje medyczne także w czasie pokoju, a w momencie kryzysu stała się autonomiczna, samowystarczalną jednostką ratunkową.

Autonomia takiej jednostki wymaga nie tylko odpowiedniego projektu architektonicznego, lecz także bieżącej wiedzy o stanie infrastruktury warunkującej jej działanie. Wydatki kwalifikowane w tym obszarze powinny obejmować mechanizmy monitorowania zasilania, wody, gazów medycznych, wentylacji, temperatury, dostępności pomieszczeń, łączności oraz zdolności szybkiego przełączenia strefy pokojowej do funkcji kryzysowej. Bez takiej weryfikacji szpital podwójnego zastosowania może istnieć formalnie, ale nie dawać pewności działania w momencie przeciążenia systemu ochrony zdrowia.

Sformułowanie tej koncepcji w polskim kontekście zawdzięczamy prof. inż. arch. Michałowi Grzymale-Kazłowskiemu, architektowi szpitalnemu[213]. Zaproponowana nazwa WAR-SOR to skrót oznaczający szpitalny oddział ratunkowy (SOR) zdolny do działania w warunkach wojennych, rozwijając koncepcje w świetle dokumentu WHO z 2025 roku poświęconego podziemnym schronom szpitalnym[214] oraz doświadczeń izraelskich i fińskich omawianych poniżej. Jego propozycja wpisuje się jednocześnie w szerszy program „Szpitale Przyjazne Wojsku", zainaugurowany w marcu 2025 roku przez Ministerstwo Obrony Narodowej pod patronatem Wojskowego Instytutu Medycznego PIB, który w pierwszym etapie pilotażowym obejmuje 25 placówek z Polski Wschodniej.[215]

Logika ekonomiczna koncepcji dual-use jest fundamentalna dla jej realizacji: koszt inwestycji w strefę podziemną spełniającą standardy budowli ochronnej jest radykalnie wyższy od normalnej infrastruktury medycznej, lecz proporcjonalnie niższy, gdy ta sama infrastruktura generuje przychody lub oszczędza koszty w trakcie codziennej eksploatacji. Dlatego WAR-SOR nie może być „schronem czekającym na wojnę", lecz musi być całodobowo funkcjonalnym elementem szpitala.

W trybie pokojowym WAR-SOR pełni rolę uzupełniającego SOR-u: triage i przyjęcia ambulansów z możliwością dekontaminacji, strefa izolacyjna dla pacjentów skażonych lub zakażonych, diagnostyka obrazowa (RTG, USG, TK, MRI, laboratorium), blok operacyjny do zabiegów planowych i nagłych, strefa wybudzeń i post-operacyjna (POP), centrum dowodzenia szpitalem (serwerownia, BMS, SAP) oraz magazyny leków, opatrunków i środków ochrony. W trybie wojennym lub kryzysowym następuje uruchomienie trybu „W": uszczelnienie budowli, aktywacja niezależnych systemów zasilania, hermetyzacja i filtracja powietrza, izolacja od infrastruktury zewnętrznej. Strefa diagnostyki, blok operacyjny i OIT działają w niezmienionej konfiguracji fizycznej, bez potrzeby przenoszenia sprzętu czy przebudowy przestrzeni[216].

WHO w raporcie z 2025 roku wskazuje na analogiczny model jako optymalne podejście do budowy odporności szpitalnej, opierając się na doświadczeniach ukraińskich, irackich, syryjskich i jemeńskich[217]. Kluczowy wniosek z analizy 617 ukraińskich placówek jest taki sam, jaki legł u podstaw propozycji WAR-SOR: ciągłość infrastruktury technicznej, która nie wymaga czasochłonnej konwersji, jest nieporównanie bardziej wartościowa niż osobna przestrzeń zarezerwowana na czas konfliktu i przez większość życia obiektu pusta[218].

Parametry techniczne budowli ochronnej, w której funkcjonuje WAR-SOR, są precyzyjnie określone przez polskie prawo. Rozporządzenie MSWiA z 21 lutego 2025 roku ustanawia trzy kategorie schronów hermetycznych (S-1, S-2, S-3) oraz trzy kategorie ukryć (U-1, U-2, U-3), różniące się przede wszystkim odpornością na fale uderzeniowa i stopniem filtracji powietrza[219]. Rozporządzenie techniczne z 4 listopada 2025 roku doprecyzowuje wymogi: wentylacja z filtrowentylacją, zapasowe źródła zasilania, komory rozprężne dla kategorii S-2 i S-3, klasy pożarowości materiałów wykończeniowych (A1, A2) oraz minimalny czas autonomii, definiowany jako „okres, w którym osoby przebywające w budowli ochronnej mają zapewnione warunki umożliwiające przetrwanie bez konieczności korzystania z otoczenia zewnętrznego"[220]. Decyzja o kategorii S dla szpitala powinna być podejmowana we współpracy z wojskiem i służbami obrony cywilnej, indywidualnie dla każdej lokalizacji; koncepcja WAR-SOR wskazuje S-1 lub S-2 jako punkt wyjścia[221].

Finansowanie takich inwestycji jest unormowane ustawowo. Ustawa o ochronie ludności i obronie cywilnej dopuszcza sfinansowanie do 100% kosztów poniesionych na tworzenie obiektów ochronnych ze środków publicznych[222], co w połączeniu z instrumentami unijnymi (Connecting Europe Facility Military Mobility, fundusze spójności zderegulowane po rewizji w 2025 roku na potrzeby infrastruktury dual-use) otwiera realne ścieżki finansowania. Warunkiem jest jednak opracowanie standardów projektowych dla szpitali WAR-SOR zanim zostaną wydane decyzje lokalizacyjne dla kolejnej fali inwestycji szpitalnych zaplanowanych w Krajowym Planie Odbudowy i budżecie NFZ na lata 2025–2030[223].

9.2 Doświadczenia zagraniczne: Izrael i Finlandia

Dwa przykłady są szczególnie instruktywne jako punkty odniesienia dla polskiej adaptacji: izraelski szpital Rambam w Hajfie, jako jedyny w pełni operacyjnie przetestowany obiekt tego typu na świecie, oraz fiński system dual-use, jako przykład integracji szpitali z systemem obrony cywilnej opartym na prawie i konsekwentnym egzekwowaniu przez kilka dekad.

Sammy Ofer Fortified Underground Emergency Hospital przy Rambam Health Care Campus w Hajfie jest najdokładniej udokumentowanym i operacyjnie sprawdzonym obiektem szpitalnym dual-use na świecie. Został oddany do użytku w 2014 roku po ośmiu latach budowy za kwotę szacowana na 140 mln USD[224]. Zajmuje trzy kondygnacje podziemne, każda o powierzchni 20 tys. m2 (łącznie 60 tys. m2), i jest zdolny do przyjęcia 2 tys. łóżek, 24 sal operacyjnych oraz działania pełnej infrastruktury intensywnej opieki medycznej, diagnostyki obrazowej, dializy i dekontaminacji[225]. W trybie pokojowym kondygnacje funkcjonują jako parking na 1 500 samochodów. Czas konwersji do pełnej gotowości operacyjnej: 72 godziny (lub 8 godzin w trybie natychmiastowym). Autonomia w warunkach hermetyzacji: 72 godziny bez jakiegokolwiek wsparcia zewnętrznego w zakresie energii, wody, gazu medycznego i żywności.

Prof. Michael Halberthal, dyrektor generalny Rambam, sformułował przyczyny budowy szpitala w słowach, które stanowią zarazem precyzyjny opis logiki ryzyka stojącego za koncepcją WAR-SOR: „W czasie II wojny libańskiej 60 rakiet spadło w promieniu pół mili od naszego kampusu. Zobowiązaliśmy się, że ten scenariusz nie powtórzy się". Dodaje, opowiadając o zdolnościach CBRN obiektu: „Możemy być tam przez bardzo długi czas. W razie wojny biologicznej lub chemicznej możemy zamknąć drzwi i być całkowicie samowystarczalni przez trzy doby"[226]. Pierwszy pełny test bojowy nastąpił 7 października 2023 roku, gdy szpital został uruchomiony w warunkach realnego konfliktu[227].

Podczas eskalacji z Hezbollahem w 2024 roku jeden z trzech poziomów szpitala pozostawał na stałym dyżurze przez 10 miesięcy. Obciążenie planistyczne założone przez IDF to rakieta na Hajfę co cztery minuty przez 60 dni. To właśnie ta skala zagrożenia, nieco mniej dramatyczna lecz strukturalnie podobna do scenariuszy branych pod uwagę przez polska doktrynę obronna

dla obszarów wschodniej flanki, uzasadnia inwestycje infrastrukturalną, która pozornie wydaje się nadmierna w warunkach pokojowych.

Tabela 9. Porównanie parametrów szpitala Rambam FUEH i propozycji WAR-SOR

Parametr	Rambam (Hajfa, 2014)	WAR-SOR (propozycja)
Liczba łóżek	2 000	dostosowana do pojemności szpitala; min. 4–12 stanowisk OIT w trybie W
Sale operacyjne	24	2–3 sale aktywne + pre-op / post-op
Liczba kondygnacji	3 poziomy po 20 000 m²	zależnie od lokalizacji; min. 1 kondygnacja podziemna
Tryb pokojowy	parking na 1 500 samochodów	SOR, blok operacyjny, diagnostyka, magazyny
Czas konwersji	72 h	bez konwersji: infrastruktura stale aktywna
Autonomia	72 h (energia, woda, gazy, żywność)	min. 72 h (wg wymagań NATO BR5)
Koszt	140 mln USD	znacznie niższy dzięki dual-use i integracji z SOR

Model fiński jest mniej spektakularny architektonicznie, gdyż opiera się na regulacjach prawnych a nie na jednorazowym przedsięwzięciu budowlanym finansowanym z filantropii. Finlandia utrzymuje ponad 50 tys. schronów w logice projektowania wszystkich schronów jako obiektów dual-use, służących w czasie pokoju jako parkingi, baseny, hale sportowe lub konferencyjne. Dla Polski transferowalność modelu fińskiego jest przede wszystkim legislacyjna. Polska ustawa schronowa z 2024 roku tworzy fundament analogiczny do fińskiego prawa budowlanego, lecz nie precyzuje jeszcze standardów projektowych dla szpitali. Opracowanie szczegółowych wytycznych jak zaprojektować szpital, a zasadniczo jego część ochronną, jest pilnym zadaniem dla resortu zdrowia, MSWiA i środowiska architektury szpitalnej, zanim rozkręcona machina inwestycyjna NFZ i Ministerstwa Zdrowia będzie realizować kolejne kontrakty budowlane według niezmienionej logiki „optymalizacji pod peace-time throughput".

9.3 Podstawy prawne i status ochrony szpitali w prawie humanitarnym

Koncepcja WAR-SOR operuje w precyzyjnie wyznaczonych ramach międzynarodowego prawa humanitarnego, które jednocześnie chronią szpitale i określają warunki utraty tej ochrony. IV Konwencja Genewska z 1949 roku w art. 18 ust. 1 stwierdza bezwzględnie: szpitale cywilne przeznaczone do opieki nad rannymi i chorymi nie mogą być pod żadnym warunkiem przedmiotem ataku i muszą być w każdym czasie szanowane i chronione przez strony konfliktu[228]. Ochrona ta może ustać wyłącznie wtedy, gdy szpital jest używany do popełniania aktów szkodliwych dla nieprzyjaciela poza obowiązkami humanitarnymi, i wyłącznie po uprzednim ostrzeżeniu z wyznaczonym terminem reakcji[229].

Kluczowe dla oceny legalności koncepcji WAR-SOR jest pytanie, czy integracja szpitala cywilnego z systemem obrony cywilnej przekształca go w cel wojskowy. Odpowiedz prawa humanitarnego jest jednoznaczna i korzystna dla koncepcji dual-use: nie. Art. 61 lit. a Protokołu Dodatkowego I definiuje obronę cywilną przez wykaz zadań humanitarnych, w tym udzielanie pomocy medycznej poszkodowanym; polska ustawa o ochronie ludności expressis verbis definiuje obronę cywilną przez odwołanie do tego właśnie przepisu[230]. W związku z tym przygotowanie ochronne szpitala w celu zapewnienia ciągłości działalności leczniczej na rzecz ludności cywilnej mieści się w art. 61 PA I i nie pozbawia go ochrony konwencyjnej.

Analiza prawna Instytutu Liebera przy West Point potwierdza, że sama budowa wzmocnionych stref szpitalnych i ich integracja z systemem obrony cywilnej nie przekształca szpitala w legitymowany cel wojskowy, pod warunkiem że obiekty te nie są używane do celów militarnych i nie goszczą zdolnych do walki kombatantów ani zapasów uzbrojenia[231]. Międzynarodowy Komitet Czerwonego Krzyża w aktualizacji komentarza do Konwencji z listopada 2025 roku podkreśla niezmienność obowiązku ochrony szpitali i potępiła ataki na infrastrukturę medyczną Ukrainy jako „naruszenia międzynarodowego prawa humanitarnego bez wyjątków"[232].

Jedyne istotne ograniczenie lokalizacyjne wynika z zakazu lokalizowania schronów cywilnych bezpośrednio przy obiektach wojskowych stanowiących legalny cel ataku. Zasada ta musi być uwzględniona już na etapie planowania przestrzennego i projektowania, w szczególności w odniesieniu do szpitali uczestniczących w programie „Szpitale Przyjazne Wojsku", gdzie bliskość baz wojskowych może stanowić dodatkowe ryzyko.

9.4 Strategia zachowania ciągłości opieki i relokacji pacjentów

Koncepcja WAR-SOR, z jej całkowitym skoncentrowaniem na funkcjach ratowniczych i zabiegowych, jest świadomie ograniczona do „pierwszej pomocy i relokacji": jej celem jest uratowanie życia i ustabilizowanie pacjenta, a następnie ewakuacja do bezpiecznych placówek zaplecza. Ta decyzja projektowa ma gruntowne uzasadnienie historyczne i kliniczne. Doświadczenia szpitali z II wojny światowej, w tym obiektów podziemnych, ujawniły, że powrót do zdrowia pacjentów w warunkach podziemnych jest ekstremalnie trudny: brak światła dziennego, wielotygodniowa izolacja i przeciążenie personelu skutkują poważnym pogorszeniem rokowań.

Skuteczność tej strategii zależy jednak od istnienia sprawnie działającego systemu relokacji, który nie został dotychczas opracowany na poziomie ogólnokrajowym. Gen. Kielera wskazuje na to wprost jako na jedno z kluczowych braków polskiego systemu: „szpitale funkcjonujące w bliskim zapleczu pola walki muszą być przygotowane do [...] zmiany priorytetów od standardowej opieki indywidualnej w stronę efektywności populacyjnej", przy jednoczesnym zapewnieniu, że jeden chirurg może nadzorować kilka równoległych operacji[233].

WHO, analizując adaptacje szpitali ukraińskich, wskazuje na trzy kategorie kluczowych zdolności, bez których żaden system relokacji nie jest efektywny. Pierwsza to zapewnione autonomiczne źródła energii, wody i gazów medycznych na minimum 72 godziny, co odpowiada wymogom NATO BR5 i standardom WAR-SOR[234]. Druga to sprawne systemy triage kryzysowego umożliwiające szybkie rozróżnienie między pacjentami wymagającymi natychmiastowej interwencji chirurgicznej, pacjentami możliwymi do leczenia ambulatoryjnego lub ewakuacji oraz przypadkami beznadziejnymi przy ograniczonych zasobach. Trzecia, i często pomijana w planowaniu, to wsparcie psychologiczne i psychiatryczne zarówno dla pacjentów, jak i dla personelu pracującego w warunkach ekstremalnego stresu. WHO jednoznacznie identyfikuje brak tego wsparcia jako jeden z głównych czynników ograniczających zdolność ukraińskich placówek do utrzymania ciągłości działalności.

Sieć zastępczych miejsc hospitalizacji (Alternate Care Sites) jest uzupełnieniem, a nie substytutem sieci WAR-SOR. Miejsca takie, jak centra kongresowe, hale sportowe czy szkoły, mogą przyjąć chorych wymagających opieki ambulatoryjnej lub obserwacji po zabiegach z WAR-SOR, umożliwiając natychmiastowe przejęcie kolejnej fali rannych. Takie przestrzenie wymagają jednak wcześniejszego planowania, przygotowania instalacyjnego (zasilanie, łatwa dostawa tlenu,

zaplecze sanitarne) i stale aktualnych protokołów aktywacji.

Wymagają one również bieżącej informacji o gotowości operacyjnej. Dla zastępczych miejsc hospitalizacji i obiektów relokacji pacjentów należy utrzymywać aktualne dane o dostępności przestrzeni, zasilaniu, wodzie, sanitariatach, możliwości dostarczenia tlenu, łączności, warunkach środowiskowych, personelu pomocniczym, drogach dojazdu oraz ograniczeniach użycia. Sama identyfikacja obiektu jako potencjalnego miejsca opieki nie wystarcza, jeżeli w momencie kryzysu nie można potwierdzić, czy obiekt jest gotowy do przyjęcia pacjentów.

Niezbędnym warunkiem sprawności systemu relokacji jest także stale aktualna baza danych zdolności szpitalnych w czasie rzeczywistym, obejmująca liczbę wolnych łóżek, dostępność sal operacyjnych, stan zapasów krwi, stężenie kadr medycznych i stan systemów zasilania. Wymóg ten jest wpisany w piąte z siedmiu NATO Baseline Requirements for National Resilience (BR5), które wprost nakazuje utrzymywanie „bazy danych zdolności medycznych (MBED) w czasie rzeczywistym" jako koniecznego narzędzia zarządzania masowymi stratami[235].

Baza ta powinna obejmować nie tylko klasyczne dane medyczne, takie jak łóżka, sale operacyjne, krew, personel i zapasy, lecz także parametry infrastrukturalne warunkujące możliwość udzielania opieki. Należy uwzględnić: dostępność zasilania awaryjnego, wody, ogrzewania lub chłodzenia, wentylacji, gazów medycznych, łączności, cyberbezpieczeństwa systemów szpitalnych oraz status miejsc zapasowych wykorzystywanych do relokacji pacjentów. Dopiero takie ujęcie pozwala traktować bazę zdolności medycznych jako narzędzie operacyjne, a nie wyłącznie ewidencyjne.

9.5 Strategiczne rezerwy leków, odporność farmaceutyczna i cyberbezpieczeństwo

Odporność szpitali dual-use i systemu relokacji pacjentów jest wprost uzależniona od dostępności leków i wyposażenia medycznego w chwili kryzysu. Polska nie posiada dotychczas transparentnego, publiczne weryfikowalnego systemu strategicznych rezerw leków dla ludności cywilnej z jasno określonymi minimalnymi poziomami i protokołami rotacji zapasów. Jest to luka strukturalna identyfikowana jako jeden z najpilniejszych wymiarów reformy: apeluje o ustawowe zobowiązanie producentów i importerów leków do utrzymywania zapasów wybranych kategorii na co najmniej 6 miesięcy, wzorując się expressis verbis na modelu fińskiej Huoltovarmuuskeskus[236].

Zagrożenie dla dostępności leków ma charakter strukturalny, nie tylko kryzysowy. Komisja Europejska oszacowała w 2021 roku, że 80% importowanych składników farmaceutycznych (API, Active Pharmaceutical Ingredients) pochodzi z pięciu krajów, przy czym same Chiny odpowiadają za około 45% wartości importu API do Unii Europejskiej[237]. Pandemia COVID-19 uzewnętrzniła katastrofalne skutki tej koncentracji: maseczki, respiratory i leki sedatywne stosowane na oddziałach intensywnej terapii stały się niedostępne w całej Europie w ciągu kilku tygodni od zamknięcia chińskich fabryk. Dla Polski, która w warunkach konfliktu mogłaby mieć jednocześnie przerwane szlaki dostaw od wschodu i przeciążone porty od zachodu, zweryfikowane i zdecentralizowane strategiczne zapasy leków stanowią pierwszą linię farmaceutycznej obrony.

Unia Europejska podejmuje pierwsze systemowe kroki w tym kierunku. Rada UE przyjęła 2 grudnia 2025 roku swoje stanowisko w sprawie Critical Medicines Act, a 12 maja 2026 roku Rada i Parlament Europejski osiągnęły porozumienie polityczne w trilogu[238]. Akt ustanawia Unijną Listę Leków Krytycznych obejmującą ponad 200 substancji czynnych, tworzy mechanizm koordynacji rezerw awaryjnych i wprowadza kryteria

odporności łańcucha dostaw do zamówień publicznych. Jednakże CMA jest aktem ramowym: faktyczna ochrona wynikająca z jego wdrożenia będzie zależeć od tempa i ambicji transpozycji krajowej. Polska ma szansę odegrać wiodącą rolę w regionie, jeśli wdroży wymagania CMA szybciej i szerzej niż minimalne standardy unijne.

Odrębne, ciągle niedostatecznie doceniane zagrożenie dla ciągłości opieki medycznej stanowią cyberataki na szpitalne systemy informatyczne. ENISA dokumentuje, że ransomware odpowiada za 54% wszystkich incydentów cyberbezpieczeństwa w sektorze zdrowia UE, a szpitale są celem 42% takich przypadków[239]. Atak na irlandzki Health Service Executive w maju 2021 roku jest dotąd najbardziej szczegółowo udokumentowanym przykładem: atakujący zaszyfrował około 80% sieci organizacji zatrudniającej ponad 130 tys. osób i operującej 70 tys. urządzeń w ponad 4 tys. lokalizacjach. Pełna odbudowa zajęła cztery miesiące; szacowany koszt odbudowy infrastruktury: 102 mln EUR, a Kontroler i Audytor Generalny Irlandii szacował dodatkowe 657 mln EUR potrzebnych inwestycji przez kolejne siedem lat.

Cyberatak na szpital może w warunkach pokojowych być równie paraliżujący jak fizyczne uderzenie w warunkach konfliktu: zatrzymuje dostęp do historii choroby, systemów dawkowania leków, rezerwacji sal operacyjnych i wyników badań diagnostycznych. W warunkach kryzysu lub konfliktu, gdy cyberatak może być skoordynowany z atakami kinetycznymi, skutki są potencjalnie katastrofalne. Projektowanie WARSOR musi zatem uwzględniać fizyczną izolację kluczowych systemów informatycznych od sieci zewnętrznych, redundantne systemy łączności niezależne od infrastruktury cywilnej oraz regularne procedury backupu przechowywane poza siecią.

9.6 Rekomendacje wdrożeniowe

Zasadnicze ograniczenie obecnej sytuacji jest natury proceduralnej, nie prawnej ani finansowej: ustawa o ochronie ludności i obronie cywilnej, rozporządzenia techniczne z 2025 roku i program „Szpitale Przyjazne Wojsku" tworzą fundament, ale brakuje standardów projektowych dla szpitali w budowlach ochronnych. Dopóki takie standardy nie zostaną opracowane i zatwierdzone, kolejne inwestycje szpitalne Będą realizowane według logiki pokojowej, a szansa wbudowania odporności w naturalny cykl inwestycyjny zostanie zaprzepaszczona na dekadę.

Pierwszym krokiem jest powołanie interdyscyplinarnego zespołu projektowego przy Ministerstwie Zdrowia, MSWiA i Ministerstwie Obrony Narodowej, który w ciągu 12 miesięcy opracuje „Wytyczne projektowe dla szpitalnych budowli ochronnych. Zespół powinien obejmować architektów szpitalnych, inżynierów budownictwa ochronnego, klinicystów z doświadczeniem medycyny ratunkowej i taktycznej (WIM-PIB jest naturalnym centrum), prawników międzynarodowego prawa humanitarnego oraz oficerów służb cywilno-wojskowych NATO.

Równocześnie należy wdrożyć systematyczny audyt istniejących szpitali pod kątem możliwości adaptacji. Priorytetem powinna być wschodnia flanka (szpitale objęte programem „Szpitale Przyjazne Wojsku") oraz szpitale powiatowe w strefach zagrożeń według wskazań BBN. Wyniki audytów powinny zasilać bazę danych zdolności medycznych (MBED) wymaganą przez NATO BR5.

W obszarze farmaceutycznym niezbędne jest przyjęcie ustawy o strategicznych rezerwach leków dla ludności cywilnej, która wzorem modelu fińskiego określiłaby minimalne poziomy zapasów dla wybranych kategorii terapeutycznych, zasady ich rotacji, decentralizację magazynowania oraz mechanizm aktywacji w sytuacji kryzysowej. Realizacja i wdrożenie unijnego

Critical Medicines Act powinno być traktowane jako minimalne standardy, które Polska powinna przekraczać, a nie ograniczać się do docelowych poziomów ambicji.

Wreszcie, szkolenie personelu medycznego do działania w warunkach ograniczonych zasobów i stresu wojennego jest elementem, który w pełni decyduje o efektywności WAR-SOR niezależnie od jakości infrastruktury. Bezużyteczna jest nawet najdoskonalsza strefa operacyjna, jeśli personel nie zna procedur triage kryzysowego, nie ma wprawy w zdublowaniu stanowisk OIT ani nie umie funkcjonować bez elektronicznego systemu zarządzania pacjentem. Wnioski z raportu WHO opierającego się na Ukrainie są jednoznaczne: regularne ćwiczenia w realistycznych warunkach są nieodłącznym warunkiem utrzymania sprawności operacyjnej szpitala odpornego na kryzysy.[240]

10 Budowa krajowego przemysłu odpornościowego

Choć pojęcie „przemysł odpornościowy” nie funkcjonuje jako wyodrębniona kategoria w urzędowych klasyfikacjach statystycznych, stanowi on nowy, strategiczny paradygmat w definiowaniu bezpieczeństwa i gospodarki państwa. Koncepcja ta integruje kluczowe segmenty tradycyjnego przemysłu, ze szczególnym uwzględnieniem sektora IT, energetyki, branży chemicznej oraz zbrojeniowej, których nadrzędnym zadaniem jest zagwarantowanie operacyjności, przetrwania i ciągłości działania struktur państwowych w warunkach skrajnego kryzysu.

W obliczu współczesnych wyzwań geopolitycznych oraz sojuszniczych zobowiązań państw NATO do alokacji do 1,5% PKB na rzecz gotowości cywilnej, cyberbezpieczeństwa i rezerw strategicznych, koncepcja ta otwiera przed Polską unikalne okno możliwości. Wolumen środków przeznaczany na budowę odporności powinien być traktowany również jako kluczowy instrument reindustrializacji. Przemyślane wydatkowanie środków publicznych w tym obszarze pozwala na realizację dwóch celów jednocześnie: diametralne podniesienie zdolności państwa do absorpcji szoków oraz stymulację krajowego ekosystemu technologicznego.

Opieranie bezpieczeństwa na masowym imporcie gotowych rozwiązań prowadzi do niebezpiecznego uzależnienia od zewnętrznych łańcuchów dostaw i obcych technologii. Prawdziwa odporność wymaga budowania rodzimego potencjału wytwórczego. Inwestycja w krajowy przemysł odpornościowy to nie tylko gwarancja bezpieczeństwa dostaw, ale także impuls do tworzenia wysokospecjalistycznych miejsc pracy, rozwoju zaawansowanych kompetencji inżynierskich i budowy realnej suwerenności technologicznej, która stanowić będzie trwały element naszej racji stanu.

10.1 Koszyk odpornościowy jako instrument reindustrializacji i suwerenności technologicznej

Decyzja zobowiązująca sojuszników NATO do przeznaczania do 1,5% PKB rocznie na ochronę infrastruktury krytycznej, cyberbezpieczeństwo, gotowość cywilną, rezerwy strategiczne i innowacje, otwiera przed Polską okno możliwości, które wykracza poza kategorie bezpieczeństwa sensu stricto. Jeśli środki te zostaną wydatkowane przemyślanie, każda złotówka z „koszyka odpornościowego" może jednocześnie wzmocnić zdolność państwa do przetrwania kryzysu i zasilić krajowy ekosystem gospodarczy, w postaci miejsc pracy, kompetencji inżynierskich, zwiększenia eksportu i technologicznej suwerenności. Jeśli natomiast wydatkowanie przyjmie formę masowego importu gotowych rozwiązań, pieniądz publiczny opuści kraj, pozostawiając za sobą infrastrukturę uzależnioną od zewnętrznych łańcuchów dostaw i zagranicznych kodów źródłowych. Polska, jako kraj wydający na obronność więcej niż jakikolwiek inny sojusznik NATO w relacji do PKB – dysponuje zarówno skalą zamówień, jak i politycznym kontekstem, by podejść do koszyka odpornościowego jako do instrumentu reindustrializacji. Niniejszy rozdział analizuje, w jaki sposób warto to zrobić, jakie wzorce oferują inne państwa europejskie i na jakich warunkach inwestycja w krajowy przemysł odporności może się stać trwałym elementem strategii bezpieczeństwa.

Punktem wyjścia musi być diagnoza: od kogo polska odporność faktycznie zależy. Odpowiedź jest niepokojąca. Polski Instytut Ekonomiczny zidentyfikował w marcu 2025 r. 321 kategorii towarów uznanych za kluczowe dla gospodarki, z których Polska pozostaje w krytycznej zależności importowej, wskaźniki podatności sięgają 0,27 w biotechnologii i 0,21–0,24 w sektorze farmaceutyczno-obronnym[241]. Europa jako całość produkuje zaledwie kilka procent światowej podaży aktywnych substancji farmaceutycznych (API), choć jeszcze w 1981 r. jej udział w produkcji globalnej wynosił 63%[242]. Chiny dostarczają 100% zużywanych w UE ciężkich pierwiastków ziem rzadkich i 97% magnezu[243], a gdy w 2025 r. Pekin ograniczył eksport magnesów neodymowych, część europejskich producentów była zmuszona wstrzymać linie montażowe. W obszarze półprzewodników Europa wytwarza dziś poniżej 10% globalnej produkcji, mimo że w 2023 r. weszła w życie ustawa o chipach z budżetem 43 mld euro i celem 20% do 2030 r.[244]. Te liczby nie są jedynie ekonomicznym tłem – są mapą słabości, którą każdy potencjalny agresor może odczytać.

10.2 Doświadczenia europejskie w budowaniu zintegrowanego ekosystemu odporności

Najbardziej spójnym modelem instytucjonalnym w obszarze niemilitarnego przemysłu odporności pozostaje fiński system oparty na Krajowej Agencji Bezpieczeństwa Dostaw – Huoltovarmuuskeskus (NESA)[245]. Warto go przeanalizować szczegółowo, bo jego logika różni się zasadniczo od polskiego podejścia budżetowego. Fundusz Bezpieczeństwa Dostaw (Huoltovarmuusrahasto), którym zarządza NESA, nie jest zasilany z podatków ogólnych, lecz z dedykowanej opłaty strategicznej doliczanej do akcyzy energetycznej: 0,00013 euro za kilowatogodzinę energii elektrycznej, 0,0068 euro za litr benzyny, 1,18 euro za tonę węgla grzewczego. Stawki te odpowiadają ok. 0,5% ceny detalicznej paliw i stanowią niewidoczną dla konsumenta składkę ubezpieczeniową na wypadek kryzysu łańcuchów dostaw. Bilans funduszu na koniec 2022 r. wynosił 2,3 mld euro, a reforma legislacyjna przyjęta w 2025 r. zakłada wzrost rocznych wpływów z ok. 42 mln euro do

92 mln euro do 2027 r.[246]. Mechanizm jest zatem w dużej mierze odporny na polityczne przetargi budżetowe, nie rywalizuje z wydatkami na edukację czy zdrowie, bo pochodzi z odrębnego, technicznego strumienia.

Model NESA opiera się na sieci około tysiąca firm działających w kilkunastu „poolach" sektorowych: energetycznym, paliwowym, teleinformatycznym, transportu morskiego, medycznym, żywnościowym i innych. Firmy objęte poolami mają ustawowe obowiązki utrzymywania zapasów bezpieczeństwa, opracowywania planów ciągłości działania i raportowania gotowości. Nie jest to jednostronne obciążenie: w zamian NESA oferuje finansowanie zapasów przez fundusz, doradztwo techniczne i uprzywilejowany dostęp do zamówień publicznych związanych z gotowością. W 2022 r. audyt cyberodporności objął 121 firm z 12 sektorów. Jest to przykład tego, jak wymagania regulacyjne mogą jednocześnie podnosić kompetencje krajowego sektora prywatnego[247]. Fiński model nie jest jednak pozbawiony ograniczeń: jego skuteczność opiera się na kilkudziesięcioletniej kulturze „kokonaisturvallisuus" (kompleksowego bezpieczeństwa), której nie można zaimportować razem z regulacją. Polskie wdrożenie analogicznej koncepcji musiałoby liczyć się z koniecznością zbudowania zaufania między administracją a sektorem prywatnym, który, jak sygnalizował w 2026 r. prezes RARS, wykazuje malejące zainteresowanie współpracą[248].

Szwecja oferuje przykład innego rodzaju: sprawnej odbudowy zdolności cywilnych po ich celowym demontażu w latach 1990–2015. Po tym jak szwedzkie siły zbrojne zredukowały swój udział w planowaniu obronnym, a obrona cywilna przestała być priorytetem, seria dokumentów strategicznych z lat 2015–2020 doprowadziła do reaktywacji koncepcji „totalt försvar" – całkowitej obrony integrującej komponent wojskowy i cywilny[249]. Efektem jest pakiet inwestycyjny ogłoszony we wrześniu 2025 r. na lata 2026–2028: 12 mld koron szwedzkich wyłącznie na obronę cywilną, w tym 4,9 mld koron na opiekę zdrowotną (magazynowanie leków, zdolności operacyjne szpitali, testy NAT dla krwiodawstwa) oraz 2,1 mld koron na zapasy żywności i wody[250]. Warto odnotować, że od 1 stycznia 2026 r. Szwecja wyodrębniła agencję odpowiedzialną za obronę cywilną (MCF – Myndigheten för civilt försvar) z dotychczasowej MSB, co oznacza instytucjonalne rozdzielenie zarządzania kryzysowego i obronności cywilnej. Ponadto Szwecja od listopada 2024 r. dystrybuuje broszurę „Om krisen eller kriget kommer" („Jeśli nastanie kryzys lub wojna") wśród całej populacji[251], a jej wersję dla firm – „Preparedness for businesses", do 130 000 podmiotów. Ten element budowania świadomości i odpowiedzialności społecznej jest integralną częścią modelu, nie dodatkiem. Co istotne, Polska jest jednym z sygnatariuszy memorandum o ochronie ludności cywilnej w regionie Bałtyku, podpisanego przez Szwecję i osiem innych państw w marcu 2026 r.[252], co tworzy formalne ramy wymiany dobrych praktyk.

Estonia dostarcza z kolei dowodu, że bardzo małe państwo może stać się eksporterem technologii odporności i osiągnąć z tego tytułu zarówno korzyści gospodarcze, jak i polityczne. Platforma X-Road, uruchomiona w 2001 r. jako szkielet cyfrowej administracji, łączy dziś ponad tysiąc organizacji, obsługuje ponad trzy miliardy zapytań rocznie i wygenerowała według szacunków oszczędności równoważne 1 345 latom pracy ludzkiej rocznie[253]. Co ważniejsze z punktu widzenia rozdziału, X-Road jest dziś wdrożona w ponad dwudziestu krajach: od Finlandii, przez Japonię i Kambodżę, po Brazylię[254], a jej ekspansją zarządza Nordic Institute for Interoperability Solutions (NIIS), spółka powołana wspólnie przez Estonię, Finlandię i Islandię. Oprogramowanie jest open source na licencji MIT, co oznacza, że Estonia nie czerpie bezpośrednich przychodów licencyjnych, ale czerpie je pośrednio: firmy estońskie, takie jak Cybernetica i Nortal, realizują wdrożenia, a e-Governance Academy eksportuje wiedzę organizacyjną. Model ten pokazuje, że „przemysł odpornościowy" nie musi oznaczać wyłącznie fizycznej produkcji, może obejmować oprogramowanie, standardy i doradztwo instytucjonalne, które są równie strategiczne.

Dopełnieniem obrazu estońskiego jest koncepcja Data Embassy[255]: ministerstwa przechowują kopie zapasowe krytycznych rejestrów państwowych w zaszyfrowanych serwerach za granicą (pierwsza ambasada w Luksemburgu, otwarta w 2017 r.), korzystając ze statusu ochrony dyplomatycznej na mocy umów dwustronnych. To innowacja doktrynalna, państwo nie może być ubezwłasnowolnione przez zniszczenie fizycznej infrastruktury na własnym terytorium. Polska, jako kraj graniczący z Rosją i Białorusią i jako kraj z udokumentowanym zagrożeniem sabotażowym[256], powinna rozważyć analogiczne rozwiązania dla systemów krytycznych w obszarze

zarządzania kryzysowego, rejestrów ludności, systemu podatkowego i ochrony zdrowia.

Niemcy, mimo opóźnionej reakcji na zagrożenie po 2022 r., budują dziś najszerzej zakrojony w Europie system regulacyjny dla operatorów infrastruktury krytycznej. Ustawa KRITIS-Dachgesetz, uchwalona przez Bundestag 29 stycznia 2026 r. i obowiązująca od 17 marca 2026 r.[257], transponuje dyrektywę CER (UE 2022/2557) i obejmuje 11 sektorów infrastruktury krytycznej. Każdy operator o zasięgu obsługującym ponad 500 000 osób ma obowiązek rejestracji w Federalnym Urzędzie Ochrony Ludności (BBK), przeprowadzenia analizy ryzyka i wdrożenia środków odporności w ciągu kolejnych dziesięciu miesięcy. Na wrzesień 2025 r. zarejestrowane były już 2 135 instalacje, a wejście w życie dyrektywy NIS2 w grudniu 2025 r. rozszerzy zakres podmiotowy z 4 500 do ok. 29 500 firm[258]. Równolegle Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) dysponuje budżetem 230,7 mln euro w 2025 r. i ponad 1 790 etatami[259], a Sondervermögen (specjalny fundusz 500 mld euro uchwalony po nowelizacji konstytucji w 2025 r.) zasila cyfryzację administracji i bezpieczeństwo zdrowotne. Warto jednak odnotować krytykę środowiska prawniczego: ustawodawca niemiecki nie skorzystał z opcji przewidzianej w dyrektywie CER, która pozwala na współfinansowanie kosztów odporności po stronie operatorów[260]. Koszty implementacji KRITIS-DachG zostały w całości przerzucone na firmy prywatne, co eksperci oceniają jako wybór krótkowzroczny, bo mniej zamożni operatorzy mogą nie być w stanie ponieść tych kosztów bez wsparcia. Polska, przygotowując analogiczną regulację, powinna rozważyć właśnie te klauzule współfinansowania.

Przykład Czech jest nieco odmienny, ale pouczający w swoim rynkowym charakterze. Czeski sektor cyberbezpieczeństwa rozwinął się bez interwencjonistycznej polityki przemysłowej, jego symbolem jest Avast (dziś część Gen Digital po fuzji z NortonLifeLock w 2022 r. za 8,1 mld dolarów), którego laboratoria badawcze zatrudniają ponad 4 000 osób, z większością w Czechach i Kalifornii. Czeski Urząd ds. Cyberbezpieczeństwa (NÚKIB) organizuje co roku Praską Konferencję Cyberbezpieczeństwa, która przyciąga ponad 400 uczestników z 40 krajów i służy eksportowi norm, kompetencji i sieci powiązań[261]. Lekcja dla Polski polega na tym, że firmy technologiczne w obszarze odporności powstają nie tylko przez zamówienia publiczne, lecz przez klimat regulacyjny, dostęp do talentów i otwartość na rynki globalne. Polska, z silnym zapleczem uczelni technicznych i rosnącym sektorem IT, dysponuje warunkami startowymi – brakuje natomiast mechanizmu, który powiązałby prywatną innowację z publicznym popytem na rozwiązania odpornościowe.

Z punktu widzenia skuteczności działania konieczne jest również przesunięcie odpowiednich zasobów. Poniższe zestawienie ilustruje różnorodność podejść stosowanych przez państwa europejskie do finansowania odporności niemilitarnej.

Tabela 10. Porównanie modeli finansowania odporności

Kraj / Agencja	Model finansowania	Skala roczna	Kluczowa cecha
Finlandia NESA	Pozabudżetowy fundusz; opłata strategiczna od energii (~0,5% ceny detalicznej)	Bilans 2,3 mld EUR; wpływy ~92 mln EUR/rok (plan 2027)	Obowiązkowe poole sektorowe; ~1 000 firm; zapasy utrzymywane przez sektor prywatny
Szwecja MCF	Budżet państwa (pakiet 2026–2028)	12 mld SEK na lata 2026–2028; 4,9 mld SEK na zdrowie	Wyodrębnienie agencji obrony cywilnej (MCF od 2026); broszura dla 130 000 firm
Niemcy BSI / BBK	Budżet federalny + Sondervermögen (500 mld EUR)	BSI: 230,7 mln EUR (2025); BMG cyber zdrowia: 189 mln EUR (2026)	KRITIS-DachG: 11 sektorów, obowiązki rejestracji i planów ciągłości; ~29 500 podmiotów NIS2
Estonia RIA / NIIS	Budżet państwa + eksport know-how przez firmy prywatne	X-Road: 3 mld zapytań/rok; eksport do >20 krajów	Open source + komercyjne wdrożenia (Cybernetica, Nortal); Data Embassy jako backup suwerenności
Polska RARS	Budżet państwa (cz. 16 KPRM / 42 MSWiA)	Niezweryfikowany całkowity budżet; zapasy leków na 3 mies., paliwa na 90 dni	Malejące zainteresowanie współpracą firm prywatnych; nieprawidłowości wg NIK 2024

10.3 Krajowy potencjał przemysłowy: stan obecny i perspektywy rozwoju sektora

Polska nie zaczyna od zera. Rządowa Agencja Rezerw Strategicznych (RARS), następca prawny Agencji Rezerw Materiałowych, zarządza zapasami żywności, paliw (na 90 dni), leków, sprzętu medycznego i od nowelizacji z 2024 r. – rezerw technologicznych. W toku pandemii COVID-19 RARS skutecznie uruchomiła rezerwy respiratorów, płynów infuzyjnych i materiałów opatrunkowych. Mechanizm funkcjonuje, ale wymaga systemowej reformy. Agencja nie wypracowała dotychczas modelu zaangażowania sektora prywatnego porównywalnego z fińskim systemem poolów. Zakup rezerw następuje głównie przez zamówienia publiczne, nie przez partnerstwo z firmami utrzymującymi zapasy na własny rachunek.

W obszarze cyberbezpieczeństwa Polska dysponuje kilkoma instytucjami i podmiotami o istotnym potencjale. NASK (Naukowa i Akademicka Sieć Komputerowa) łączy funkcje B+R, operatora rejestrów i centrum edukacyjnego; CERT Polska odnotował w 2024 r. ponad 100 000 incydentów. EXATEL, spółka Skarbu Państwa działająca jako operator telekomunikacyjny dla sektora administracji i energetyki, posiada zdolności w obszarze detekcji zagrożeń. Asseco Poland, jedna z największych firm IT w Europie Środkowej, obsługuje systemy dla administracji podatkowej, ZUS i sektora bankowego. Comarch dostarcza systemy dla operatorów energetycznych. To jest infrastruktura myśli i kompetencji, która przy odpowiednim zamówieniu publicznym mogłaby się stać eksportowym rdzeniem polskiego przemysłu odpornościowego – analogiem czeskiego NÚKIB-ekosystemu albo estońskiej sieci Cybernetica–Nortal. Do tego potencjału należy dodać krajowe kompetencje w zakresie integracji systemów, telemetrii, IoT, analizy danych, sztucznej inteligencji, komunikacji kryzysowej, cyberbezpieczeństwa oraz utrzymania infrastruktury technicznej. W połączeniu z potrzebami samorządów, centrów zarządzania kryzysowego, operatorów infrastruktury i systemu ochrony ludności tworzy to podstawę do rozwoju krajowego segmentu technologii monitorowania gotowości zasobów odpornościowych. Segment ten może obejmować zarówno sprzęt, oprogramowanie, usługi integracyjne, serwis, audyt techniczny, jak i standardy danych.

W przemyśle farmaceutycznym Polska posiada zakłady z wieloletnim dorobkiem: Polfa Tarchomin (antybiotyki, heparyny), Adamed (leki kardiologiczne i onkologiczne), Gedeon Richter Polska, zakłady w Kutnie i Pabianicach. Udział krajowej produkcji w zużyciu leków jest jednak niski i to pomimo że Polska należy do państw UE z jednym z najsilniejszych obowiązków utrzymywania zapasów leków refundowanych (3 miesiące)[262]. Paradoks ten: silne zapasy, słaba produkcja, jest dokładnie tym problemem, który próbuje zaadresować Critical Medicines Act przyjęty przez Radę UE 2 grudnia 2025 r. i uzgodniony na poziomie politycznym przez Parlament Europejski 12 maja 2026 r.[263] Ustawa ta wprowadza kategorię „projektów strategicznych" (strategic projects), które mogą korzystać z uproszczonych procedur administracyjnych, pomocy państwa na nowych warunkach i preferencji w zamówieniach publicznych. Polska była wśród państw lobbujących za silniejszym finansowaniem unijnym tych projektów podczas negocjacji Rady[264]. Warto jednak odnotować, że Rada UE w grudniu 2025 r. wykreśliła z tekstu artykuł 4 dotyczący strategicznego celu samowystarczalności, co osłabia obowiązkowy charakter reindustrializacji farmaceutycznej. Realizacja tej ścieżki wymaga od Polski proaktywnego podejścia.

10.4 Implementacja celów odpornościowych poprzez rozwój rodzimych zdolności wytwórczych

Sojusznicze Baseline Requirements for National Resilience – siedem filarów gotowości na wypadek kryzysu przyjętych na Szczycie Warszawskim w 2016 r. i potwierdzonych w Hadze, są użytecznym filtrem do oceny, gdzie krajowa produkcja ma największe strategiczne uzasadnienie.

Ciągłość rządzenia i funkcjonowania służb publicznych wymaga systemów IT, łączności szyfrowanej i oprogramowania zarządzania kryzysowego, które nie mogą zawieść w przypadku sankcji, cyberataku lub zakłócenia łańcucha dostaw. Import gotowych rozwiązań od dostawców spoza UE wprowadza tu ryzyko technologicznej zależności o charakterze egzystencjalnym. Polska powinna rozważyć warunkowanie zamówień na krytyczne systemy IT od wymogów lokalizacji kodu, audytowalności i obowiązku przeniesienia wiedzy do krajowych podmiotów, wzorem wymagań, które BSI nakłada na dostawców systemów rządowych w Niemczech.

Bezpieczne dostawy energii wymagają nie tylko dywersyfikacji źródeł surowcowych, ale i krajowej zdolności do budowy, serwisowania i integracji magazynów energii, systemów smart grid i awaryjnego zasilania. Polska posiada potencjał przemysłowy w tym obszarze: zakłady elektroenergetyczne, firmy inżynieryjne obsługujące PSE i operatorów dystrybucyjnych. Mechanizm zamówień odpornościowych, wzorowany na szwedzkim modelu kontraktowania z firmami prywatnymi utrzymującymi zapasy bezpieczeństwa, mógłby ten potencjał sformalizować i wzmocnić.

Zarządzanie niekontrolowanym przemieszczaniem się ludności oraz zapasy żywności i wody to dwa filary, w których polska produkcja rolno-spożywcza i przemysłowa tworzy naturalną przewagę. Polska jest jednym z największych eksporterów żywności w UE. Problem nie leży w braku zdolności wytwórczych, lecz w braku mechanizmów kontraktowania z RARS, które angażowały by krajowych producentów w system rezerw, podobnie jak NESA angażuje fińskie firmy spożywcze i transportowe w sektorowych poolach. Warto rozważyć wprowadzenie analogicznych umów wieloletnich z polskimi dostawcami w zamian za gwarantowany rynek zbytu na potrzeby rezerw państwowych.

Odporne systemy łączności to obszar, gdzie Estonia jest wzorem niedoścignionym w swojej efektywności kosztowej – ale też gdzie Polska ma szansę zbudować własny profil eksportowy. Systemy X-Road są dziś wdrażane w Ukrainie jako element odbudowy infrastruktury cyfrowej; Polska, jako jeden z kluczowych partnerów Ukrainy w tym procesie, mogłaby współtworzyć polski odpowiednik NIIS (platformy zarządzającej X-Road) lub wdrożyć otwarte narzędzia interoperacyjności w ramach własnej e-administracji, a następnie oferować tę kompetencję państwom partnerskim. Nie jest to spekulacja: NASK i COI mają techniczną zdolność do pełnienia takiej roli; brakuje natomiast decyzji politycznej i dedykowanego programu.

Odporne systemy transportu zamykają katalog. Infrastruktura drogowa i kolejowa o parametrach umożliwiających przemieszczanie sił zbrojnych (nośność mostów, skrajnia tuneli, pojemność terminali) jest inwestycją cywilną z efektem wojskowym i odwrotnie. Polska realizuje tu kilka programów, ale ich spójność z wymaganiami NATO Mobility jest wciąż przedmiotem dyskusji. Kluczowe dla krajowego przemysłu jest to, że zamówienia na tego rodzaju infrastrukturę: mosty, węzły logistyczne, magazyny paliw, powinny być warunkowane polskim wykonawstwem, z transferem technologii i budową lokalnych kompetencji inżynierskich tam, gdzie stosuje się technologię zagraniczną.

10.5 Lokalna treść w zamówieniach odpornościowych

Trzy warunki decydują o tym, czy środki z koszyka odpornościowego rzeczywiście zasilą krajowy przemysł, czy opuszczą Polskę przez kanał importowy.

Po pierwsze, warunek definicyjny: Polska musi aktywnie uczestniczyć w kształtowaniu metodyki NATO dla kategorii 1,5% PKB przed przeglądem w 2029 r. Definicja ta jest wciąż otwarta, a jej ostateczna treść przesądzi, co może być do niej zaliczone i tym samym, jak dużą przestrzeń mają poszczególne państwa na krajową politykę przemysłową. Polska powinna delegować ekspertów do prac NATO i aktywnie promować szeroką definicję obejmującą farmaceutyki, systemy IT i rezerwy rolno-spożywcze.

Po drugie, warunek instytucjonalny: skuteczność każdego modelu odpornościowego, czy to fińskiego, szwedzkiego, czy przyszłego polskiego, zależy od jakości agencji koordynującej. W Polsce RARS wymaga głębokiej reformy zarządczej: wzmocnienia mechanizmów kontroli wewnętrznej, nowego modelu angażowania sektora prywatnego i przekształcenia w podmiot działający bardziej na wzór operatora sieci partnerskiej niż centralnego magazyniera państwa. Warto przy tym rozważyć uniezależnienie finansowania RARS od corocznych decyzji budżetowych, na przykład przez opłatę strategiczną doliczaną do stawek operatorów infrastruktury krytycznej. Wzorzec fiński wskazuje, że takie rozwiązanie jest technicznie i prawnie wykonalne.

Po trzecie, warunek zamówień publicznych: sam fakt istnienia odpowiednich firm krajowych nie przełoży się na ich wzrost, jeśli zamówienia publiczne nadal będą przyznawane wedle kryteriów wyłącznie cenowych, bez klauzul dotyczących lokalizacji produkcji, transferu technologii i udziału krajowych podwykonawców. W tym zakresie warto rozważyć idealny wzorzec stosowany przy kontraktach zbrojeniowych, gdzie rząd warunkowo wiąże zakupy z montażem krajowym, transferem wiedzy inżynierskiej i włączaniem polskich poddostawców. Analogiczna logika powinna być stosowana w zamówieniach na systemy cyberbezpieczeństwa, sprzęt medyczny, instalacje energetyczne i infrastrukturę logistyczną objętą koszykiem odpornościowym.W przypadku technologii cyfrowych i systemów wspierających zarządzanie kryzysowe klauzule lokalnej treści powinny obejmować również lokalny serwis, kontrolę nad danymi, możliwość audytu kodu lub konfiguracji, zdolność utrzymania systemu w kraju, dostępność kompetencji integracyjnych oraz odporność na uzależnienie od pojedynczego zagranicznego dostawcy. W obszarze odporności nie wystarczy zakup systemu; konieczne jest utrzymanie kompetencji pozwalających go rozwijać, integrować, zabezpieczać i naprawiać w warunkach kryzysowych.

W przypadku rozwiązań odpornościowych, które nie istnieją jeszcze na rynku w dojrzałej postaci albo wymagają dostosowania do specyficznych potrzeb państwa, samorządów lub operatorów infrastruktury, należy rozważyć wykorzystanie trybu partnerstwa innowacyjnego. Jest to procedura zamówieniowa pozwalająca zamawiającemu na rozwijanie innowacyjnego produktu, usługi lub robót budowlanych, jeżeli nie są one dostępne na rynku w oczekiwanej postaci. Taki model może służyć budowie nowych zdolności odpornościowych w zespołach łączących administrację publiczną, krajowe firmy technologiczne, uczelnie, instytuty badawcze, operatorów infrastruktury i ekspertów lokalnych.

Partnerstwo innowacyjne jest szczególnie przydatne tam, gdzie celem zamawiającego nie jest zakup gotowego produktu, lecz stworzenie rozwiązania odpowiadającego na złożony problem operacyjny. Dzięki temu zamówienia publiczne mogą stać się instrumentem budowy krajowego przemysłu odpornościowego, a nie wyłącznie mechanizmem zakupu rozwiązań dostępnych u zewnętrznych dostawców.

Równolegle niezbędna jest systematyczna mapa krytycznych zależności importowych w łańcuchach dostaw istotnych dla każdego z siedmiu

filarów. Polska importuje 321 kategorii towarów kluczowych dla gospodarki, ale ta liczba jest punktem wyjścia, nie wnioskiem. Konieczne jest przejście od listy towarów do mapy przyczyn: które zależności wynikają z nieodwracalnej specjalizacji globalnej (np. chipy projektowane wyłącznie na Tajwanie), a które ze zwykłej niskiej rentowności inwestycji krajowych, braków w polityce zamówień publicznych lub niedostosowania regulacji. Dla tych drugich, a należy przyjąć, że jest ich więcej, istnieje przestrzeń działania. Programy dywersyfikacji powinny być prowadzone dwutorowo: przez rozbudowę krajowych zdolności wytwórczych w wybranych segmentach (farmaceutyka, elektronika użytkowa krytyczna, komponenty energetyczne) oraz przez dywersyfikację źródeł zagranicznych, tak by żaden pojedynczy kraj nie dostarczał ponad 65% potrzeb w żadnej kategorii strategicznej, analogicznie do progu zapisanego w unijnym rozporządzeniu o surowcach krytycznych[265].

Istnieje przy tym ryzyko pułapki protekcjonizmu. Zbyt restrykcyjne wymogi krajowe mogą kolidować z prawem zamówień publicznych UE, blokować dostęp do najlepszych dostępnych technologii i generować renty monopolistyczne dla wybranych podmiotów krajowych. Doświadczenia z ochroną sektora elektroenergetycznego w kilku krajach UE pokazują, że granica między uzasadnioną ochroną infrastruktury krytycznej a nieuzasadnionym protekcjonizmem jest cienka. Remedium jest transparentność i proporcjonalność: wymogi krajowe powinny być powiązane z weryfikowalnymi kryteriami bezpieczeństwa (audytowalność kodu, jurysdykcja danych, fizyczna lokalizacja serwerów), a nie z narodowością właściciela firmy.

Strategiczne okno jest otwarte. Zobowiązanie haskie, ustanowienie minimalnego poziomu 0,3% PKB rocznie na gotowość cywilną oraz instrumenty europejskie takie jak Fundusz Bezpieczeństwa i Obrony, tworzą razem wyjątkowy moment legislacyjny i finansowy. Równolegle nadchodzi przegląd trajektorii NATO w 2029 r. i wejście w życie kolejnych aktów prawa UE: Critical Medicines Act, KRITIS-transponowanych regulacji krajowych, Preparedness Union Strategy. Wszystkie te instrumenty stwarzają formalne uzasadnienie dla polityki, w której zakup odporności i budowa krajowych zdolności przemysłowych są jednym działaniem, a nie dwiema konkurującymi pozycjami budżetowymi. Wzorce europejskie wskazują, że nie ma jednej właściwej ścieżki. Finlandia wybrała model pozabudżetowego funduszu zasilanego opłatą od energii i sieci poolów przemysłowych. Szwecja reaktywowała obronę cywilną jako część całkowitej obrony, przy silnym zaangażowaniu społecznym. Estonia zbudowała globalną markę cyfrowej odporności z otwartego kodu i kompetencji eksperckich. Niemcy postawiły na regulację narzucającą obowiązki na operatorów infrastruktury krytycznej, choć jak wskazują krytycy, zbyt ostrożnie podchodząc do współfinansowania po stronie publicznej. Czechy pozwoliły sektorowi prywatnemu rosnąć we własnym tempie, inwestując w jakość regulatora i prestiż krajowej konferencji. Polska ma dostatecznie dużo własnych zasobów: przemysłowych, akademickich, instytucjonalnych, by nie kopiować żadnego z tych modeli wprost, lecz zbudować podejście hybrydowe, odpowiadające jej skali, geopolitycznej pozycji i strukturze gospodarczej. Kluczową decyzją jest to, czy koszyk odpornościowy będzie traktowany jako budżet zakupowy, z naturalną tendencją do importu najtańszego dostępnego produktu, czy jako polityka przemysłowa z wbudowaną logiką bezpieczeństwa. W obecnych warunkach geopolitycznych odpowiedź na to pytanie ma konsekwencje, które wykraczają poza granice jednej kadencji parlamentarnej.

CZĘŚĆ III

Efekty, mierniki i rekomendacje

Jeśli Część I uzasadniała konieczność komponentu 1,5% PKB, a Część II proponowała jego alokację i źródła finansowania, to Część III zamyka logiczny obieg raportu, odpowiadając na pytanie najtrudniejsze i najczęściej pomijane w debacie publicznej: *z jakim skutkiem* te środki zostaną wydane i *w jaki sposób* rozliczyć państwo z ich efektywności. To właśnie tutaj raport mierzy się wprost z ryzykiem przewijającym się przez wcześniejsze rozdziały – groźbą „kreatywnej księgowości", w której rutynowe inwestycje cywilne podaje się za wkład w odporność sojuszniczą, tworząc iluzję bezpieczeństwa bez realnego przyrostu zdolności. Przeciwwagą dla tego ryzyka są dwa filary tej części. Pierwszy to przeformułowanie samej natury wydatków odpornościowych: w świetle modelu potrójnej dywidendy, mnożników fiskalnych i efektów zaufania społecznego nakłady te przestają być kosztem zamrożonym, a stają się policzalną inwestycją o zwrocie realizowanym niezależnie od tego, czy kryzys ostatecznie nastąpi. Drugi filar to zestaw proponowanych mierników efektywności, które przekładają deklaracje polityczne na audytowalne rezultaty zgodne z wymogami Artykułu 3 Traktatu Waszyngtońskiego. Część zamyka katalog propozycji i rekomendacji: kierunki zmian ustawodawczych, koncepcja organu koordynującego, rola samorządów i organizacji pozarządowych, a także rejestr ryzyk wdrożeniowych. Podobnie jak w częściach wcześniejszych, rekomendacje te mają charakter ramy wyjściowej adresowanej do decydentów, a nie zamkniętego planu, świadomie otwartej na uszczegółowienie w toku prac legislacyjnych i uzgodnień międzyresortowych. Ich rolą jest przekucie analizy zawartej w niniejszym raporcie w spójną mapę drogową budowy odporności Rzeczypospolitej w dekadzie 2026–2035.

11 Efekty społeczne i gospodarcze oraz proponowane mierniki efektywności

Elastyczna definicja wydatków w ramach 1,5% PKB rodzi ryzyko klasyfikowania zwykłych inwestycji cywilnych jako wkładu w odporność sojuszniczą. Aby temu zapobiec, program musi opierać się o rygorystyczne mierniki efektywności i odzwierciedlać wymogi Artykułu 3 Traktatu Waszyngtońskiego.

Ryzyko to dotyczy również finansowania zasobów, które istnieją formalnie, lecz nie mają potwierdzonej gotowości operacyjnej. Dlatego mierniki efektywności powinny obejmować nie tylko produkty inwestycyjne, takie jak liczba obiektów, miejsc, systemów lub zakupionych urządzeń, lecz także zdolność ich użycia w scenariuszu kryzysowym: dostępność, sprawność, czas uruchomienia, ciągłość działania, aktualność danych oraz możliwość niezależnej weryfikacji statusu.

11.1 Potrójna dywidenda z odporności

Tradycyjne ujęcie analizy kosztów traktuje wydatki na obronę cywilną jako kapitał zamrożony. Współczesna polityka publiczna korzysta jednak z modelu „Potrójnej Dywidendy z Odporności", opracowanego przez Bank Światowy oraz Global Facility for Disaster Reduction and Recovery (GFDRR)[266]. Model ten dowodzi, że nakłady na prewencję generują zyski zawsze, niezależnie od tego, czy kryzys ostatecznie nastąpi:

- **I dywidenda (uniknięcie strat):** Bezpośrednia ochrona życia i redukcja kosztów zniszczeń infrastruktury.
- **II dywidenda (odblokowanie potencjału):** Bezpieczeństwo redukuje niepewność i ryzyko rynkowe, stymulując inwestycje oraz przedsiębiorczość.
- **III dywidenda (dodatkowe korzyści):** Codzienne zyski z infrastruktury budowanej w modelu podwójnego zastosowania (dual-use).

Badania gospodarcze potwierdzają, że każdy 1 dolar zainwestowany w odporność i przygotowanie do kryzysu pozwala zaoszczędzić aż 13 dolarów w postaci uniknięty zniszczeń i zahamowania spadku PKB.[267]

11.2 Efekty społeczno-gospodarcze wzrostu odporności

Kapitał społeczny to rdzeń odporności. Regularne badania Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dowodzą, że wiara obywateli w skuteczność mechanizmów reagowania kryzysowego zwiększa ogólne zaufanie do instytucji państwowych o 2,4 punktu procentowego. Efekt ten wprost ratuje życie – dane z okresu pandemii COVID-19 z państw OECD udowodniły, że w społeczeństwach cechujących się wyższym poziomem zaufania do administracji śmiertelność była zauważalnie niższa, ponieważ obywatele solidarnie przestrzegali wytycznych[268].

Bezpieczeństwo operacyjne przenosi się na poziom lokalny. Ustawodawstwo umożliwia współfinansowanie inwestycji dla samorządów (dotacje mogą pokryć nawet do 100% kosztów w przypadku budowli ochronnych). Wzmacnia to miasta, zapobiegając szybkiemu paraliżowi struktur terytorialnych w razie wstrząsu.

Efekt lokalny powinien być jednak oceniany nie tylko przez skalę współfinansowania, lecz także przez zdolność samorządu do bieżącego ustalenia, które zasoby pozostają gotowe do użycia. Dotyczy to w szczególności obiektów ochrony ludności, miejsc czasowego pobytu i zakwaterowania ewakuowanych, lokalnych źródeł energii, zasobów wodnych, łączności, logistyki oraz infrastruktury technicznej. Im krótszy czas uzyskania wiarygodnego statusu tych zasobów, tym większa zdolność gminy lub miasta do ograniczenia chaosu organizacyjnego i utrzymania zaufania mieszkańców.

Wydatki 1,5% PKB to potężny impuls fiskalny. Zrewidowane badania Międzynarodowego Funduszu Walutowego udowadniają, że w rzeczywistości kryzysowej mnożnik dla inwestycji publicznych rośnie do wartości od 0,9 do 1,7[269]. Oznacza to, że każda zainwestowana złotówka pomnaża się w gospodarce. W sektorach zaawansowanych technologicznie, takich jak rozbudowa bezpiecznych sieci energetycznych, efekt stymulujący może wynosić kilkaset procent. 10% środków powinno być kierowanych na systemy innowacyjne i uniezależnianie łańcuchów dostaw. Inwestowanie w krajowe technologie kryptograficzne i sztuczną inteligencję (AI) podwójnego zastosowania stymuluje sektor IT. Generuje to tzw. „dywidendę obronną", tworząc wysokopłatne, stabilne miejsca pracy, których nie da się łatwo zdelokalizować.[270]

11.3 Proponowane mierniki efektywności

Odejście od anachronicznego rozliczania środków wymaga oparcia się o mierzalne wskaźniki rezultatów. Poniższe ramy logiczne przeciwdziałają rozmyciu odpowiedzialności:

Wskaźniki powinny być możliwe do zasilania zarówno danymi z audytów, ćwiczeń i przeglądów okresowych, jak i danymi operacyjnymi pochodzącymi z systemów ewidencji, paszportyzacji, monitorowania oraz raportowania gotowości zasobów. Pozwala to ograniczyć rozbieżność między stanem deklarowanym a rzeczywistą zdolnością użycia infrastruktury w kryzysie.

Wydatkowanie zasobów rzędu 1,5% PKB na obronę cywilną nie stanowi wyłącznie kosztu operacyjnego państwa. Zgodnie z modelem Potrójnej Dywidendy, jest to strategiczna polityka reindustrializacji, która obniża makroekonomiczne ryzyko Polski, stymuluje sektor budowlano-technologiczny i buduje zaufanie rządzonych. Bezwzględnym wymogiem sukcesu tej reformy pozostaje twarda ewaluacja nałożona przez KPI oraz wytyczne NATO, uniemożliwiające klasyfikację pozbawionych znaczenia inwestycji jako filarów bezpieczeństwa.

Tabela 11. Przykłady proponowanych mierników efektywności

Kategoria KPI	Wskaźnik	Znaczenie Operacyjne
Produkt	Liczba miejsc schronowych / 1000 mieszkańców	Fizyczny przyrost nowych, certyfikowanych obiektów ochronnych z podziałem na stopień hermetyczności.
Rezultat	% ludności z dostępem w 10/20 minut	Badanie zasięgu na mapach (izochrony). Obywatel musi dotrzeć do schronu pieszo w max. 10 minut w mieście i 20 minut na wsi.
	Czas gotowości obiektów	Weryfikacja, czy obiekt komercyjny osiągnie 100% autonomii (woda, wentylacja) w nałożonym rygorze prawnym 48 godzin.
	Odsetek zasobów z potwierdzonym statusem gotowości	Procent obiektów ochrony ludności, miejsc zakwaterowania ewakuowanych, lokalnych zasobów energii, wody i łączności posiadających aktualny status dostępności, sprawności, pojemności i ograniczeń użycia.
	Czas uzyskania statusu zasobów krytycznych	Czas potrzebny administracji lub centrum zarządzania kryzysowego do uzyskania wiarygodnej informacji o dostępności i sprawności obiektów ochrony ludności, miejsc zakwaterowania, energii, wody, łączności oraz infrastruktury technicznej niezbędnej do ochrony ludności.
Wpływ	Czas przywrócenia usług (RTO – Recovery Time Objective)	Szybkość, z jaką krytyczne usługi (energetyka, szpitale) powracają do działania po cyberataku lub ataku kinetycznym.
	Wyniki testów funkcjonalnych	Regularna ewaluacja odporności systemowej podczas ćwiczeń (np. nordycki model Nordic Pine) oraz dynamiki zachowań społecznych.

12 Propozycje i rekomendacje

12.1 Proponowane zmiany ustawodawcze

Realizacja programu wymaga gruntownej reformy otoczenia prawnego. Obecny stan charakteryzuje się fragmentacją kompetencji, zaległościami implementacyjnymi wobec prawa unijnego oraz brakiem instrumentów zapewniających wieloletnią ciągłość finansowania. Poniżej wskazano kluczowe akty wymagające uchwalenia, nowelizacji lub uzupełnienia o przepisy wykonawcze, uszeregowane według pilności i znaczenia dla operacjonalizacji komponentu 1,5% PKB.

Akty wykonawcze do ustawy o ochronie ludności i obronie cywilnej. Ustawa z 5 grudnia 2024 r., tworzy ramowy fundament systemu, lecz jej skuteczność zależy od terminowego wydania kompletu rozporządzeń wykonawczych. Priorytetem jest doprecyzowanie definicji i klasyfikacji obiektów ochronnych, katalogu wymagań techniczno-sanitarnych oraz – co kluczowe dla samorządów – trwałych mechanizmów dotacji celowych na zadania zlecone, sięgających do 100% kosztów wzmocnień w obiektach dual-use.

Nowelizacja prawa budowlanego i warunków technicznych. Nałożenie obowiązku projektowania schronów w nowych inwestycjach wielorodzinnych i obiektach użyteczności publicznej wymaga osadzenia norm technicznych bezpośrednio w rozporządzeniu w sprawie warunków technicznych, jakim powinny odpowiadać budynki. Należy skodyfikować normatywy metrażowe, wymogi wentylacyjne, hermetyczności i zasilania awaryjnego, a także procedury odbioru i certyfikacji, tak aby standard ochronny był weryfikowalny na etapie pozwolenia na użytkowanie, a nie deklaratywny.

Nowelizacja ustawy o rezerwach strategicznych. Rozszerzenie i uelastycznienie mandatu Rządowej Agencji Rezerw Strategicznych powinno objąć zdefiniowanie minimalnych poziomów rezerw produktów leczniczych, wyrobów medycznych, żywności i paliw, mechanizmy ich rotacji zapobiegające przeterminowaniu oraz reguły współpracy z sektorem prywatnym w modelu rezerw kontraktowanych. Celem jest przejście od rezerw doraźnych do trwałego, audytowalnego systemu odporności zaopatrzeniowej.

Regulacja ciągłości systemu ochrony zdrowia w warunkach kryzysu. Operacjonalizacja koncepcji szpitali podwójnego zastosowania wymaga nowelizacji ustaw regulujących działalność leczniczą oraz Państwowe Ratownictwo Medyczne o przepisy dotyczące trybu pracy w stanie zagrożenia, protokołów relokacji pacjentów,

ochrony placówek zgodnie z międzynarodowym prawem humanitarnym oraz cyberbezpieczeństwa danych medycznych.

Ustanowienie wieloletnich ram finansowania. Najpoważniejszym ryzykiem dla całego programu jest jego rozliczanie w rocznej perspektywie budżetowej, narażającej nakłady odpornościowe na cięcia w pierwszej kolejności. Zasadne jest ustanowienie odrębnego instrumentu – funduszu celowego lub ustawy o finansowaniu zadań odpornościowych – który zabezpieczy ciągłość komponentu 1,5% PKB w horyzoncie planowania obronnego NATO (2026–2035), z mechanizmem zasady dodatkowości uniemożliwiającym substytucję wydatków bieżących.

Wskazane zmiany powinny być wprowadzane sekwencyjnie: w pierwszej kolejności akty wykonawcze i nowelizacje domykające zaległości implementacyjne wobec prawa UE, następnie regulacje sektorowe (zdrowie, rezerwy), a równolegle – jako warunek trwałości – ramy finansowania wieloletniego.

12.2 Organ koordynujący – Rada ds. Odporności

Propozycją usprawnienia koordynacji jest powołanie Rady ds. Odporności jako organu koordynującego wydatkowanie komponentu 1,5% PKB. Rada powinna działać przy Kancelarii Prezesa Rady Ministrów i skupiać przedstawicieli kluczowych resortów (MON, MSWiA, MZ, MF, MRiT), służb specjalnych, samorządów oraz środowisko ekspertów. Do jej zadań należałoby planowanie, monitoring i ewaluacja alokacji środków, a także pełnienie roli strażnika katalogu wydatków kwalifikowanych, zdefiniowanego w części wcześniejszej niniejszego raportu. Fundamentalne wyzwanie realizacji komponentu 1,5% PKB, sygnalizowana już we wstępie do raportu, polega na tym, że odporność cywilna, w odróżnieniu od precyzyjnie skatalogowanych zdolności wojskowych, jest pojęciem rozproszonym pomiędzy budżetami wielu resortów. Schrony pozostają w gestii MSWiA i samorządów, infrastruktura krytyczna dzieli się między Rządowe Centrum Bezpieczeństwa, ministerstwa sektorowe i operatorów, cyberbezpieczeństwo łączy kompetencje MC, NASK i służb, rezerwy strategiczne podlegają RARS, a ciągłość ochrony zdrowia – MZ. W modelu resortowym (silosowym) każdy z tych podmiotów optymalizuje własny wycinek, lecz nikt nie odpowiada za odporność państwa jako całości. Skutkiem są luki na styku kompetencji, dublowanie inwestycji oraz, co raport identyfikuje jako ryzyko kluczowe, podatność na „kreatywną księgowość", w której rozproszenie odpowiedzialności uniemożliwia rozliczenie efektu zbiorczego.

Podejście *whole-of-government* (zintegrowanego działania administracji) odwraca tę logikę: traktuje odporność jako cel horyzontalny, nadrzędny wobec podziałów resortowych, którego realizacja wymaga wspólnego planowania, jednolitej metodyki sprawozdawczej i jednego ośrodka rozliczalności. Nie chodzi o centralizację wykonawstwa – zadania pozostają w kompetencji poszczególnych resortów i samorządów, lecz o koordynację strategiczną, która zapewnia, że nakłady wszystkich uczestników składają się na spójny, mierzalny przyrost zdolności. To właśnie ten paradygmat leży u podstaw natowskiego Artykułu 3 oraz siedmiu Baseline Requirements, które zakładają, że odporność jest wypadkową skoordynowanego wysiłku całego aparatu państwa, a nie sumą niezależnych działań sektorowych.

Sprawdzonym odniesieniem jest fiński model „bezpieczeństwa kompleksowego" (comprehensive security) z Komitetem Bezpieczeństwa koordynującym współdziałanie administracji, sił zbrojnych, sektora prywatnego i organizacji społecznych[271], a także szwedzka koncepcja „obrony totalnej" (totalförsvar), integrująca wymiar wojskowy i cywilny w jednym systemie planowania[272]. Wspólnym mianownikiem obu rozwiązań jest istnienie trwałego, ponadresortowego

ośrodka, który nadaje kierunek i egzekwuje spójność, nie zastępując przy tym wykonawców.

Lokalizacja przy KPRM zapewnia Radzie pozycję ponad podziałami resortowymi oraz bezpośrednie umocowanie polityczne na poziomie szefa rządu, warunek konieczny skuteczności w modelu *whole-of-government*. Do zadań Rady należałoby: (1) opracowanie i coroczna aktualizacja zintegrowanego planu wydatków 1,5% PKB w horyzoncie wieloletnim, zsynchronizowanego z cyklem planowania obronnego NATO; (2) prowadzenie jednolitego rejestru projektów i sprawozdawczości w oparciu o wspólne mierniki efektywności; (3) weryfikacja kwalifikowalności wydatków zgłaszanych przez resorty, zapobiegająca podciąganiu rutynowych inwestycji pod kategorię odporności; (4) identyfikacja luk i nakładania się kompetencji oraz rekomendowanie korekt alokacji; (5) ewaluacja efektów na podstawie ćwiczeń funkcjonalnych i testów systemowych.

Skuteczna odporność nie zamyka się w granicach administracji. Dlatego podejście whole-of-government powinno być pomyślane jako rdzeń szerszego modelu *whole-of-society*, w którym Rada pełni rolę interfejsu między państwem a samorządami, sektorem prywatnym (operatorzy infrastruktury krytycznej, przemysł odpornościowy), organizacjami pozarządowymi i obywatelami. Ten wymiar, rola samorządów i NGO, rozwinięto w kolejnych podrozdziałach, które należy czytać jako uszczegółowienie społecznego komponentu architektury koordynacyjnej zarysowanej w niniejszym punkcie.

12.3 Organ koordynujący – Minister ds. Odporności

Jednocześnie proponuje się powołanie stanowiska Ministra ds. Odporności jako organu koordynującego działania zapobiegające sytuacjom kryzysowym, katastrofom i innym zdarzeniom zagrażającym funkcjonowaniu państwa i społeczeństwa, Wzorce międzynarodowe można odnaleźć w Danii (Minister of Resilience and Preparedness) czy Szwecji (Minister for Civil Defence).

Minister powinien być odpowiedzialny m.in. za reagowanie i zarządzanie kryzysowe w ścisłej współpracy z właściwymi resortami oraz sektorami, a także za monitorowanie alokacji środków przeznaczanych na odporność państwa. Stanowisko to stanowiłoby bezpośrednią kontynuację oraz instytucjonalne rozwinięcie prac nowo powołanego Pełnomocnika Rządu do spraw Wzmocnienia Odporności Państwa[273], zapewniając trwałość prowadzonych działań i skuteczniejszą koordynację polityki odporności na poziomie całej administracji publicznej. Utworzenie zintegrowanego resortu sprzyjałoby konsolidacji działań podejmowanych w obszarach bezpieczeństwa militarnego i cywilnego, ochrony ludności, infrastruktury krytycznej, cyberbezpieczeństwa oraz ciągłości funkcjonowania państwa w obliczu współczesnych zagrożeń hybrydowych i sytuacji nadzwyczajnych.

12.4 Rola samorządu terytorialnego

Samorządy terytorialne odgrywają kluczową rolę w systemie gotowości cywilnej. To one stanowią pierwszą linię reagowania w sytuacji kryzysowej, dysponują wiedzą o lokalnych uwarunkowaniach i zarządzają znaczną częścią infrastruktury nadającej się do adaptacji ochronnej, szkołami, halami sportowymi, parkingami podziemnymi czy obiektami komunalnymi, które w modelu podwójnego zastosowania mogą pełnić funkcję miejsc doraźnego schronienia. Ustawa o ochronie ludności i obronie cywilnej czyni z jednostek samorządu terytorialnego głównego wykonawcę zadań z zakresu budowli ochronnych i planowania ewakuacji, co wymaga adekwatnego i przewidywalnego modelu finansowania.

Model ten powinien opierać się na trzech filarach. Pierwszym są dotacje celowe na zadania zlecone: budowę i utrzymanie schronów oraz planowanie ewakuacji, pokrywające, zgodnie z konstrukcją ustawową, nawet do 100% kosztów. Mechanizm ten realizowany jest już częściowo poprzez program „Ochrona Ludności i Obrona Cywilna", w którym szacunkowo 80–90% środków kierowanych jest bezpośrednio do JST. Drugim filarem powinny być mechanizmy zachęt dla gmin inwestujących w gotowość ponad wymagane minimum – premie finansowe, podwyższone stopy współfinansowania lub priorytet w dostępie do funduszy dla samorządów osiągających określone wskaźniki pokrycia (np. odsetek mieszkańców z dostępem do schronu w czasie dojścia pieszego). Trzecim filarem są wspólne zamówienia grupowe prowadzone przez centrale zakupowe (na poziomie powiatu lub województwa), agregujące popyt wielu gmin na typowe komponenty infrastruktury odpornościowej: agregaty, systemy wentylacji hermetycznej, drzwi gazoszczelne, magazyny energii, co obniża koszty jednostkowe i standaryzuje jakość.

Kluczowym warunkiem powodzenia tego modelu jest jednak uwzględnienie zróżnicowanej zdolności absorpcyjnej samorządów. Doświadczenia z pierwszego okresu obowiązywania ustawy pokazują, że mniejsze gminy, zwłaszcza wiejskie, nie nadążają z wykorzystaniem przyznanych środków z powodu braków kadrowych i administracyjnych, co prowadzi do zwrotu lub przesuwania niewykorzystanych dotacji. Aby środki rzeczywiście przełożyły się na odporność, model finansowania musi być uzupełniony o wsparcie pozafinansowe: gotowe wzorce projektowe i specyfikacje techniczne schronów, doradztwo inżynieryjne organizowane na poziomie regionalnym oraz uproszczone procedury sprawozdawcze. W tej roli naturalnym ogniwem koordynującym pozostaje Rada ds. Odporności, która powinna pełnić funkcję interfejsu między poziomem centralnym a samorządowym, zapewniając spójność standardów i sprawiedliwy podział środków między ośrodki o różnym potencjale.

12.5 Rola organizacji pozarządowych

Organizacje pozarządowe (NGO) stanowią niezbędny element systemu reagowania kryzysowego. W modelu *whole-of-society*, omówionym w pkt 12.2, państwo nie jest jedynym gwarantem odporności – jej rzeczywistą głębię tworzy gęsta sieć podmiotów społecznych zdolnych do działania w pierwszych, krytycznych godzinach kryzysu, zanim uruchomione zostaną pełne zasoby administracji. Doświadczenia nordyckie potwierdzają wartość tego podejścia: w fińskim modelu kompleksowego bezpieczeństwa oraz szwedzkiej obronie totalnej organizacje ochotnicze mają status formalnego ogniwa systemu, z przypisanymi zadaniami, finansowaniem i miejscem w planach obronnych. Polski potencjał w tym obszarze: od Ochotniczych Straży Pożarnych, przez organizacje harcerskie, po wyspecjalizowane fundacje ratownicze i humanitarne, jest znaczący, lecz dotychczas wykorzystywany w sposób doraźny i niesystemowy.

Rola sektora pozarządowego obejmuje cztery podstawowe obszary. Pierwszym jest edukacja i szkolenie, prowadzenie lokalnych akcji podnoszących świadomość zagrożeń oraz umiejętności samopomocy, stanowiących uzupełnienie programów szkoleniowych dla obywateli. Drugim jest wsparcie logistyczne dla służb ratowniczych: zaplecze osobowe, transportowe i magazynowe, zwłaszcza w sytuacjach przekraczających doraźne zdolności służb państwowych. Trzecim i szczególnie istotnym – jest opieka nad grupami wrażliwymi (seniorami, osobami z niepełnosprawnościami, dziećmi), które w sytuacji kryzysowej wymagają zindywidualizowanego wsparcia, jakiego zestandaryzowane procedury państwowe często nie są w stanie zapewnić. Czwartym obszarem jest monitorowanie i rzecznictwo na rzecz praw obywateli w kontekście odporności: funkcja kontrolna, dbająca o to, by działania na rzecz bezpieczeństwa pozostawały proporcjonalne i zgodne z prawami podstawowymi.

Aby ten potencjał przełożył się na realną zdolność operacyjną, program powinien przewidywać trzy mechanizmy włączenia. Pierwszym jest kontraktowanie zadań publicznych z organizacjami pozarządowymi, w oparciu o przepisy o działalności pożytku publicznego i wolontariaciem zapewniając stabilne, wieloletnie finansowanie zadań z zakresu gotowości, a nie jedynie jednorazowe granty. Drugim jest integracja NGO w krajowych i lokalnych planach zarządzania kryzysowego, tak by ich zasoby i kompetencje były ujęte w oficjalnych procedurach reagowania, z jasno przypisanymi rolami i ścieżkami uruchamiania. Trzecim jest zapewnienie dostępu do ćwiczeń i szkoleń organizowanych przez służby państwowe, wspólne ćwiczenia funkcjonalne (na wzór nordyckich ćwiczeń obrony totalnej) są jedynym sposobem zweryfikowania, czy współdziałanie administracji i sektora społecznego rzeczywiście funkcjonuje pod presją, a nie tylko na papierze.

Koordynację współpracy z sektorem pozarządowym, kontraktowania, planowania i ewaluacji wspólnych ćwiczeń – powinna zapewniać Rada ds. Odporności, traktując NGO jako pełnoprawnego partnera architektury odpornościowej, a nie wyłącznie wykonawcę zadań zleconych.

Przypisy końcowe

1 Defence Spending: Who Is Doing What? International Centre for Defence and Security, 2025, https://icds.ee/en/defence-spending-who-is-doing-what-september-2025/
2 https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/8ee4bbb6-6bde-481c-bc43-1455f0e45fd7-KWP_2310.pdf
3 https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal
4 Janes (dawniej znane jako Jane's Information Group) to renomowany, brytyjski ośrodek analityczny typu wywiad z otwartych źródeł (OSINT). Specjalizuje się w analizie i dostarczaniu rzetelnych danych na temat obronności, sprzętu wojskowego, sił zbrojnych, przestrzeni powietrznej, bezpieczeństwa morskiego oraz rynków zbrojeniowych na całym świecie.
5 Zob. https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf
6 J. Kupiński, Odporność państwa w kontekście bezpieczeństwa narodowego – ujęcie teoretyczne, „Bezpieczeństwo. Teoria i praktyka", 2025, nr 2, s. 139.
7 Infosecurity24, Jak wygląda polska odporność?, 2023, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc
8 DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE , s. 13.
9 NATO, Resilience, civil preparedness and Article 3, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3#heading-0
10 IEA, Ukraine's Energy Security: A Pre-Winter Assessment, October 2025; Kyiv School of Economics
11 https://defence24.pl/polityka-obronna/strategiczny-kabel-telekomunikacyjny-na-baltyku-uszkodzony
12 https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/
13 NATO, Vilnius Summit Communique, 11 July 2023, paragraf 65.
14 https://www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security
15 NATO, Washington Summit Communique, 9-10 July 2024.
16 CERT Polska, Raport Roczny 2024; NASK, 2024
17 CSIRT GOV, dane za 2024 r.;
18 https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/
19 ENISA, Threat Landscape 2024, 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
20 https://edz.bib.uni-mannheim.de/edz/pdf/swd/2021/swd-2021-0352-en.pdf
21 https://ec.europa.eu/commission/presscorner/api/files/attachment/874736/Factsheet_GD_European%20Critical%20Raw%20Materials%20Act%20.pdf
22 https://pie.net.pl/numer-11-2025-20-marca-2025/
23 Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949, ICRC, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949?activeTab=1949GCs-APs-and-commentaries
24 Protocol Additional to the Geneva Conventions of 12 August 1949, and of the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, ICRC, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=
25 Violence Aimed at Spreading Terror among the Civilian Population, ICRC, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule2
26 The Sendai Framework Terminology on Disaster Risk Reduction, United Nations Office for Disaster Risk Reduction (UNDRR), 2017, https://www.undrr.org/terminology/disaster
27 Disaster Risk Reduction Terminology, United Nations Office for Disaster Risk Reduction (UNDRR),
28 General Definitions and Concepts, EM-DAT Documentation, https://www.undrr.org/drr-glossary/terminology https://doc.emdat.be/docs/data-structure-and-content/general-definitions-and-concepts/
29 A. Żebrowski, I. Szkurłat, Zagrożenia dla ludności cywilnej w globalnym środowisku bezpieczeństwa. Wybrane aspekty, „Rocznik Nauk Społecznych" 2024, t. 16, nr 1, s. 33-34.
30 Ibidem, s. 36-39.
31 Natural disaster, United Nations, https://unterm.un.org/unterm2/en/view/UNHQ/70B287180C5658B885257ABF005660DC
32 Natural Disasters, NYU School of Global Public Health, https://publichealth.nyu.edu/explore/what-is-climate-change/natural-disasters
33 Disaster Year in Review 2024, UCLouvain-CRED, 05.2025, https://files.emdat.be/2025/05/CredCrunch78.pdf
34 Coronavirus disease (COVID-19) pandemic, World Health Organization Europe, https://www.who.int/europe/emergencies/situations/covid-19
35 S. Lietaer et al., Blind Spots in Belgian Flood Risk Governance: The Case of the Summer 2021 Floods in Wallonia, United Nations University Research Report, 2024, https://cris.unu.edu/sites/cris.unu.edu/files/UNU-CRIS_Research-Report_2402_0.pdf
36 Pakistan Floods 2022. Post-Disaster Needs Assessment, Ministry of Planning Development & Special Initiatives, 10.2022, https://www.undp.org/pakistan/publications/pakistan-floods-2022-post-disaster-needs-assessment-pdna
37 2022 Pakistan floods: 1700 killed and millions affected, British Red Cross, https://www.redcross.org.uk/stories/disasters-and-emergencies/world/climate-change-and-pakistan-flooding-affecting-millions
38 I. Nabi, Responding to Pakistan floods, Brookings, 10.02.2023, https://www.brookings.edu/articles/pakistan-floods/
39 January 2025 Los Angeles County Wildfires, Congress.gov, 16.01.2025, https://www.congress.gov/crs-product/IF12871
40 J. McKoy, Death Count for 2025 LA County Wildfires Likely Higher than Records Show, BU Research Finds, Boston University, 12.08.2025, https://www.bu.edu/articles/2025/death-count-california-wildfires-higher-than-recorded/
41 Untersuchungsausschuss Flutkatastrophe Nordrhein-Westfalen, Abschlussbericht, 2023
42 UNOCHA, Flash Appeal Turkey-Syria Earthquake, 2023
43 Overview 2023: Greece – Lessons Not Learned, International Association of Wildland Fire, 2023, https://www.iawfonline.org/article/overview-2023-greece/
44 Technological disasters, UCLouvain, 09.2020, https://www.cred.be/sites/default/files/cc60.pdf
45 Major Engineering Disasters from the Past Decade, Case Western Reserve University, 12.03.2026, https://online-engineering.case.edu/blog/disastrous-engineering-failures-due-to-ethics; 2021 Texas Power Grid Failure – a preventable disaster, University of Michigan, 27.12.2024, https://limos.engin.umich.edu/deitabase/2024/12/27/2021-texas-power-grid-failure/
46 P. Donati, The prediction of social catastrophes: Between necessity and contingency, „Journal for the Theory of Social Behaviour" 2023, vol. 54, no. 1, p. 270.

47 G. Buldioski, How Civil Society Can Strengthen Europe's Preparedness and Defence, Visegrad Insight, 28.10.2025, https://visegradinsight.eu/app/uploads/2025/10/How_Civil_Society_Can_Strengthen_Preparedness-and-Defence_Goran-Buldioski_Visegrad_Insight-Policy_-Brief.pdf

48 War without End. Deterring Russia's Shadow War, Center for European Policy Analysis, 04.2026, https://cepa.org/wp-content/uploads/2026/03/CEPA-Russia-Shadow-War-3.26.26.pdf

49 Działania w Rosji mają różnorodne „wariacje", jednak łączy je charakter „poniżej poziomu eskalacji", rozproszenie oraz trudność w jednoznacznej atrybucji. Co istotne, w swojej doktrynie Rosja zasadniczo nie rozpoznaje jasnych granic pomiędzy wojną i pokojem, a także zagrożeniami wewnętrznymi i zewnętrznymi. Jak wskazuje cytowany wcześniej raport CEPA, dla Kremla wojna w Ukrainie, działania na terytorium Europy oraz represje wobec opozycjonistów w samej Rosji nie są oddzielnymi „konfliktami", ale tworzą wspólny, płynny i elastyczny front. „Wojna z cienia" jest w tej sytuacji uzupełnieniem zdolności konwencjonalnych i ma je uzupełniać, m.in. poprzez: wykorzystanie powiązań ideologicznych czy przestępczych w Europie (proxies, kontakt z organizacjami, partiami politycznymi, itp.), sabotaż i manipulację infrastrukturą krytyczną oraz działania w przestrzeni cyfrowej.

50 The Climate Dictionary: An everyday guide to climate change, UNDP, 02.02.2023, http://atepromise.undp.org/news-and-stories/climate-dictionary-everyday-guide-climate-change

51 Climate Migration, DGAP, https://dgap.org/en/research/glossary/climate-foreign-policy/climate-migration

52 C3S/ECMWF i WMO, European State of the Climate 2024, kwiecień 2025, https://climate.copernicus.eu/esotc/2024

53 T. Janoš et al., Heat-related mortality in Europe during 2024 and health emergency forecasting to reduce preventable deaths, „Nature Medicine", wrzesień 2025, https://www.nature.com/articles/s41591-025-03954-7

54 London School of Hygiene & Tropical Medicine / Imperial College London, Climate change-driven summer heat caused 16,500 additional deaths across Europe, wrzesień 2025, https://www.lshtm.ac.uk/newsevents/news/2025/climate-change-driven-summer-heat-caused-16500-additional-deaths-across-europe

55 EEA, Economic losses from weather- and climate-related extremes in Europe, październik 2025, https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related

56 EEA, Climate risks to the economy, Europe's environment 2025, wrzesień 2025, https://www.eea.europa.eu/en/europe-environment-2025/thematic-briefings/climate-change/climate-risks-to-the-economy

57 S. Usman et al. (University of Mannheim & European Central Bank), Dry-roasted NUTS: early estimates of the regional impact of 2025 extreme weather, „European Economic Review", wrzesień 2025, https://www.uni-mannheim.de/en/news/extreme-weather-events-in-summer-2025-europe-faces-long-term-losses-of-126-billion-euros/

58 EEA, Water and climate impacts, Europe's environment 2025, wrzesień 2025, https://www.eea.europa.eu/en/europe-environment-2025/thematic-briefings/biodiversity-and-ecosystems/water-and-climate-impacts

59 EEA, Drought impact on ecosystems in Europe, grudzień 2025, https://www.eea.europa.eu/en/analysis/indicators/drought-impact-on-ecosystems-in-europe

60 EEA, European Climate Risk Assessment (EUCRA), EEA Report No 1/2024, https://www.eea.europa.eu/publications/european-climate-risk-assessment

61 https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/729467/EPRS_BRI(2022)729467_EN.pdf

62 https://www.bruegel.org/analysis/defence-and-climate-seven-points-common-agenda

63 https://institutdelors.eu/content/uploads/2026/03/PP321_Study_Defence_Climate_Matelly.pdf

64 ENISA Sectorial Threat Landscape: Public Administration, European Agency for Cybersecurity, 11.2025, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Public%20Administration%20TL%202024%20-%20v1.2.pdf

65 R. L Hostis, EU struggles to protect itself from cyberattacks, Euranet Plus, 22.01.2026, https://euranetplus-inside.eu/eu-struggles-to-protect-itself-from-cyberattacks/

66 S. Custer, D. Mathew, B. Burgess i in., Ukraine: Measuring civic space risk, resilience, and Russian influence in the lead up to war, AidData, 2023, https://www.aiddata.org/publications/ukraine-measuring-civic-space-risk-resilience-and-russian-influence-in-the-lead-up-to-war

67 Defence Expenditure of NATO Countries (2014-2025)Defence Expenditure of NATO Countries (2014-2025), NATO, 2026, https://www.nato.int/content/dam/nato/webready/documents/finance/def-exp-2025-en.pdf

68 MH Government, UK Government Resilience Action Plan, 2025, https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html#annex-d-acronyms-and-definitions

69 https://www.gov.uk/government/news/uk-to-deliver-on-5-nato-pledge-as-government-drives-greater-security-for-working-people

70 Institute for Fiscal Studies, UK Defence Spending: Composition, Commitments and Challenges, Zielona Księga IFS, 2025, https://ifs.org.uk/publications/uk-defence-spending-composition-commitments-and-challenges

71 UK Defence Expenditure, CBP-8175, House of Commons Library, 2025, Raport opisuje nowy dwuwarstwowy model jako „new two-part definition of defence spending", w którym szacowany udział łączny wyniesie „at least 4.1% of GDP in 2027", https://commonslibrary.parliament.uk/research-briefings/cbp-8175/

72 Strategic Defence Review 2025: Key Points and Paper Series, CBP-10406, House of Commons Library, 2025, https://commonslibrary.parliament.uk/research-briefings/cbp-10406/

73 UK Budget 2025: Government Reconfirms Defence Spending Increase, Pinsent Masons, 2025, https://www.pinsentmasons.com/out-law/news/government-reconfirms-defence-spending-increase

74 UK Defence Spending, Institute for Government, 2025, https://www.instituteforgovernment.org.uk/explainer/uk-defence-spending

75 Resilienzstrategie, Bundesministerium des Innern, 2022, https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/resilienzstrategie/resilienzstrategie-node.html#:~:text=Die%20Strategie%20zur%20St%C3%A4rkung%20der%20Resilienz%20gegen%C3%BCber%20Katastrophen%20(kurz:%20Resilienzstrategie,Gemeinwesens%20gegen%C3%BCber%20Katastrophen%20zu%20st%C3%A4rken.

76 Fiscal Foundations for the Coming Years: German Government Adopts 2025 Federal Budget and €500bn Investment Package, Bundesministerium der Finanzen, komunikat prasowy, 2025 r. https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2025/2025-06-24-2-government-draft-2025-federal-budget.html

77 https://www.bundesfinanzministerium.de/Monatsberichte/Ausgabe/2026/04/Inhalte/Kapitel-2-Analysen/2-1-svik-zusaetzlichkeit-der-investitionen.html).

78 Business Sweden, Germany's Record Defence Modernisation Drive, 2025, https://www.business-sweden.com/insights/blogs/germany-a-new-era-for-investment/germanys-record-defence-modernisation-drive

79 Clean Energy Wire, Germany's New Budget Plans See Defence Spending Boost, Energy Cost Cuts, https://www.cleanenergywire.org/news/germanys-new-budget-plans-see-defence-spending-boost-energy-cost-cuts

80 Bertelsmann Stiftung Europe, What's in a Number? Making NATO's 1.5% Spending Goal Work for European Resilience, 2025 r.

81 NATIONAL STRATEGIC REVIEW 2025, Secrétariat général de la défense et de la sécurité nationale, 2025, s. 37

82 EU Member States' Defence Budgets, ATA(2025)772846, Parlament Europejski, 2025, https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772846/EPRS_ATA(2025)772846_EN.pdf

83 HM Government / MoD, International Defence 2025 (fn. 2). Raport techniczny NATO wyjaśnia: „From 2009 French defence expenditure excludes the Gendarmerie which is now financed separately by the Ministry of the Interior. This change more accurately reflects the NATO definition for defence expenditure, but has led to lower levels of defence spending."

84 Bertelsmann Stiftung Europe, What's in a Number? ... op. cit.
85 Veiligheidsstrategie voor het Koninkrijk der Nederlanden, Rijksoverheid, 2023, s. 40.
86 https://www.government.nl/latest/news/2025/06/13/the-netherlands-supports-nato-5-target
87 Bertelsmann Stiftung Europe, ... op. cit.
88 Resilience in the context national security, Departamento de Seguridad Nacional, 2024, s. 10- 12.
89 Estrategia de Seguridad Nacional 2021,Departamento de Seguridad Nacional, 2021 s. 20.
90 Resilience, U. S. Department of Homeland Security, 2026, https://www.dhs.gov/topics/resilience
91 Taking the Pulse: Does Meeting the 5 Percent of GDP Target Enable Europe to Confront the Russian Threat?, Carnegie Endowment for International Peace / Strategic Europe, 2025, https://carnegieendowment.org/europe/strategic-europe/2025/06/taking-the-pulse
92 Euronews, Defence Spending: Which EU Countries Are on Course to Hit NATO's 5% of GDP Target?, 2025,https://www.euronews.com/my-europe/2025/09/04/defence-spending-which-eu-countries-are-on-course-to-hit-natos-35-of-gdp-target
93 Bertelsmann Stiftung Europe, ... op. cit.
94 Can Europe Deliver NATO's Five Percent?, Intereconomics, 2026, https://www.intereconomics.eu/contents/year/2026/number/2/article/can-europe-deliver-nato-s-five-percent.html
95 NATO's New Spending Target: Challenges and Risks Associated with a Political Signal, SIPRI, 2025, https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal
96 NATO's 5% Defense Mandate Exposes Europe's Creative Accounting, Washington Times, 2025, https://www.washingtontimes.com/news/2025/sep/8/natos-5-defense-mandate-exposes-europes-creative-accounting/
97 NATO, The Hague Summit Declaration, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration
98 https://www.rte.ie/news/2025/0625/1520200-nato-funding-explainer/
99 Department of State USA, Whitaker briefing, Cytat: „We would expect Allies to be even more vigilant in holding each other accountable for year-on-year progress.
100 NATO, Overview – 2025 NATO Summit in The Hague: https://www.nato.int/en/news-and-events/events/2025/6/overview---2025-nato-summit-in-the-hague. Dane: w 2025 r. wszyscy sojusznicy osiągnęli lub przekroczyli próg 2%; europejscy sojusznicy i Kanada zwiększyli wydatki o 20% r/r; łączne wydatki europejskie i kanadyjskie: powyżej 574 mld USD (ceny z 2021 r.).
101 Janes, „Analysis: NATO leaders agree to invest 5% of GDP on defence and security by 2035", Brooks Tigner, 2025, https://www.janes.com/defence-intelligence-insights/defence-and-national-security-analysis/nato-leaders-agree-to-invest-5-of-gdp-on-defence-and-security-by-2035
102 Kramer, Binnendijk, Atlantic Council, op. cit. Szacunek: 1,5% PKB liczonego NATO (~55 bln USD) = ok. 825 mld USD rocznie; dla członków poza USA (~26 bln USD) = ok. 390 mld USD
103 Helena Quis, Torben Schutz, „What's in a Number? Making NATO's 1.5% Spending Goal Work for European Resilience", Bertelsmann Stiftung Europe, 17 czerwca 2025 r. (aktualizacja 27 sierpnia 2025 r.): https://bst-europe.eu/security-policy/whats-in-a-number-making-natos-1-5-spending-goal-work-for-european-resilience/
104 Lorenzo Scarazzato, Diego Lopes da Silva, Nan Tian, Xiao Liang, „NATO's new spending target: challenges and risks associated with a political signal", SIPRI Commentary/Essay, 2025 r.: https://www.sipri.org/commentary/essay/2025/natos-new-spending-target-challenges-and-risks-associated-political-signal
105 Carlo Bastasin, „Europe's difficult trade-off between military and welfare spending: the Italian case", Brookings Institution, 2025, https://www.brookings.edu/articles/europes-difficult-trade-off-between-military-and-welfare-spending-the-italian-case/
106 Washington Times, „NATO's 5% defense mandate exposes Europe's creative accounting", 2025, https://www.washingtontimes.com/news/2025/sep/8/natos-5-defense-mandate-exposes-europes-creative-accounting/
107 Quis, Schutz, Bertelsmann Stiftung Europe, op. cit. Cytat: „national fire brigades or childcare costs for defence personnel have been counted as defence-related spending. Some of these costs, currently claimed under the 2%, may be more appropriately assigned to the future 1.5% category, if guidelines were clear.
108 Bohmelt, „Can Europe Deliver NATO's Five Percent?", Intereconomics, 2026, https://www.intereconomics.eu/contents/year/2026/number/2/article/can-europe-deliver-nato-s-five-percent.html.
109 SIPRI Fact Sheet, „Trends in World Military Expenditure, 2025", kwiecien 2026 r.: https://www.sipri.org/sites/default/files/2026-04/2604_milex_2025.pdf. Cytat: „inflated or inconsistently defined military spending figures may misrepresent NATO members' actual military capability and distort assessments of the balance of forces, potentially shaping threat perceptions and capability development based on spending levels that do not accurately reflect operational capacity."
110 Quis, Schutz, Bertelsmann Stiftung Europe, op. cit. Trzy ryzyka strategiczne: (1) creative accounting; (2) opportunistic prioritisation; (3) brak koordynacji transgranicznej.
111 Tamze. Cytat: „the pressure to meet spending targets quickly may lead to opportunistic prioritisation. Instead of addressing actual resilience and defence needs, countries may focus on areas where funding or planning and industrial capacity is available. Germany's experience with its military special fund, where availability of capacity shaped spending more than strategic gaps, illustrates this risk."
112 DSEI, „The end nears for Germany's special defence fund. New Chancellor, new investment?", 2025, https://www.dsei.co.uk/news/end-nears-germanys-special-defence-fund-new-chancellor-new-investment
113 Lucie Beraud-Sudreau, „Explainer: The proposed hike in German military spending", SIPRI Commentary, 2022 r.: https://www.sipri.org/commentary/blog/2022/explainer-proposed-hike-german-military-spending. Cytat: „If the Sondervermögen is indeed to be spent within just three years, it may be of limited help to address persistent capability gaps within the German armed forces. Procurement projects are notorious for being overlong and drawn-out."
114 Quis, Schutz, Bertelsmann Stiftung Europe, op. cit. Cytat: „unclear and uncoordinated investment priorities hinder the development of cross-border cooperation needed to raise Europe's overall defence readiness. Without alignment on civil preparedness, opportunities for burden-sharing and joint capability development are lost."
115 Tamze. Cytat: „if the increase in civil preparedness spending fails to produce credible and measurable improvements in Europe's defence and deterrence posture, the initiative risks ultimately backfiring. In the medium term, this could erode trust, fuel political disillusionment and strain the transatlantic relationship."
116 Rym Momtaz, „Taking the Pulse: Does Meeting the 5 Percent of GDP Target Enable Europe to Confront the Russian Threat?", Carnegie Endowment for International Peace, Strategic Europe, czerwiec 2025 r.: https://carnegieendowment.org/europe/strategic-europe/2025/06/taking-the-pulse-does-meeting-the-5-percent-of-gdp-target-enable-europe-to-confront-the-russian-threat. Cytat: „Poland, the Baltics, and the Nordic states are already reaching the target or have a plan to do it within a few years, so it is indeed possible. [...] the risk is that by 2035 it will be too late."
117 Wilson Beaver, „The 2025 NATO Summit", Heritage Foundation, 2025 r.: https://www.heritage.org/defense/report/the-2025-nato-summit. Cytat: „Defense analysis should focus on the 3.5 percent of GDP target for core defense spending, not the 5 percent total that includes related infrastructure spending."
118 Quis, Schutz, Bertelsmann Stiftung Europe, op. cit. Pełna rekomendacja NRPP: „NATO should establish a dedicated NATO Resilience Planning Process (NRPP) as a distinct planning track for civil preparedness. This process would ensure that developing civil resilience, a complex process, receives the necessary political attention, strategic direction and targeted resources. It would serve to operationalise the concept of resilience by setting measurable benchmarks, assessing progress across allies, identifying capability gaps and facilitating coordinated action."

119 Kramer, Binnendijk, Atlantic Council, op. cit. Rekomendacja szósta: „task NATO's Allied Command Transformation with developing guidelines that could be implemented at NATO headquarters, with guidance to nations by the assistant secretary general and with NATO permanent representatives providing national input".
120 Tamże. Rekomendacja pierwsza: włączenie wydatków sektora prywatnego wzmacniających obronność; piąta: ochrona łańcuchów dostaw zgodnie z NATO Defense-Critical Supply Chain Security Roadmap (czerwiec 2024) i Updated Defence Production Action Plan (luty 2025)
121 Quis, Schutz, Bertelsmann Stiftung Europe, op. cit.
122 Riccardo Perona, „Safeguarding the Effectiveness of the Security Action for Europe through Soft Law", IEP@Bocconi University, 2025 r.: https://iep.unibocconi.eu/safeguarding-effectiveness-security-action-europe-through-soft-law
123 Zgodnie z wytycznymi NATO z zakresu Baseline Requirements for National Resilience, nakłady muszą przekładać się na ciągłość funkcjonowania państwa w warunkach kryzysu o wysokiej intensywności.
124 Postulat silnie akcentowany w opracowaniach Heinrich Böll Stiftung (HBS), wskazujących, że łączenie funkcji cywilnych i obronnych to jedyny sposób na zrównoważone utrzymanie celów inwestycyjnych w państwach demokratycznych bez wywoływania sprzeciwu społecznego.
125 Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2025 poz. 1908; uchwalanie nr 72 Rady Ministrów z 27 maja 2025 r., M. P. 2025 poz. 541.
126 Program OLIOC 2025–2026: szacunek 80–90% do JST na podstawie alokacji opisanych w komunikacie MSWiA, kwiecień 2025 r.
127 Ustawa z dnia 4 grudnia 2025 r. o szczegolnych zasadach realizacji zadan zwiazanych z inwestycja w zakresie bezpieczenstwa i obronnosci realizowana w ramach KPO (druk sejmowy nr 1885); decyzja wykonawcza Rady UE 9590/25 z 17 czerwca 2025 r.
128 https://www.gov.pl/web/fundusze-regiony/mfipr-i-bgk-uruchamiaja-inwestycje-w-bezpieczenstwo-i-obronnosc
129 KPO – rozdział REPOWEREU: alokacja 12,14 mld zł dotacji i 99,09 mld zł pożyczek. Decyzja wykonawcza Rady UE z 17 czerwca 2025 r., s. 4–12.
130 Portal Komunalny, Partnerstwo publiczno-prywatne w Polsce. Umowy za 1,6 mld zł, raport 2025 r.; Instytut Sobieskiego, Infrastruktura dual-use w formule PPP, 2023 r.
131 European Commission, European Defence Fund Work Programme 2025; Zbiam.pl, Polskie podmioty w niemal co drugim projekcie EDF, marzec 2026 r.
132 European Commission, RESCEU – Civil Protection Mechanism; komunikat KE z 20 grudnia 2023 r. ws. alokacji 690 mln euro na rezerwy CBRN; KE, Commissioner Lahbib in Poland to visit EU strategic reserves, 9 stycznia 2025 r.
133 GDDKiA, komunikat o projektach dual-use w ramach CEF Military Mobility, maj 2025 r.; propozycja KE z lipca 2025 r. zwiększenia CEF Military Mobility do 17,6 mld euro w MFF 2028-2034.
134 Atlantic Council, NATO needs to define the substance of its 1.5 percent pledge, sierpien 2025 r.; SIPRI, NATOs new spending target: challenges and risks, lipiec 2025 r.
135 Prawo.pl, Rząd przesuwa niewykorzystane pieniądze na ochronę ludności na 2026 r., grudzień 2025 r.; Portal Samorządowy, Do maja nie zdażą. Apel gmin wiejskich, 2026 r.
136 https://www.gov.pl/attachment/5cbf2719-811a-49e7-bfd9-53c83b35fac2
137 https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
138 https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych
139 https://ec.europa.eu/commission/presscorner/api/files/document/print/pl/ip_25_856/IP_25_856_PL.pdf
140 https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf
141 https://www.finlex.fi/api/media/statute-foreign-language-translation/688086/mainPdf/main.pdf?timestamp=2011-04-28T21%3A00%3A00.000Z
142 https://www.ifrc.org/docs/IDRL/Laws/Switzerland_Civil%20Protection%20System.pdf
143 https://www.mcf.se/en/
144 https://infosecurity24.pl/za-granica/estonia-przeszkoli-ludnosc-z-postepowania-w-sytuacjach-kryzysowych
145 http://nik.gov.pl/najnowsze-informacje-o-wynikach-kontroli/budowle-ochronne-miejsca-ukrycia.html
146 https://bip.brpo.gov.pl/pl/content/rpo-bezpieczenstwo-zagrozenia-obrona-cywilna-schrony-mswia-odpowiedz
147 Luka w sercu systemu ochrony ludności, HOLDFORT, White paper, 2026, https://pliki.holdfort.pl/HFT-WhitePaper-Luka_w_systemie_ochrony_ludnosci-20260609.pdf
148 Możliwe jest również późniejsze zaadaptowanie istniejących obiektów sportowych do pełnienia podwójnej funkcji zob. np. Schrony S-1 pod Orlikami. Witamy w bezpiecznej Polsce jutra https://innpoland.pl/225418,schrony-s-1-pod-orlikami-witamy-w-bezpiecznej-polsce-jutra
149 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20240001907
150 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250000235
151 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250000932
152 https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20250001548
153 Luka w sercu systemu ochrony ludności, HOLDFORT, White paper, 2026, https://pliki.holdfort.pl/HFT-WhitePaper-Luka_w_systemie_ochrony_ludnosci-20260609.pdf
154 Propozycja reformy siatki kategorii za: Luka..., 2026
155 Rozporządzenie MSWiA z dnia 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych oraz warunków technicznych ich użytkowania i usytuowania (Dz.U. 2025 poz. 1548), §4 ust. 2. Oficjalny tekst: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20250001548/O/D20251548.pdf
156 Rozporządzenie Rady Ministrów z dnia 31 lipca 2025 r. w sprawie szczegółowych warunków wyznaczania budynków użyteczności publicznej, w których zapewnia się budowle ochronne (Dz.U. 2025 poz. 1070)
157 Pelastuslaki (Rescue Act 379/2011), https://finlex.fi/en/legislation/translations/2011/eng/379. Ministerstwo Spraw Wewnętrznych Finlandii: https://intermin.fi/en/rescue-services/preparedness/civil-defence-shelters
158 Finland has civil defence shelters for about 4.8 million people, Ministry of the Interior, 2023, https://intermin.fi/en/-/finland-has-civil-defence-shelters-for-about-4.8-million-people
159 Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz (BZG), SR 520.1, https://www.fedlex.admin.ch/eli/cc/2020/887/de
160 BABS (Bundesamt für Bevölkerungsschutz), Schutzräume für die Bevölkerung, https://www.babs.admin.ch/de/schutzraeume
161 Swedish Civil Defence and Resilience Agency (MCF) https://www.mcf.se/contentassets/e0b6f3ddc621475d9071ff3545f1e643/skyddsrum-sr-15-2024_240614.pdf
162 Civil defense shelters, Swedish Civil Defence and Resilience Agency, https://www.krisinformation.se/en/hazards-and-risks/shelters-evacuation-and-warning-systems/shelters/
163 Mamad Safety in Israel: Critical Assessment & Modern, 2025, https://sheltersecurityproducts.com/2025/07/11/mamad-safety-israel-modern-warfare/
164 The Finnish civil defence shelter system – Evolution of the regulation and technical specification 1954–2011 https://aaltodoc.aalto.fi/items/04df3ae1-36da-4e56-8e67-8189754c634c
165 https://www.plattformj.ch/artikel/237092/
166 https://nto.pl/miliony-na-schrony-a-efekt-zerowy-mieszkancy-wciaz-bez-miejsc-schronienia/ar/c1p2-28934407
167 https://inzynierbudownictwa.pl/rozporzadzenia-w-sprawie-obiektow-zbiorowej-ochrony-regulacje-mswia-i-rady-ministrow-z-2025-r/
168 https://foreignpolicy.com/2022/11/12/ukraine-russia-war-kyiv-metro-transit-shelter-missiles/
169 https://finland.fi/life-society/helsinki-underground-where-the-city-plays-swims-and-shelters/
170 https://www.france24.com/en/live-news/20250404-finland-s-colossal-bomb-shelters-a-model-for-jittery-europe
171 https://www.babs.admin.ch/dam/en/sd-web/8gRLhzuAROFB/20230501KonzeptSchutzbauten-de.pdf
172 https://www.washingtonpost.com/news/in-sight/wp/2015/03/17/hidden-in-plain-sight-the-anatomy-of-israeli-bomb-shelters/
173 https://www.huoltovarmuuskeskus.fi/en/a/topical-questions-and-answers-about-security-of-supply

174 INFRASTRUKTURA DUAL-USE W FORMULE PARTNERSTWA PUBLICZNO-PRYWATNEGO, https://sobieski.org.pl/wp-content/uploads/PPP_W_INFRASTRUKTURZE_E_BOOK.pdf
175 Seria norm międzynarodowych dotyczących bezpieczeństwa systemów automatyki przemysłowej i sterowania (IACS), definiująca m.in. poziomy bezpieczeństwa (SL) oraz model stref i kanałów – zones and conduits
176 ITRE ATT&CK – attack.mitre.org; CISA – cisa.gov; E-ISAC – publiczne katalogi technik, taktyk i procedur atakujących
177 Najwyższa Izba Kontroli, *Funkcjonowanie systemu łączności w służbach podległych MSWiA*, 2025, s. 10, https://bip.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole,25494.html [dostęp: 18.06.2026].
178 Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. z 2024 r. poz. 1907).
179 Art. 74 ust. 1–4 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. z 2024 r. poz. 1907).
180 Najwyższa Izba Kontroli, *Funkcjonowanie systemu łączności w służbach podległych MSWiA*, 2025, s. 10, https://bip.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole,25494.html [dostęp: 18.06.2026].
181 Tamże, s. 13.
182 Tamże, s. 25.
183 Tamże, s. 29-30.
184 Tamże, s. 13, 32.
185 Tamże, s. 13.
186 Tamże, s 62.
187 Tamże, s. 34, 39 .
188 Tamże, s 8.
189 Tamże, s 49
190 Art. 155 ust. 1–6 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. z 2024 r. poz. 1907).
191 Art. 156 ust. 1–6 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. z 2024 r. poz. 1907).
192 Ministerstwo Spraw Wewnętrznych i Administracji, Ocena Skutków Regulacji. Projekt ustawy o ochronie ludności i obronie cywilnej, 2024, s. 12, [online] https://www.zpp.pl/storage/library/2024-06/8d7ec929f3dd8b975c9f7b162b095d3f.pdf [dostęp: 18.06.2026].
193 Najwyższa Izba Kontroli, *Funkcjonowanie systemu łączności w służbach podległych MSWiA*, 2025, s. 6, https://bip.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole,25494.html [dostęp: 19.06.2026].
194 MCXTEND, *Public Safety Broadband Spending to Exceed $6.3 Billion by 2028, Says SNS Telecom & IT*, 2026, https://www.mcxtend.com/news/public-safety-broadband-spending-to-exceed-6-3-billion-by-2028-says-sns-telecom-it[dostęp: 19.06.2026].
195 Erillisverkot Ltd., *Virve 2 Ready for Deployment – What Constitutes a Reliable Service?*, 2025, https://www.erillisverkot.fi/en/virve-2-ready-for-deployment-what-constitutes-a-reliable-service/ [dostęp: 19.06.2026].
196 MCXTEND, *Public Safety Broadband Spending to Exceed $6.3 Billion by 2028, Says SNS Telecom & IT*, 2026, https://www.mcxtend.com/news/public-safety-broadband-spending-to-exceed-6-3-billion-by-2028-says-sns-telecom-it [dostęp: 19.06.2026].
197 European Commission – Directorate-General for Migration and Home Affairs, *Enhancing Europe's Capacity to React: Preparing the European Critical Communication System (EUCCS)*, 2026, https://home-affairs.ec.europa.eu/news/enhancing-europes-capacity-react-preparing-european-critical-communication-system-2026-01-30_en [dostęp: 19.06.2026].
198 Ibidem.
199 Ibidem.
200 European Union Agency for the Space Programme (EUSPA), *Observer: What is IRIS²?*, 2024, https://eu-space.europa.eu/news/observer-what-iris2 [dostęp: 19.06.2026].
201 Ibidem.
202 Raport 5G – Szanse, Zagrożenia Wyzwania Fundacja Digital Poland, Instytut Kościuszki https://digitalpoland.org/assets/publications/2020-5 g-szanse-zagrozenia-wyzwania/2020-5 g-szanse-wyzwania-zagrozenia.pdf
203 Ustawa o ochronie ludności i obronie cywilnej art. 203 w zw. z art. 194 (nowelizującym art. 31 ust. 2 ustawy o Agencji Mienia Wojskowego) (Dz. U. z 2024 r. poz. 1907).
204 Tamże, art. 157
205 Tamże, art. 154 ust. 3 i 6
206 Ministerstwo Spraw Wewnętrznych i Administracji, Ocena Skutków Regulacji. Projekt ustawy o ochronie ludności i obronie cywilnej, 2024, s. 12, [online] https://www.zpp.pl/storage/library/2024-06/8d7ec929f3dd8b975c9f7b162b095d3f.pdf [dostęp: 18.06.2026].
207 https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5 g-security [dostęp: 23.06.2026]
208 Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2025 rok https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025, s. 28 [dostęp: 23.06.2026]
209 WHO, Surveillance System for Attacks on Health Care (SSA), 2026: https://www.who.int/europe/news/item/08-05-2026-3000-attacks-on-health-care-in-ukraine-verified-by-who-since-full-scale-invasion; UN Ukraine, komunikat z 19 sierpnia 2024 r.: https://ukraine.un.org/en/276820-grim-milestone-world-humanitarian-day-who-records-1940-attacks-healthcare-ukraine-start-full
210 WHO, komunikat prasowy dyrektora regionalnego WHO na Europe dr. Hansa Henri P. Klugego, 2026, op. cit. Cytat: „Every one of these attacks is a violation of international humanitarian law."
211 Tamże. Badanie oparte na ankiecie 617 ukraińskich placówek ochrony zdrowia.
212 Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2024 poz. 1907. Tekst jednolity: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20240001907/T/D20241907L.pdf
213 Grzymała-Kazłowski M., „WAR SOR. Podstawowe założenia do projektowania szpitala czasów wojny i pokoju", maszynopis, sierpień 2025 r.
214 WHO Regional Office for Europe, „Underground shelters and services in hospitals", Copenhagen, WHO, 2 kwietnia 2025 r. (WHO-EURO-2025-11046-50818-77024). Pełny tekst: https://iris.who.int/bitstream/handle/10665/380994/WHO-EURO-2025-11046-50818-77024-eng.pdf
215 Ministerstwo Obrony Narodowej, „Program Szpitale Przyjazne Wojsku", gov.pl: https://www.gov.pl/web/obrona-narodowa/program-szpitale-przyjazne-wojsku. Porozumienie podpisane 20 marca 2025 r.; pilotaż: 25 szpitali z Polski Wschodniej. MILMAG: https://milmag.pl/program-szpitale-przyjazne-wojsku-wzmocnienie-systemu-bezpieczenstwa-zdrowotnego/
216 Grzymała-Kazłowski M., op. cit.
217 WHO Regional Office for Europe, op. cit. Cytat: „comprehensive framework for establishing and managing underground hospital shelters during emergencies, with a focus on crises involving chemical, biological, radiological and nuclear (CBRN) threats."
218 WHO Regional Office for Europe, op. cit. Badanie 617 placówek ukraińskich wskazuje na braki w modernizacji piwnic, brakach generatorów, zapasach wody i tlenu medycznego jako główne utrudnienia w prowadzeniu działalności w warunkach ataku.
219 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 lutego 2025 r. w sprawie kryteriów uznawania obiektów budowlanych albo ich części za budowle ochronne, Dz.U. 2025 poz. 235.
220 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 listopada 2025 r. w sprawie warunków technicznych dla budowli ochronnych oraz warunków technicznych ich użytkowania i usytuowania, Dz.U. 2025 poz. 1548. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20250001548/O/D20251548.pdf
221 Grzymała-Kazłowski M., op. cit. Projekt rozporządzenia MSWiA w sprawie warunków technicznych budowli ochronnych określa kategorie S-1, S-2, S-3 (schrony hermetyczne) i U-1, U-2, U-3 (ukrycia). Decyzja o kategorii powinna być wypracowywana we współpracy z wojskiem i służbami obrony cywilnej dla każdej lokalizacji.
222 Ustawa z dnia 5 grudnia 2024 r., op. cit., art. 92-94 i art. 206. Art. 206 dopuszcza sfinansowanie do 100% kosztów poniesionych na tworzenie obiektów ochronnych ze środków publicznych.
223 Gielerak G., op. cit.
224 JNS / Columbus Jewish News, 2024 r.: https://www.columbusjewishnews.com/jns/haifa-readies-world-s-largest-underground-hospital/
225 Sammy Ofer Fortified Underground Emergency Hospital, Rambam Health Care Campus, Hajfa. Źródła: strona oficjalna szpitala: https://www.rambamhcc.com/sammy-ofer-fortified-underground-hospital;

American Friends of Rambam: https://aforam.org/the-sammy-ofer-fortified-underground-emergency-hospital/; Times of Israel, 12 października 2023 r.: https://www.timesofisrael.com/amid-northern-jitters-haifas-fortified-underground-hospital-readies-for-war/

226 Times of Israel, 12 października 2023 r., op. cit. Cytat oryginalny prof. Michaela Halberthala (CEO Rambam): „We can be there for a really long time. In case of biological or chemical warfare, we can close the doors and be totally self-sufficient for three days without any help from the outside."

227 Times of Israel, op. cit. Opis pełnego uruchomienia 7 października 2023 r. jako pierwszego wojennego wdrożenia obiektu; również: Israel365 News, 2023: https://israel365news.com/282289/rambam-hospital-conducts-emergency-drill-new-underground-medical-unit

228 IV Konwencja Genewska z 12 sierpnia 1949 r., art. 18 ust. 1. Tekst ICRC: https://ihl-databases.icrc.org/assets/treaties/380-GC-IV-EN.pdf. Cytat: „Civilian hospitals organized to give care to the wounded and sick... may in no circumstances be the object of attack."

229 Tamże, art. 19 ust. 1. Warunki utraty ochrony: jedynie wykonywanie działań szkodliwych dla nieprzyjaciela poza obowiązkami humanitarnymi, po uprzednim ostrzeżeniu z wyznaczonym terminem.

230 Tamże, art. 2 ust. 2. Ustawa definiuje obronę cywilna przez odwołanie do art. 61 lit. a Protokołu dodatkowego I do Konwencji Genewskich z 12 sierpnia 1949 r., co obejmuje m.in. udzielanie pomocy medycznej i organizacje opieki nad rannymi i chorymi.

231 Schmitt M., „The Legal Protection of Hospitals during Armed Conflict", Lieber Institute West Point, 2023: https://lieber.westpoint.edu/legal-protection-hospitals-during-armed-conflict/. Interpretacja: przygotowanie ochronne szpitala nie przekształca go w cel wojskowy; wyposażenie systemu obrony cywilnej jako świadczenie pomocy ludności cywilnej mieści się w art. 61 lit. a PI.

232 ICRC, „Reaffirming the obligation to protect medical facilities and support their functioning", 2025, https://blogs.icrc.org/law-and-policy/2025/11/20/reaffirming-the-obligation-to-protect-medical-facilities-and-support-their-functioning/

233 Tamże. Cytat: „szpitale funkcjonujące w bliskim zapleczu pola walki muszą być przygotowane do podejmowania natychmiastowych działań ratujących życie, co wymaga zmiany priorytetów od standardowej opieki indywidualnej w stronę efektywności populacyjnej."

234 WHO Regional Office for Europe, op. cit. Główne wyzwania zidentyfikowane na Ukrainie: bezpieczne miejsca leczenia, generatory, zapasy wody, tlen w butlach, zapasy medyczne, wsparcie psychologiczne personelu.

235 NATO, „Resilience, civil preparedness and Article 3", https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3. Baseline Requirement 5 (BR5): „Ability to deal with mass casualties and disruptive health crises: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure."

236 Gielerak G., op. cit. Rekomendacja 4: ustawowy obowiązek producenta i importera leków do utrzymywania zapasów wybranych kategorii (min. 6 miesięcy antybiotyków i anestetyków), wzorowany na modelu fińskim.

237 Rada UE, „New rules for critical medicines in the EU": https://www.consilium.europa.eu/en/policies/critical-medicines-act/. Cytat (Komisja Europejska, 2021): 80% importowanych składników farmaceutycznych pochodzi z pięciu krajów; Chiny: 45% wartości importu API do UE.

238 Rada UE, „Critical Medicines Act: Council agrees its position on new rules to tackle shortages", 2025 r.: https://www.consilium.europa.eu/en/press/press-releases/2025/12/02/critical-medicines-act-council-agrees-its-position-on-new-rules-to-tackle-shortages/. EMA, porozumienie z 12 maja 2026 r.: https://www.ema.europa.eu/en/news/ema-welcomes-political-agreement-critical-medicines-act

239 ENISA, „Health Threat Landscape (January 2021 to March 2023)", lipiec 2023 r. URL: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf.

240 Gielerak G., „Nowa architektura bezpieczeństwa medycznego państwa", WIM-PIB / Defence24, 28 marca 2025 r. URL: https://wim.mil.pl/2025/03/28/nowa-architektura-bezpieczenstwa-medycznego-panstwa/

241 Polski Instytut Ekonomiczny, Tygodnik Gospodarczy 45/2025, listopad 2025; PIE, analizy krytycznych zależności importowych Polski od Chin, marzec 2025.

242 Rada Unii Europejskiej, stanowisko ws. Critical Medicines Act, 2 grudnia 2025; Europejski Komitet Ekonomiczno-Społeczny, Securing Europe's medicine supply, 2024.

243 Komisja Europejska, Strategic Dependencies Review, SWD(2021)352 i SWD(2022)41; Europejski Parlament, EPRS, dane o surowcach krytycznych, 2024.

244 Komisja Europejska, Rozporządzenie (UE) 2023/1781 – European Chips Act, 13 września 2023; Europejski Trybunał Obrachunkowy, ocena realizacji celu 20%, 2025.

245 Huoltovarmuuskeskus (NESA), The National Emergency Supply Agency – opis instytucji, huoltovarmuuskeskus.fi

246 NESA, Finances, huoltovarmuuskeskus.fi/en/organisation/funding-and-legislation/finances, dostęp kwiecień 2026.

247 NESA, Cyber preparedness of Finnish sectors at a good basic level, komunikat, 2022.

248 https://wyborcza.pl/7,75398,32742150,strategia-przetrwania-jak-droga-przez-meke-szef-rars-o-polskim.html

249 Fundacja Pułaskiego, All hands on deck: Civil resilience as part of Total Defence in the Baltic Sea basin, pulaski.pl, 2025

250 Rząd Szwecji, New package for stronger civil defence, government.se, 17 września 2025 (zaktualizowano 1 października 2025).

251 Rząd Szwecji, Om krisen eller kriget kommer – dystrybucja 5 mln egzemplarzy do gospodarstw domowych, listopad 2024; MCF, Preparedness for businesses – In case of crisis or war, 20 stycznia 2026.

252 Rząd Szwecji, Total defence – informacje o MoU państw bałtyckich z marca 2026, government.se/government-policy/total-defence.

253 e-Estonia, X-Road – opis platformy, e-estonia.com/solutions/interoperability-services/x-road; GovInsider, Estonia's X-Road: data exchange in the world's most digital society, 2025.

254 George James Consulting, How can X-Road data exchange be used by other nations?, 2025; Komisja Europejska, X-Road – cross-border co-development of national data exchange platform, ec.europa.eu

255 e-Estonia, Data Embassy, e-estonia.com/solutions/e-governance/data-embassy, dostęp kwiecień 2026.

256 CSIS, Seth G. Jones, Russian Sabotage Operations in Europe, marzec 2025; Globsec/ICCT, raport o incydentach sabotażowych, październik 2025. Polska zajmuje pierwsze miejsce w rankingu z 20 udokumentowanymi incydentami od 2022 r.

257 A&O Shearman, Critical infrastructure: New legislation in Germany and its practical impact, marzec 2026; Luther Lawfirm, KRITIS-DachG Enters into Force, 2026.

258 Gleiss Lutz, Resilience compliance as a board-level duty, 2025; Pond Security, KRITIS-DachG 2026, pond-security.com.

259 BSI, Kurzprofil des BSI, bsi.bund.de; Behörden Spiegel, Rekordhaushalt für das BSI, 18 sierpnia 2025.

260 Luther Lawfirm, KRITIS-DachG Enters into Force: New Obligations, Significant Fines and Many Open Questions, 2026.

261 NÚKIB, Prague Cyber Security Conference 2026 – 7. edycja, 17–18 marca 2026; Cybil Portal, Czech Republic – National Cyber and Information Security Agency.

262 Crowell & Moring, The New EU Pharma Package: Interplay with the Critical Medicines Act, 2025 – zestawienie obowiązków stockpilingu w państwach UE.

263 Rada Unii Europejskiej, New rules for critical medicines in the EU, consilium.europa.eu, 2 grudnia 2025 (stanowisko Rady) i 12 maja 2026 (porozumienie polityczne z PE).

264 EU Perspectives, Lowered ambitions, raised eyebrows: Council OKS Critical Medicines Act, 2 grudnia 2025.

265 Polski Instytut Ekonomiczny, Tygodnik Gospodarczy 45/2025, listopad 2025; por. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1252 – Critical Raw Materials Act, art. 5: próg 65% uzależnienia od jednego dostawcy jako wartość referencyjna dla określenia „nadmiernej zależności".

266 The Triple Dividend: Investing in resilience to boost growth and job creation https://blogs.worldbank.org/en/climatechange/the-triple-dividend--investing-in-resilience-to-boost-growth-and
The Triple Dividend of resilience, https://www.gfdrr.org/sites/default/files/publication/The_Triple_Dividend_of_Resilience.pdf

267 New report finds investing in resilience saves jobs and incomes, U.S. Chamber of Commerce, 2024, https://www.uschamber.com/climate-change/new-report-finds-investing-in-resilience-saves-jobs-and-incomes

268 Does Government Trust Matter? The Effectiveness of Policy Responses in the Health-Disaster Era, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC12072026/

269 Raport MFW wcale nie dał odpowiedzi na pytanie: oszczędzać czy wydawać, 2013, https://www.obserwatorfinansowy.pl/tematyka/rynki-finansowe/bankowosc/raport-mfw-wcale-nie-przyblizyl-odpowiedzi-na-pytanie-oszczedzac-czy-wydawac/

270 How a surge in defence and dual-use technology investment could reconfigure the global AI race, Chatam House, 2026, https://www.chathamhouse.org/2026/04/how-surge-defence-and-dual-use-technology-investment-could-reconfigure-global-ai-race/02

271 Security Strategy for Society (Yhteiskunnan turvallisuusstrategia), uchwała rządu Finlandii z 16 stycznia 2025 r. – najważniejszy dokument koordynujący koncepcję kompleksowego bezpieczeństwa (kokonaisturvallisuus), przypisujący zadania strategiczne wszystkim gałęziom administracji. Koordynację i monitoring sprawuje Komitet Bezpieczeństwa (Turvallisuuskomitea), powołany rozporządzeniem rządu nr 77/2013, w składzie 20 członków i 4 ekspertów reprezentujących administrację, służby i biznes. https://turvallisuuskomitea.fi/en/security-strategy-for-society/ oraz https://turvallisuuskomitea.fi/en/security-committee/operation/

272 Koncepcja obrony totalnej (totalförsvar) reaktywowana decyzją rządu Szwecji z 10 grudnia 2015 r. po aneksji Krymu; integruje obronę wojskową i cywilną w podejściu whole-of-society. Kierunki rozwoju nakreślił raport Komisji Obrony „Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025" (Ds 2017:66). https://www.government.se/government-policy/total-defence/

273 Kancelaria Prezesa Rady Ministrów, *Projekt rozporządzenia Rady Ministrów w sprawie ustanowienia Pełnomocnika Rządu do spraw Wzmocnienia Odporności Państwa*, 2026, https://www.gov.pl/web/premier/projekt-rozporzadzenia-rady-ministrow-w-sprawie-ustanowienia-pelnomocnika-rzadu-do-spraw-wzmocnienia-odpornosci-panstwa [dostęp: 19.06.2026].