

INFRASTRUKTURA ODPORNOŚCI PAŃSTWA



Rysunek 1. Architektura programu: trzy filary, funkcje krytyczne i państwo-regulator.

FORMUŁA NACZELNA

Koherentne systemy: polityczny, społeczny, gospodarczy i technologiczny, służą codziennie rozwojowi społeczno-gospodarczemu i tworzą odporność państwa do działania w sytuacjach kryzysowych.

FORMUŁA PROGRAMU

NIE BETON BEZ SYSTEMU

Schron, mikrosieć, magazyn, centrum danych albo punkt medyczny staje się infrastrukturą odporności dopiero wtedy, gdy ma właściciela, sprawne instalacje, obsadę, aktualną informację, przeciwiczony tryb działania i mierzalny wynik.

Infrastruktura odporności państwa to całość materialnych, cyfrowych, organizacyjnych i społecznych zdolności, które pozwalają przewidzieć zakłócenie, ograniczyć straty, utrzymać funkcje krytyczne, szybko odtworzyć działanie oraz wykorzystać doświadczenie do budowy nowych przewag. Jej rdzeniem jest sieć codziennie użytecznych obiektów i usług dual-use: szkół, garaży, metra, przychodni, magazynów, mikrosieci, centrów danych, systemów ostrzegania, centrów kompetencji i budowli ochronnych.

Program rozwija opublikowaną koncepcję Rezyliencji TechnoSanacji: „Nie bunkier zamiast przyszłości. Infrastruktura, która służy codziennie i ratuje w kryzysie”. Wydanie drugie zachowuje trzy filary programu odporności — społeczny, gospodarczy i technologiczny — lecz ustawia je pod **formułą naczelną**, która dodaje filar czwarty i nadrzędny: **system polityczny**, czyli zdolność państwa do sterowania pozostałymi trzema. Ciężar przesuwają się z deklaracji na portfel inwestycji, standardów, danych, ćwiczeń i odpowiedzialności.



Rysunek 2. Cykl odporności: przewidywanie, absorpcja, odtworzenie, adaptacja i transformacja.

Co zmienia formuła naczelną

Formuła naczelną nie jest mottem. Jest zdaniem sprawdzalnym, wobec którego weryfikuje się każdy rozdział, każdy mechanizm i każdy wskaźnik tego dokumentu. Zawiera cztery rozstrzygnięcia, a każde z nich wyklucza konkretny błąd projektowy powtarzający się w polskiej debacie o ochronie ludności niezależnie od orientacji politycznej.

Reguła warunków łącznych. Cztery systemy nie są wariantami do wyboru. System polityczny bez technologicznego steruje na ślepo. System technologiczny bez politycznego jest sterowany z zewnątrz. System gospodarczy bez społecznego nie ma kto obsłużyć w kryzysie. System społeczny bez gospodarczego nie ma czym działać. Odporność powstaje wyłącznie na przecięciu czterech, a nie jako suma czterech osobnych programów.

Rozstrzygnięcie formuły	Co wyklucza	Konsekwencja dla programu
Koherencja czterech systemów — politycznego, społecznego, gospodarczego i technologicznego	Sektorowe traktowanie odporności: osobno „obrona cywilna”, osobno energetyka, osobno cyfryzacja	Jedna architektura funkcji krytycznych, jeden słownik mierników, jeden graf zależności dla wszystkich sektorów
Służą codziennie rozwojowi społeczno-gospodarczemu	Aktywa martwe: obiekty i zapasy, które przez dekady nie tworzą wartości i dlatego nie są utrzymywane	Zasada dual-use jako reguła projektowa, a nie oszczędność; budżet cyklu życia zamiast jednorazowego CAPEX
Tworzą odporność — zdolność, nie deklarację	Wskaźniki aktywności: liczba zakupów, szkoleń, przyjętych planów i wydanych złotych	Pomiar zdolności: pokrycie operacyjne, czas aktywacji, autonomia, czas odtworzenia, zamknięte działania naprawcze
Do działania w sytuacjach kryzysowych — utrzymanie funkcji, nie przetrwanie obiektu	Mylenie posiadania zasobu ze zdolnością jego użycia w godzinie próby	Właściciel wyniku, standard minimalnej usługi, maksymalny czas przerwy i przewidziany tryb działania dla każdej funkcji

Metryka i status dokumentu

Element	Informacja
Tytuł	Infrastruktura odporności państwa. Wydanie koncentruje się wokół formuły naczelnej.
Numer w serii	seria dokumentów programowych TechnoSanacji (numeracja ciągła).
Charakter	Dokument programowy, strategiczny i edukacyjny; nie jest obowiązującym prawem, projektem budowlanym ani instrukcją alarmową.
Cel	Zwiększenie świadomości społecznej oraz ustanowienie wykonalnego i sprawdzalnego modelu budowy odporności państwa w czterech koherentnych systemach.
Unikalność	Cztery drogi dowodowe (cybernetyczna, systemowa sieciowa strukturalna); doprecyzowane i uzasadnione tezy naczelne; test zgodności i napięcia nierozstrzygnięte; aneks A ze słownikiem; aneks B z bibliografią.
Adresaci	Generacja Z, seniorzy, obywatele, administracja, wspólnoty lokalne, przedsiębiorcy, operatorzy infrastruktury, służby, eksperci i media.
Podstawa	Materiały programowe TechnoSanacji i destylaty bibliotek operacyjnych (RES, SYS, CybControl, MultiAgent, Obrona, Energia, AHP), korpus schronów i odporności, obowiązujące polskie akty prawne oraz oficjalne źródła UE, NATO, Finlandii, Szwecji i Szwajcarii.
Stan źródeł	wrzesień 2026 r.; przed wdrożeniem należy ponownie zweryfikować teksty jednolite, przepisy wykonawcze, normy i finansowanie.
Zasada prawna	Projekt programowy ≠ obowiązujące prawo. Każda inwestycja wymaga właściwej procedury, projektu, uzgodnień, zezwoleń, certyfikacji i nadzoru.

Dwanaście zobowiązań programu

Zobowiązania są operacyjnym rozwinięciem formuły naczelnej. Dwa ostatnie są nowe w wydaniu drugim i wynikają wprost z uzasadnień cybernetycznego oraz strukturalnego.

1. Budujemy sieć zdolności, a nie katalog obiektów.
2. Najpierw chronimy życie, prawa i ciągłość podstawowych usług.
3. Każda funkcja krytyczna ma właściciela, zastępcę, standard minimalny i czas odtworzenia.
4. Każdy obiekt ma paszport odporności, plan aktywacji, budżet cyklu życia i wyniki ćwiczeń.
5. Schrony cywilne pozostają oddzielone od funkcji wojskowych i są projektowane zgodnie z prawem humanitarnym.
6. Infrastruktura dual-use ma tworzyć wartość w pokoju i osiągać gotowość w zdefiniowanym czasie.
7. AI i RAG wspierają rozpoznanie, lecz człowiek zachowuje mandat, podpis i odpowiedzialność.
8. Dane kryzysowe nie służą marketingowi politycznemu, profilowaniu komercyjnemu ani represji niezwiązanej z zagrożeniem.
9. Gen Z i seniorzy współtworzą lokalne mapy ryzyk, pamięć procedur i testy dostępności.
10. Każda złotówka jest rozliczana przez wynik: pokrycie, gotowość, autonomię, czas odtworzenia i wykonaną korektę.
11. Każdy miernik wyniku ma przypisany wskaźnik ryzyka, który wykrywa jego nadużycie — pomiar bez bezpiecznika degeneruje się w sprawozdawczość.
12. Odporność obywatelska wzmacnia zdolność publiczną i nigdy jej nie zastępuje — państwo nie przerzuca ryzyka na obywatela.

SPIS TREŚCI

FORMUŁA PROGRAMU	1
Co zmienia formuła naczelna	2
Metryka i status dokumentu	3
Dwanaście zobowiązań programu	4
SPIS TREŚCI	5
1. DEFINICJA I SENS INFRASTRUKTURY ODPORNOŚCI PAŃSTWA.....	8
1.1. Cztery rodzaje infrastruktury.....	8
1.2. Zasada dual-use	8
1.3. Odporność jako inwestycja rozwojowa	9
1.4. Trzy poziomy, na których formuła musi być spełniona.....	10
2. FORMUŁA NACZELNA I CZTERY DROGI DOWODOWE	10
2.1. Osiem tez naczelnych publikacji.....	10
2.2. Uzasadnienie cybernetyczne	11
2.3. Uzasadnienie systemowe.....	13
2.4. Uzasadnienie sieciowe.....	15
2.5. Uzasadnienie strukturalne.....	16
2.6. Test czterech uzasadnień	17
3. DIAGNOZA 2026: OD LUKI PRAWNEJ DO LUKI WYKONAWCZEJ	19
3.1. Sygnały pozytywne	19
3.2. Dwanaście luk systemowych.....	19
3.3. Ryzyka kaskadowe	20
4. ARCHITEKTURA SYSTEMU: 12 FUNKCJI I 8 WARSTW ZDOLNOŚCI.....	21
4.1. Osiem warstw infrastruktury odporności.....	22
4.2. Standard minimalnej usługi i maksymalnego czasu przerwy	23
5. KRAJOWY SYSTEM SCHRONÓW I BUDOWLI OCHRONNYCH	24
5.1. Typologia prawna i funkcjonalna	25
5.2. Kategorie i standard — proste objaśnienie	25
5.3. Model docelowy sieci	26
5.4. Kolejność budowy sieci: cztery kroki zamiast jednego celu liczbowego	26
5.5. Paszport odporności obiektu	27
6. SPOŁECZNA INFRASTRUKTURA ODPORNOŚCI I PROGRAM 2G	28
6.1. Powszechny standard przygotowania	28
6.2. Role Generacji Z.....	29
6.3. Role seniorów	29
6.4. Standard dual-key	29
6.5. Odporność poznawcza.....	29

7. ENERGIA, WODA, ZDROWIE, ŻYWNOŚĆ, TRANSPORT I ŁĄCZNOŚĆ	30
7.1. Cytadela odporności — węzeł dual-use	31
7.2. Minimalne zasady ciągłości	31
7.3. Odporność blisko mieszkańca	32
7.4. Minimalne czasy autonomii — katalog startowy	32
8. GOSPODARKA ODPORNOŚCI I KRAJOWY PRZEMYSŁ DUAL-USE	33
8.1. Krajowy łańcuch dostaw infrastruktury odporności	33
8.2. Finansowanie według cyklu życia	33
8.3. Zamówienie na wynik	34
8.4. Bezpieczniki antyzawłaszczeniowe portfela	34
9. AI, RAG, CYFROWY BLIŹNIAK I PAMIĘĆ PAŃSTWA	35
9.1. Narodowy Graf Odporności	36
9.2. RAG — odpowiedź ze źródłem	36
9.3. Minimalny standard agenta AI	37
9.4. Cyfrowy bliźniak	37
9.5. Pamięć państwa	37
10. ZARZĄDZANIE, PRAWA OBYWATELSKIE I ODPOWIEDZIALNOŚĆ	38
10.1. Struktura odpowiedzialności	38
10.2. Karta praw obywatela w systemie odporności	39
10.3. RACI dla obiektu i funkcji	39
10.4. Granica między sprawczością a nadzorem	40
11. MODELE ZAGRANICZNE I POLSKA ADAPTACJA	40
12. KPI, KRI, PUBLICZNY REJESTR I NIEZALEŻNY AUDYT	42
12.1. KPI — mierniki wyniku	42
12.2. KRI — wskaźniki ryzyka	43
12.3. Publiczny rejestr i poziomy jawności	43
12.4. Niezależny audyt	44
12.5. Narodowy Indeks Odporności	44
13. MAPA DROGOWA: 100 DNI — 10 LAT	44
13.1. Pierwsze 100 dni	45
13.2. Dwanaście miesięcy	45
13.3. Trzy lata	45
13.4. Pięć lat	45
13.5. Dziesięć lat	46
14. PORTFEL PROJEKTÓW PILOTAŻOWYCH	46
14.1. Karta projektu pilotażowego	47
15. TEST GOTOWOŚCI ORGANIZACJI I WSPÓLNOTY	47

15.1. Interpretacja	48
16. TEST ZGODNOŚCI Z FORMUŁĄ NACZELNĄ I NAPIĘCIA NIEROZSTRZYGNIE	49
16.1. Test zgodności rozdziałów z formułą	49
16.2. Napięcia nierozstrzygnięte.....	50
16.3. Warunki, przy których program należałoby zmienić.....	50
ANEKS A. SŁOWNIK POJĘĆ, TERMINÓW I SKRÓTÓW	51
A.1. Skróty, akronimy i oznaczenia	51
A.2. Pojęcia cybernetyczne	53
A.3. Pojęcia systemowe i odpornościowe	55
A.4. Pojęcia sieciowe	57
A.5. Pojęcia strukturalne, prawne i operacyjne.....	58
A.6. Pojęcia ustrojowe i programowe TechnoSanacji.....	60
ANEKS B. BIBLIOGRAFIA I BAZA DOWODOWA.....	61
B.1. Cybernetyka, teoria sterowania i regulacji.....	61
B.2. Polska szkoła cybernetyki: układy samodzielne i tory sterowania.....	62
B.3. Teoria systemów, niezawodność i inżynieria odporności	62
B.4. Teoria sieci i odporność infrastruktury krytycznej	63
B.5. Zdolność państwa, organizacja i antyzawłaszczenie	64
B.6. Odporność jako polityka publiczna: ramy, pomiar i krytyka.....	65
B.7. Ochrona ludności, obrona cywilna i obrona totalna.....	66
B.8. Infrastruktura krytyczna, cyberodporność i suwerenność technologiczna	67
B.9. Energia, woda, żywność i zdrowie jako tor zasilający	68
B.10. Odporność społeczna, zaufanie i odporność poznawcza.....	68
B.11. Sztuczna inteligencja, systemy wieloagentowe i nadzór algorytmiczny.....	69
B.12. Polska — prawo i programy publiczne.....	70
B.13. Dokumenty programowe TechnoSanacji i destylaty bibliotek operacyjnych.....	70
B.14. Adresy źródeł internetowych	71
B.15. Nota o źródłach	71

JAK CZYTAĆ DOKUMENT

Czytelnik może zacząć od rozdziałów 1–4, następnie przejść do schronów (5), Programu 2G (6), technologii (9), mierników (12) i mapy drogowej (13).

Rozdział 2 jest warstwą dowodową: tam znajdują się uzasadnienia cybernetyczne, systemowe, sieciowe i strukturalne, do których pozostałe rozdziały odsyłają. Czytelnik praktyczny może go pominąć przy pierwszym czytaniu i wrócić do niego przy sporze o rozstrzygnięcie.

Ekspert techniczny powinien każdorazowo sięgać do obowiązujących aktów prawnych i norm; aneks A objaśnia pojęcia, aneks B wskazuje źródła.

1. DEFINICJA I SENS INFRASTRUKTURY ODPORNOŚCI PAŃSTWA

Odporność państwa to zdolność wspólnoty narodowej do zachowania życia, praw obywatelskich, tożsamości, sterowności i podstawowych funkcji mimo wojny, katastrofy, pandemii, blackoutu, cyberataku, awarii przemysłowej, kryzysu finansowego, przerwania łańcuchów dostaw albo gwałtownej zmiany technologicznej.

Infrastruktura odporności jest materialnym i organizacyjnym nośnikiem tej zdolności. Obejmuje obiekty, instalacje, zapasy, dane, oprogramowanie, procedury, kompetencje, finansowanie, łączność, sieci współpracy i mechanizmy korekty. Nie jest osobnym sektorem: łączy ochronę ludności z energetyką, zdrowiem, logistyką, gospodarką, cyberbezpieczeństwem i zarządzaniem publicznym.

Definicja robocza wydania II. Odporność państwa to zdolność Narodu-jako-systemu do przewidzenia, wytrzymania, odtworzenia i zaadaptowania się po wstrząsie **z zachowaniem tożsamości i sterowności**. Dwa ostatnie słowa są rozstrzygnięciem: państwo, które przetrwało fizycznie, lecz utraciło zdolność samodzielnego sterowania, nie jest państwem odpornym — jest państwem sterowanym z zewnątrz.

1.1. Cztery rodzaje infrastruktury

Rodzaj	Co obejmuje	Przykład wyniku
Fizyczna	Budowle ochronne, sieci energii i wody, transport, magazyny, szpitale, centra danych, obiekty logistyczne.	Obiekt utrzymuje minimalną usługę mimo awarii zewnętrznej.
Cyfrowa	Rejestry, systemy ostrzegania, chmura, łączność, cyberochrona, graf wiedzy, kopie offline.	Decyzja i komunikacja są możliwe także przy utracie podstawowej sieci.
Organizacyjna	Właściciel wyniku, zastępstwo, procedury, ćwiczenia, umowy, RACI, ciągłość dostaw i serwisu.	Wiadomo, kto uruchamia zasób, w jakim czasie i na jakich zasadach.
Spółeczna	Zaufanie, kompetencje, wolontariat, sieci sąsiedzkie, Program 2G, komunikacja i odporność poznawcza.	Ludzie rozumieją komunikat, współdziałają i wspierają osoby zależne.

Podział ten nie jest klasyfikacją porządkującą, lecz **wykazem warunków koniecznych**. Infrastruktura fizyczna bez organizacyjnej jest zasobem bez dysponenta. Cyfrowa bez społecznej jest komunikatem bez odbiorcy. Organizacyjna bez fizycznej jest planem bez środków. Społeczna bez cyfrowej jest gotowością bez informacji. Program mierzy więc nie cztery osobne wskaźniki, lecz **najstańsze ogniwo w każdej funkcji krytycznej**.

1.2. Zasada dual-use

Infrastruktura dual-use jest użyteczna codziennie, lecz może zostać szybko przetłączona do funkcji ochronnej. Garaż może być parkingiem i ukryciem; hala — obiektem sportowym i punktem przyjęcia ludności; szkoła — miejscem edukacji i lokalnym centrum wsparcia; mikrosieć — źródłem tańszej energii i zasilaniem awaryjnym; centrum danych — zapleczem usług cyfrowych i ciągłości państwa.

Dual-use jest w tym dokumencie **konsekwencją formuły naczelnej, a nie sposobem na oszczędność**. Formuła wymaga, by systemy „służyły codziennie”. Obiekt, który nie służy codziennie, nie jest obserwowany, nie ma budżetu utrzymania, nie ma obsady i nie ma powodu, by ktokolwiek zauważył jego degradację. Doświadczenie fińskie, szwedzkie i szwajcarskie pokazuje tę samą zależność: utrzymywane są te obiekty, które mają pokojowego użytkownika i pokojowego właściciela wyniku.

REGUŁA PROJEKTOWA

Funkcja pokojowa nie może osłabiać funkcji ochronnej. Konwersja musi być opisana, finansowana, ćwiczona i możliwa w ustawowym lub przyjętym standardzie czasu.

Test odwrotny: jeżeli usunięcie funkcji ochronnej nie zmieniałoby niczego w codziennym użytkowaniu obiektu, obiekt jest dual-use wyłącznie na papierze.

1.3. Odporność jako inwestycja rozwojowa

Nakład na odporność jest w debacie publicznej przedstawiany jako koszt alternatywny wobec rozwoju. Formuła naczelna odwraca tę relację: systemy, które służą codziennie rozwojowi, są tym samym zasobem, który w kryzysie utrzymuje funkcje państwa. Wydatek na odporność:

- podnosi jakość usług publicznych i bezpieczeństwo inwestycji;
- zmniejsza straty i skraca przestoje po kryzysie;
- rozwija krajowe łańcuchy dostaw, serwis i produkcję dual-use;
- wymusza interoperacyjność danych, energii i łączności;
- buduje kompetencje lokalne oraz współpracę Gen Z z seniorami;
- wzmacnia wiarygodność Polski wobec obywateli, inwestorów, NATO i UE;
- obniża koszt kapitału i koszt ubezpieczenia dla regionów o udokumentowanej ciągłości usług;
- tworzy popyt publiczny, dzięki któremu krajowe komponenty ochronne uzyskują pierwszego wymagającego odbiorcę.

Argument ekonomiczny ma jednak granicę, którą wydanie drugie wskazuje wprost. Redundancja jest **dobrem publicznym**: przedsiębiorstwo nie internalizuje społecznej korzyści z zapasu, którego samo nie użyje, dlatego rynek systematycznie niedodostarcza odporności. To uzasadnia interwencję państwa. Symetrycznie jednak nadmiar rezerw ma policzalny koszt fiskalny i zniekształca rynek, a nadmiar centralnej kontroli prowadzi do usztywnienia systemu. **Celem nie jest maksimum zapasów, kontroli i procedur, lecz optymalny bufor pod policzone ryzyko** — rozstrzygnięcie rozwinięte w rozdziale 2.2 i 8.

1.4. Trzy poziomy, na których formuła musi być spełniona

Poziom	Kto odpowiada	Co znaczy spełnienie formuły
Obiekt	Właściciel i zarządca obiektu	Obiekt ma pokojowego użytkownika, paszport odporności, obsadę, przewidzianą konwersję i mierzalną pojemność operacyjną.
Węzeł lokalny	Gmina, powiat, operator węzła	W promieniu życia codziennego mieszkańca istnieje miejsce łączące informację, zasilanie, wodę, pierwszą pomoc i schronienie.
System państwa	Właściciel Narodowej Strategii Odporności	Dwanaście funkcji krytycznych ma właściciele, standardy minimalne, graf zależności, mierniki i domkniętą pętlę korekty na alokacji budżetowej.

Spełnienie formuły na jednym poziomie nie przenosi się automatycznie na pozostałe. Sprawny obiekt w niesprawnym węźle nie tworzy zdolności; sprawne węzły bez krajowego właściciela wyniku nie tworzą systemu. Dlatego program mierzy zdolność **jednocześnie na trzech poziomach**, a raport roczny pokazuje najłabszy z nich, nie średnią.

2. FORMUŁA NACZELNA I CZTERY DROGI DOWODOWE

Rozdział jest warstwą dowodową dokumentu. Formuła naczelna ma status twierdzenia, nie hasła, dlatego wymaga uzasadnienia prowadzonego równolegle w czterech porządkach: **cybernetycznym** (czy pętla sterowania się domyka), **systemowym** (czy granica systemu i jego dynamika są poprawnie ujęte), **sieciowym** (gdzie leży ryzyko kaskadowe) i **strukturalnym** (czy istnieje organizacja zdolna to wykonać). Każdy zasadniczy mechanizm programu ma wskazane wszystkie cztery uzasadnienia; mechanizm, dla którego którakolwiek rubryka pozostaje pusta, jest kandydatem do przeprojektowania.

2.1. Osiem tez naczelnych publikacji

Tezy T1–T4 opisują przedmiot i cel, T5–T6 kolejność działania, T7–T8 warunki, bez których program pozostaje deklaracją.

Niniejszy rozdział stanowi warstwą dowodową dokumentu. Z uwagi na to, że formuła naczelna ma status twierdzenia, a nie jedynie hasła, wymaga ona uzasadnienia prowadzonego równolegle w czterech porządkach: cybernetycznym, systemowym, sieciowym i strukturalnym.

Każdy zasadniczy mechanizm programu ma przypisane wszystkie cztery uzasadnienia, a pozostawienie którejkolwiek z rubryk wakatowej oznacza, że dany mechanizm kwalifikuje się do przeprojektowania. Poniższa tabela przedstawia osiem tez naczelnych publikacji, gdzie T1–T4 odnoszą się do przedmiotu i celu, T5–T6 wskazują kolejność działania, a T7–T8 określają warunki chroniące program przed pozostaniem czystą deklaracją.

Nr	Teza	Konsekwencja operacyjna
T1	Odporność jest mierzalną zdolnością regulatora , nie deklaracją ani stanem posiadania.	Rdzeniem programu jest Narodowy Indeks Odporności i słownik KPI/KRI, a nie katalog obiektów.
T2	Polsce nie brakuje zasobów ani ramy prawnej — brakuje domkniętej pętli między zasobem, wynikiem i decyzją o zasobie.	Priorytetem jest egzekucja, pomiar i rozliczalność, nie kolejny akt programowy.
T3	Infrastruktura krytyczna to graf zależności , nie zbiór obiektów; ryzyko siedzi w sprzężeniach.	Narodowy Graf Odporności i mapa 50 podatności kaskadowych poprzedzają decyzje inwestycyjne.
T4	Dual-use nie jest oszczędnością, lecz warunkiem utrzymania zdolności w czasie.	Obiekt bez pokojowego użytkownika i pokojowego właściciela wyniku nie wchodzi do portfela.
T5	Wąskim gardłem jest utrzymanie, obsada i dane , nie sama budowa.	CAPEX przyznawany wyłącznie z wieloletnim OPEX, właścicielem utrzymania i planem ćwiczeń.
T6	Odporność to optymalne pasmo , nie maksimum: nadmiar rezerw i nadmiar centralizacji też są patologią.	Bufory projektowane pod policzone ryzyko; subsydiarność operacyjna zamiast centralnego zarządu.
T7	Zdolność państwa jest problemem organizacyjnym , nie budżetowym.	Jeden właściciel wyniku end-to-end, RACI dla funkcji i obiektu, jednostka dostarczania z twardym KPI.
T8	Pętla domyka się na alokacji albo nie domyka się wcale.	Każde wiążące rozstrzygnięcie programu ma pozycję w planie finansowym, termin i właściciela rezultatu.

2.2. Uzasadnienie cybernetyczne

Państwo jest w tym dokumencie traktowane jako **regulator**: podsystem utrzymujący wybrane zmienne układu w wyznaczonych granicach mimo zakłóceń. Formuła naczelna opisuje warunki, w których taki regulator działa.

Twierdzenie o dobrym regulatorze

Conant i Ashby dowiedli, że **każdy dobry regulator systemu musi być modelem tego systemu**. Regulator, który nie ma wiernego modelu rzeczywistości — danych o obiektach, zależnościach i skutkach własnych decyzji — nie steruje, lecz reaguje przypadkowo. Z tego twierdzenia wynikają wprost trzy instytucje programu: **Narodowy Graf Odporności** (model zależności), **paszport odporności obiektu** (model pojedynczego węzła) oraz **cyfrowy bliźniak funkcji lub regionu** (model dynamiki). Nie są to narzędzia informatyczne administracji, lecz techniczne wykonanie warunku sterowalności. Rozbieżność między pojemnością formalną a operacyjną obiektów nie jest błędem statystycznym — jest **awarią modelu regulatora**.

Prawo wymaganej różnorodności

Ashby: „tylko różnorodność może pochłoniąć różnorodność”. Regulator opanuje tyle klas zaburzeń, ile ma stanów odpowiedzi. Katalog zagrożeń, na które musi odpowiedzieć infrastruktura odporności — blackout, cyberatak, uderzenie kinetyczne, powódź, skażenie, pandemia, przerwanie dostaw, dezinformacja — ma różnorodność, której nie pochłonie jeden typ obiektu ani jeden szczebel decyzji. Stąd trzy rozstrzygnięcia programu: **warstwowa sieć schronienia** (schrony, ukrycia, MDS, punkty schronienia, obiekty dual-use) zamiast jednej kategorii; **wielopoziomowe bilansowanie** energii i łączności zamiast jednego źródła; oraz **Program 2G**, który włącza obywateli, młodzież i seniorów jako amplifikator różnorodności regulatora. Odporność obywatelska jest w tym ujęciu nie substytutem zdolności publicznej, lecz sposobem zwiększenia repertuaru odpowiedzi państwa.

Model systemu żywotnego i sygnał algedoniczny

Model Beera wyróżnia pięć podsystemów koniecznych do przeżycia organizacji na każdym poziomie rekurencji: S1 — operacje, S2 — koordynacja i antykolizja, S3 — zarządzanie bieżące z audytem, S4 — rozpoznanie otoczenia i przyszłości, S5 — tożsamość i reguła nadrzędna. Osiem warstw infrastruktury odporności (rozdział 4.1) mapuje się na ten model jednoznacznie, a typowe patologie polskiego systemu ochrony ludności dają się nazwać jako **brak lub przerost konkretnego S**.

Podsystem	Odpowiednik w programie	Patologia przy braku
S1 — operacje	Zarządcy obiektów, operatorzy sieci, służby, samorząd, wspólnoty.	Plan bez wykonawcy; zasób bez dysponenta.
S2 — koordynacja	Standardy, rejestr OZO, interoperacyjność danych, energii i łączności.	Silosy sektorowe; niespójne dane o tym samym obiekcie.
S3 — zarządzanie i audyt	Centrum Odporności i Ciągłości, budżet cyklu życia, niezależny audyt.	Nie wiadomo, czy S1 wykonuje; sprawozdanie zastępuje pomiar.
S4 — rozpoznanie	Krajowy Rejestr Ryzyk, horizon scanning, cyfrowy bliźniak, wnioski z ćwiczeń.	Reakcja wyłącznie wstecz; powtarzanie tej samej awarii.
S5 — tożsamość i reguła	Formuła naczelna, karta praw obywatela, czerwone linie, mandat konstytucyjny.	S3 i S4 walczą o zasoby; brak kryterium rozstrzygania sporu.

Osobnym wymogiem jest **kanał algedoniczny** — droga alarmowa omijająca hierarchię, którą sygnał o zdarzeniu krytycznym dociera wprost do poziomu zdolnego podjąć decyzję. Zdarzenie, dla którego nie przewidziano wskaźnika, musi mieć własne wejście do systemu; inaczej informacja o nim ginie w szczeblach pośrednich. W programie kanałem tym jest jawny sygnał pilny w Centrum Odporności i Ciągłości, z progiem, oknem czasowym i skutkiem uzgodnionym **przed** kryzysem, nie w jego trakcie.

Tor sterowniczy i tor zasilający

Polska szkoła cybernetyki społecznej rozdziela dwa tory każdego układu samodzielnego: **tor sterowniczy** (informacja: dane, łączność, modele, przekaz publiczny) i **tor zasilający** (energomateria: energia, paliwa, woda, części, leki, komponenty). Układ traci samodzielność, gdy przerwany zostaje którykolwiek z nich. Cały rozdział 7 jest konsekwencją tego rozróżnienia: schron bez energii i wody to obiekt z torem sterowniczym i bez toru zasilającego; sprawna sieć zasilania bez łączności i danych to odwrotność tego samego błędu. Trzecim parametrem jest **czas decyzyjny** — droga od zarejestrowania bodźca do wykonania odpowiedzi; struktura ma go minimalizować, a nie chronić hierarchię.

Warunek sprzężenia zwrotnego i cybernetyka drugiego rzędu

Strumień informacji jest sprzężeniem zwrotnym **wtedy i tylko wtedy**, gdy istnieje wskazany organ, termin i instrument zmiany decyzji. Pulpit wskaźników bez właściciela miernika i bez instrumentu realokacji jest sprawozdawczością, nie sterowaniem. To jest cybernetyczna treść tezy T8: pętla domyka się na alokacji albo nie domyka się wcale.

Cybernetyka drugiego rzędu dokłada warunek, którego klasyczna nie miała: **obserwator jest częścią obserwowanego systemu**. Regulator odporności — administracja, operator, dostawca, agent AI — nie stoi na zewnątrz społeczeństwa; ma własne interesy i reprodukuje sam siebie. Problem przesuwają się więc z pytania „jak sterować lepiej” na pytanie „**kto pilnuje sterującego**”. Karta praw obywatela, jawny rejestr, niezależny audyt, rotacja i audyt obywatelski nie są dodatkiem etycznym do programu inżynierskiego — są operacjonalizacją drugiego rzędu. Państwo zdolne bez kontroli regulatora produkuje państwo nadzoru; kontrola regulatora bez zdolności produkuje bezsilną procedurę. Program musi domknąć obie pętle jednocześnie.

GRANICA ATENUACJI

Agregacja danych o obiektach, sieciach i zależnościach jest poprawnym zmniejszaniem różnorodności wejścia. Profilowanie zachowań obywateli nią nie jest.

Kompresja dotyczy danych **o systemie**, nie o ludziach. Ta granica jest w programie regułą konstytucyjną, nie preferencją projektanta.

2.3. Uzasadnienie systemowe

Trzy pojęcia odporności — i wybór programu

Literatura rozdziela odporność **inżynierską** (powrót do jednej równowagi, mierzony czasem powrotu), **ekologiczną** (utrzymanie tożsamości układu przy zmianie stanu) oraz **zdolność transformacji** (przejście do stanu lepszego po szoku trwałym). Program przyjmuje ujęcie drugie i trzecie łącznie: system skrojony wyłącznie pod „powrót do normy” jest ślepy na szoki trwałe — demograficzne, technologiczne, klimatyczne i geopolityczne. Stąd cykl odporności w pięciu fazach: przewidywanie, absorpcja, odtworzenie, adaptacja i **transformacja** — a nie w trzech.

Prędkość szoku	Wymagana zdolność	Instrument programu	Miernik
Szok przejściowy — „odbicie”	Absorpcja i odtworzenie	Rezerwy rotowane, schronienie, redundancja, black-start, procedury ręczne.	Czas odtworzenia funkcji; autonomia w godzinach i dniach.
Szok trwały — „przeskok naprzód”	Adaptacja i transformacja	Realokacja kapitału i kadr, przekwalifikowanie, zmiana standardu, nowy łańcuch dostaw.	Odsetek wniosków wdrożonych i ponownie przetestowanych.

Granica systemu przesądza wynik

Najczęstszy błąd analityczny w inwestycjach ochronnych polega na liczeniu kosztu obiektu zamiast kosztu systemowego. Porównywalność wariantów wymaga jednej granicy systemu, obejmującej: budowę, serwis, energię, przeglądy, wymianę komponentów, obsadę, ćwiczenia, koszt niedostarczonej usługi w czasie awarii oraz koszt utraconej alternatywy. Dlatego podstawowym miernikiem inwestycyjnym programu nie jest koszt miejsca, lecz **koszt uzyskania jednego sprawnego miejsca operacyjnego w pełnym cyklu życia**.

Awaria normalna, ściśle sprzężenie i luz systemowy

W układach złożonych i ściśle sprzężonych awarie są własnością konstrukcji, a nie odchyleniem od normy. Im ciaśniej system jest zoptymalizowany, tym szybciej zakłócenie rozchodzi się w nim, zanim zdąży zostać zrozumiane. Konsekwencje projektowe są trzy: **luz systemowy** (celowy nadmiar czasu, zasobu lub przepustowości, ekonomicznie „nieefektywny”, obronnie konieczny), **procedury ręczne** dla każdej funkcji zautomatyzowanej oraz **degradacja łagodna** — projektowanie tak, by system pod obciążeniem tracił zdolności stopniowo i w kontrolowanej kolejności, zamiast załamywać się skokowo.

Odporność jako pasmo, nie maksimum

Teza T6 ma podstawę w analizie pułapek adaptacyjnych: nadmiar centralnej kontroli prowadzi do **pułapki sztywności** i katastrofalnego rozpadu, a jej niedomiar do **pułapki ubóstwa**. Nadmiar rezerw ma policzalny koszt fiskalny i zaburza rynek. Nawet wysokie zaufanie społeczne nie jest monotonicznie korzystne: w środowiskach wysokiego zaufania uogólnionego jednostki potrafią niedoszacować ryzyka i rozluźnić ostrożność. Program buduje więc zaufanie **warstwowo** — instytucjonalne i do źródeł, nie hurtowe — a bufor projektuje pod policzone ryzyko z jawną analizą kosztu utrzymania.

Prawo Goodharta i punkty dźwigni

Miernik, który staje się celem, przestaje być dobrym miernikiem. Dlatego każdy KPI programu ma przypisany **KRI wykrywający jego nadużycie**: pokrycie operacyjne jest liczone wyłącznie dla obiektów z ważnym przeglądem, czas aktywacji mierzy się w teście zaskoczenia, a liczba ćwiczeń nie zastępuje odsetka zamkniętych działań naprawczych. Symetrycznie obowiązuje zasada punktów dźwigni: **reguła jest silniejszym punktem interwencji niż parametr budżetowy**. Zmiana zasady „CAPEX bez OPEX nie jest przyznawany” zmienia system trwalej niż jednorazowe zwiększenie nakładu.

2.4. Uzasadnienie sieciowe

Państwo jest siecią sieci

Energetyka, telekomunikacja, woda, transport, finanse, zdrowie i administracja tworzą jeden graf: węzłami są obiekty, funkcje i operatorzy, krawędziami — zależności fizyczne, cyfrowe, geograficzne i logiczne. Ten czteropodział zależności jest w programie obowiązkowym polem paszportu odporności obiektu, ponieważ każdy typ zależności zrywa się inaczej i inaczej się go zastępuje.

Typ zależności	Na czym polega	Przykład w programie	Bezpiecznik
Fizyczna	Wyjście jednego węzła jest wejściem drugiego.	Schron zasilany wyłącznie z sieci elektroenergetycznej.	Mikrosieć, agregat, magazyn, paliwo, N+1.
Cyfrowa	Zależność przez stan informacji i sterowanie.	Pompa wody sterowana systemem operatora zewnętrznego.	Tryb ręczny, segmentacja, kopie offline, zero trust.
Geograficzna	Wspólne położenie, wspólne zdarzenie niszczące.	Centrum kryzysowe i zapasowe w tej samej strefie zalania.	Rozproszenie przestrzenne, analiza zagruzowania.
Logiczna	Zależność przez rynek, umowę, regulację lub decyzję.	Jeden dostawca filtrów dla całego kraju.	Drugi dostawca, zapas części, plan wyjścia.

Odporne, lecz kruche

Sieci infrastrukturalne mają silnie nierównomierny rozkład powiązań: nieliczne węzły skupiają bardzo wiele połączeń. Taka struktura jest **odporna na awarie losowe i krucha wobec uderzenia celowanego w węzeł centralny**. Konsekwencja programowa jest ostra: awaria jest losowa, lecz przeciwnik nie jest. Priorytet osłony należy się nie obiektom największym, lecz obiektom o najwyższej **centralności pośrednictwa** — tym, przez które przechodzi najwięcej najkrótszych ścieżek zasilania, łączności i logistyki. Węzeł krytyczny to nie to samo co węzeł duży.

Kaskada w sieciach współzależnych

Najważniejsze ustalenie sieciowe dla infrastruktury odporności brzmi: w układach sprzężonych awaria **nie degraduje systemu łagodnie, lecz przechodzi w nagłe, nieciągłe załamanie wzajemnej łączności** przy uszkodzeniu mniejszym niż próg pojedynczej sieci. Dlatego zdarzenie początkowe i efekt kaskadowy są w tym dokumencie analizowane zawsze łącznie (rozdział 3.3), a plan odtworzenia zaczyna się od pytania, która para sieci zerwie się pierwsza. Trzy mechanizmy łagodzą kaskadę i wszystkie trzy są wpisane w program: **redundancja powiązań, lokalność zależności** (bilansowanie na poziomie zasięgu skutków) oraz **zdolność odcięcia** — praca wyspowa, która przerywa propagację i zamienia załamanie skokowe w proces odwracalny.

Z tego samego aparatu wynika przestroga: dodanie zależności bywa stabilizujące, lecz nie zawsze. Integracja infrastruktury zwiększa odporność tylko przy właściwej strukturze powiązań;

bezrefleksyjne „więcej integracji” tworzy nowe ścieżki kaskady. Każda decyzja o spięciu dwóch systemów wymaga więc analizy topologicznej, nie wyłącznie argumentu efektywnościowego.

Druga ścieżka i pojedynczy punkt awarii

Operacyjną postacią analizy sieciowej jest wymóg **drugiej ścieżki**: dla każdego węzła krytycznego musi istnieć alternatywna trasa przepływu o określonym koszcie uruchomienia i czasie przełączenia. Brak drugiej ścieżki definiuje pojedynczy punkt awarii — element, którego utrata usuwa funkcję całego systemu. Wymóg dwóch niezależnych kierunków ewakuacji z budowli ochronnej, dwóch kanałów ostrzegania i dwóch dostawców komponentu krytycznego to ta sama zasada zastosowana w trzech warstwach.

Sieć społeczna jako warstwa grafu

Graf odporności nie kończy się na infrastrukturze. Informację nową przenoszą kontakty spoza własnego środowiska — to uzasadnia obywatelską sieć obserwacji, pluralizm źródeł i strukturę Programu 2G, w którym Generacja Z i seniorzy stanowią dwa różne zbiory słabych więzi, docierające do innych części społeczności. Kapitał społeczny wiążący bez pomostowego utrwala izolację; program wymaga więc obu i mierzy zasięg dotarcia do osób zależnych, nie sam fakt istnienia wolontariatu.

2.5. Uzasadnienie strukturalne

Zdolność państwa jest problemem organizacyjnym

Teza T7 opiera się na spójnym wyniku współczesnych badań nad zdolnością państwa: zdolność najlepiej modelować jako **własność organizacji**, a nie funkcję nakładu. Państwo o wysokich wydatkach i niskiej zdolności dowieszenia ma trzy rozpoznane przyczyny: fragmentację (brak centrum zdolnego priorytetyzować), rozjazd bodźców (personel reaguje na ścieżkę awansu, nie na misję) oraz brak modelu własnego aparatu. Miernikiem organizacji jest więc **odsetek zadań domkniętych w cyklu** — od zamiaru do zweryfikowanego wyniku — a nie liczba przyjętych dokumentów. Program przyjmuje ten miernik wprost jako KPI „Uczenie” (rozdział 12.1).

Prawo Conwaya: mandat przed systemem

Struktura budowanego systemu odwzorowuje strukturę komunikacyjną organizacji, która go tworzy. Wniosek dla programu jest jednoznaczny: **integracja mandatu musi poprzedzać integrację systemów**. Wspólny rejestr obiektów zbudowany przez sześć instytucji bez jednego właściciela wyniku odtworzy w danych te same sześć silosów. Dlatego pierwsze sto dni zaczyna się od powołania właściciela programu i przyjęcia jednolitego słownika, a nie od przetargu na platformę.

Jeden właściciel wyniku

Rozproszenie odpowiedzialności jest w diagnozie 2026 luką numer cztery i ma precyzyjną nazwę strukturalną: **współodpowiedzialność bez odpowiedzialnego**. Macierz RACI rozstrzyga ją jedną regułą — dla każdej funkcji krytycznej i każdego obiektu istnieje dokładnie jedna rola „A” (Accountable), obsadzona osobą lub organem, nie zespołem. Brak właściciela na którymkolwiek poziomie przenosi odpowiedzialność w górę i zatrzymuje ją tam, gdzie nie ma instrumentów wykonawczych.

Subsydiarność operacyjna

Centralizacja zwiększa spójność standardu i zmniejsza zdolność reakcji lokalnej; decentralizacja odwrotnie. Program rozstrzyga to napięcie podziałem ról, a nie kompromisem: **centrum ustala standard minimalny, finansuje i audytuje; samorząd, operator i wspólnota wykonują**. Doświadczenie ukraińskie po 2022 r. i doświadczenie pandemiczne wskazują w tę samą stronę: silna odporność jest funkcją silnej samorządności, pod warunkiem, że standard i pomiar pozostają wspólne.

Antyzawłaszczenie jako wymóg konstrukcyjny

Program uruchamia wieloletni strumień zamówień na komponenty ochronne, serwis, energię awaryjną i oprogramowanie. Każdy taki strumień tworzy skoncentrowaną korzyść przy rozproszonym koszcie, czyli klasyczne warunki przechwycenia regulatora. Bezpieczniki muszą być wpisane w architekturę od początku, nie doklejone po pierwszym skandalu: jawność kryteriów i wyników, rejestr konfliktu interesów, rotacja składów oceniających, obowiązkowy plan wyjścia od dostawcy, zakaz uzależnienia funkcji krytycznej od jednego modelu, chmury lub dostawcy oraz niezależny audyt z jawnym raportem.

Bezpiecznik antyneoliberalny

Literatura krytyczna wobec pojęcia odporności wskazuje realne ryzyko: „odporny obywatel” bywa figurą przerzucenia odpowiedzialności z państwa na wspólnotę. Program odrzuca to wprost i czyni z odrzucenia zobowiązanie numer dwanaście. **Odporność obywatelska jest wzmocnieniem, nie substytutem zdolności publicznej**. Standard gotowości domowej, Program 2G i wolontariat zwiększają różnorodność regulatora; nie zwalniają państwa z obowiązku zapewnienia miejsca ochronnego, ostrzeżenia, wody, energii i opieki.

2.6. Test czterech uzasadnień

Tabela jest narzędziem roboczym: kolumny odpowiadają czterem drogom dowodowym z podrozdziałów 2.2–2.5. Każdy zasadniczy mechanizm programu musi mieć wypełnione wszystkie cztery rubryki. Pusta rubryka nie oznacza, że mechanizm jest zły — oznacza, że nie wiadomo, co go utrzyma przy życiu po zmianie rządu, ceny albo priorytetu politycznego.

WARUNEK FALSYFIKACJI

Formuła naczelna byłaby obalona, gdyby dało się wykazać, że państwo osiąga trwałą zdolność działania w kryzysie, utrzymując infrastrukturę, która **nie służy codziennie i nie jest mierzona**.

Doświadczenie fińskie, szwedzkie i szwajcarskie oraz polska diagnoza z lat 1997–2024 wskazują zależność odwrotną: infrastruktura bez pokojowego użytkownika i bez pomiaru degraduje się do wartości ewidencyjnej, a nie operacyjnej.

Mechanizm	Cybernetyka	System	Sieć	Struktura
Narodowy Graf Odporności	Buduje model regulatora (Conant–Ashby).	Wyznacza granicę systemu dla rachunku kosztu.	Ujawnia węzły krytyczne i ścieżki kaskady.	Wymusza jeden słownik i jednego właściciela danych.
Paszport odporności obiektu	Model pojedynczego węzła w modelu regulatora.	Domyka rachunek cyklu życia obiektu.	Zapisuje cztery typy zależności i drugą ścieżkę.	Przypisuje właściciela, zastępcę i termin przeglądu.
Pokrycie operacyjne jako KPI	Sprzężenie zwrotne o stanie zdolności.	Odróżnia zdolność od stanu posiadania.	Liczone po realnych trasach dojścia, nie po promieniu.	Wiąże wynik z odpowiedzialnością organu.
Infrastruktura dual-use	Utrzymuje aktualność modelu przez codzienne użycie.	Obniża koszt netto zdolności w cyklu życia.	Zagęszcza sieć węzłów blisko ludności.	Daje pokojowego właściciela wyniku i budżet utrzymania.
Mikrosieć i praca wyspowa	Poszerza repertuar odpowiedzi regulatora.	Tworzy luz systemowy i degradację łagodną.	Przerywa kaskadę energia–łączność.	Lokalizuje decyzję u operatora obiektu.
Program 2G	Amplifikacja różnorodności regulatora.	Buduje zdolność adaptacyjną, nie tylko absorpcyjną.	Dodaje warstwę słabych więzi do grafu.	Tworzy standard dual-key dla zadań wysokiego wpływu.
RAG ze źródłem i human-in-command	Skraca czas decyzyjny bez oddania mandatu.	Ogranicza pozorną pewność modelu.	Chroni węzeł zaufania przed zatruciem.	Zapewnia ślad decyzji i zaskarżalność.
Publiczny rejestr i audyt obywatelski	Domyka pętlę drugiego rzędu — kontrola regulatora.	Wykrywa nadużycie miernika (Goodhart).	Ujawnia rozbieżność mapy i realnego dojścia.	Bezpiecznik antyzawłaszczeniowy.
Brama stop/go i domknięcie budżetowe	Instrument zmiany decyzji — warunek sprzężenia.	Sekwencja: dyscyplina, priorytety, efektywność.	Kieruje środki do węzłów o najwyższej centralności.	Wiąże rozstrzygnięcie z pozycją planu finansowego.

3. DIAGNOZA 2026: OD LUKI PRAWNEJ DO LUKI WYKONAWCZEJ

Polska posiada dziś ustawową podstawę ochrony ludności i obrony cywilnej. Ustawa z 5 grudnia 2024 r. obowiązuje od 1 stycznia 2025 r., a w 2025 r. wydano kolejne rozporządzenia dotyczące kryteriów uznawania budowli ochronnych, ewidencji, miejsc doraźnego schronienia i warunków technicznych. Nowelizacja z 17 kwietnia 2026 r. uzupełniła system m.in. o rozwiązania dotyczące punktów schronienia. Oznacza to przejście od wieloletniej luki prawnej do luki wykonawczej: inwestycji, kadr, danych, serwisu, ćwiczeń i rozliczalności.

Teza rozdziału (T2). Rama prawna odporności w Polsce dorównuje dziś rozwiązaniom państw nordyckich i bałtyckich. Brakująca część nie jest normatywna, lecz **regulacyjna w sensie cybernetycznym**: między zasobem, wynikiem i decyzją o zasobie nie ma domkniętej pętli.

3.1. Sygnały pozytywne

- Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 przewidział 16,7 mld zł na 2025 r. i 17,2 mld zł na 2026 r.;
- w 2026 r. administracja wskazuje budowę i adaptację schronów, ukryć i miejsc doraźnego schronienia jako priorytet;
- powstały szczegółowe wymagania techniczne dla kategorii ukryć i schronów oraz zasady ich usytuowania;
- ochrona ludności stała się zadaniem własnym jednostek samorządu terytorialnego, co lokalizuje wykonanie tam, gdzie leży wiedza o terenie;
- ustawa zakotwiczyła finansowanie na poziomie nie niższym niż 0,3% PKB, co po raz pierwszy wiąże zadanie z przewidywalnym strumieniem;
- rośnie świadomość potrzeby łączenia ochrony ludności, energii, łączności, medycyny, cyberbezpieczeństwa i logistyki;
- UE i NATO wzmacniają podejście whole-of-society oraz inwestycje w odporność i infrastrukturę dual-use.

3.2. Dwanaście luk systemowych

Wydanie drugie rozszerza katalog o dwie luki wynikające z uzasadnień cybernetycznego i strukturalnego. Każda luka jest opisana jako miejsce, w którym pętla regulacji jest otwarta.

1. **Niepełna inwentaryzacja i niejednolita jakość danych** o rzeczywistej gotowości obiektów — regulator nie ma wiernego modelu obiektu sterowania.
2. **Rozbieżność między pojemnością formalną a operacyjną**: miejscem ewidencyjnym a miejscem, które można bezpiecznie udostępnić w godzinie próby.
3. **Brak wspólnej mapy zależności** między energią, wodą, łącznością, zdrowiem, transportem, finansami i administracją — ryzyko kaskadowe pozostaje niewidoczne aż do momentu realizacji.
4. **Rozproszenie odpowiedzialności** oraz trudność wskazania jednego właściciela wyniku end-to-end: współodpowiedzialność bez odpowiedzialnego.
5. **Niedostateczny budżet cyklu życia**: zakup i remont bez wieloletniego serwisu, testów, wymiany filtrów i odtworzenia zapasów.

6. **Nierówny dostęp regionalny i funkcjonalny**, zwłaszcza dla osób starszych, z niepełnosprawnościami i zależnych od urządzeń medycznych.
7. **Słaba pamięć instytucjonalna**: rozproszone wnioski z ćwiczeń, awarii i kontroli; brak obowiązku zamknięcia zalecenia i ponownego testu.
8. **Uzależnienia od pojedynczych dostawców** energii, chmury, oprogramowania, filtracji i specjalistycznego serwisu — pojedyncze punkty awarii w warstwie logicznej.
9. **Niedostateczna komunikacja ryzyka**: obywatel nie zawsze wie, co jest schronem, ukryciem, miejscem doraźnym i kiedy z nich korzystać.
10. **Przewaga wskaźników aktywności nad wskaźnikami zdolności**: liczymy zakupy i szkolenia zamiast czasu aktywacji i czasu odtworzenia.
11. **Brak instrumentu zmiany decyzji po pomiarze**: wynik pomiaru nie wraca do decyzji budżetowej następnego roku, więc pomiar nie jest sprzężeniem zwrotnym.
12. **Brak kanału algedonicznego**: sygnał o zdarzeniu krytycznym, dla którego nie przewidziano wskaźnika, nie ma drogi omijającej szczyble pośrednie.

3.3. Ryzyka kaskadowe

Tabela nie jest katalogiem zagrożeń, lecz zapisem **sprzężeń między sieciami**. W układach współzależnych zdarzenie początkowe nie degraduje systemu łagodnie: przechodzi w nagłe załamanie wzajemnej łączności przy uszkodzeniu mniejszym niż próg pojedynczej sieci. Dlatego bezpiecznik infrastrukturalny jest zawsze mechanizmem **odcięcia lub drugiej ścieżki**, a nie samym wzmocnieniem węzła.

Zdarzenie początkowe	Efekt kaskadowy	Pierwsza zrywana para sieci	Bezpiecznik infrastrukturalny
Blackout	Brak łączności, wody, płatności, ogrzewania, paliw, leków i danych.	Energia → telekomunikacja	Mikrosieci, black-start, BESS, paliwa, łączność zapasowa, tryb offline.
Cyberatak	Paraliż rejestrów, operatorów, logistyki i komunikacji publicznej.	Sterowanie cyfrowe → usługa fizyczna	Segmentacja, kopie offline, zero trust, ręczne procedury, test wyjścia.
Atak rakietowo-dronowy	Uszkodzenia energetyki, transportu, zdrowia i infrastruktury mieszkaniowej.	Węzły o wysokiej centralności → cała sieć	Schronienie, rozproszenie, zapasy, ochrona pożarowa, odbudowa modułowa.
Powódź / nawałnica	Utrata dróg, zasilania, wody, łączności i dostępu do opieki.	Zależność geograficzna → wszystkie warstwy w strefie	Mapy ryzyka, obiekty poza strefą zalania, mobilne zasoby, alternatywne korytarze.
Awaria chemiczna	Skażenie powietrza, ewakuacja, przeciążenie zdrowia i komunikacji.	Strefa skażenia → transport i zdrowie	Filtrowentylacja, detekcja, izolacja, komunikat, dekontaminacja, triage.
Przerwanie łańcucha dostaw	Brak części, filtrów, leków i komponentów serwisowych.	Zależność logiczna → utrzymanie obiektów	Drugi dostawca, zapas rotowany, kwalifikacja komponentu krajowego.
Operacja informacyjna	Utrata zaufania do komunikatu, chaotyczne zachowania, przeciążenie służb.	Tor poznawczy → wykonanie procedur	Prebunking, wielokanałowość, jawne źródło, ćwiczenia komunikacyjne.

Program przyjmuje regułę analityczną: **plan odtworzenia zaczyna się od wskazania pary sieci, która zerwie się pierwsza**, a nie od listy obiektów do naprawy. Mapa 50 największych podatności kaskadowych, uruchamiana w pierwszych stu dniach, jest zapisem tych par, nie rankingiem obiektów.

DIAGNOZA W JEDNYM ZDANIU

Polsce nie brakuje pojedynczych zasobów ani podstawy prawnej. Brakuje jednolitego systemu, który łączy je w mierzalną zdolność, przypisuje właściciela, zabezpiecza pełny cykl życia i szybko koryguje błąd.

4. ARCHITEKTURA SYSTEMU: 12 FUNKCJI I 8 WARSTW ZDOLNOŚCI



Rysunek 3. Dwanaście funkcji krytycznych, które państwo musi utrzymać w kryzysie.

NATO ujmuje odporność przez ciągłość rządzenia, podstawowych usług i cywilnego wsparcia obrony, opisaną siedmioma wymaganiami bazowymi. Model fiński wyróżnia siedem funkcji życiowych państwa, model singapurski pięć filarów z jawnym filarem psychologicznym. TechnoSanacja rozwija tę logikę do **dwunastu funkcji krytycznych**, ponieważ dwunastka odpowiada polskiej strukturze kompetencyjnej i pozwala przypisać właściciela bez dzielenia jednej funkcji między dwa resorty.

Każda funkcja ma minimalny poziom usługi, maksymalny czas przerwy, właściciela, zastępcę, tryb offline, zasoby, kolejność odtworzenia i ćwiczenie. Myślenie **funkcjami, a nie obiektami**, jest rozstrzygnięciem systemowym: infrastruktura krytyczna to graf zależności państwa widziany od strony zagrożenia, więc chroni się zdolność do wykonania funkcji, a nie budynek, w którym funkcja jest dziś wykonywana.

Funkcja	Minimalny standard	Przykładowy KPI
Kierowanie państwem	Ciągłość decyzji, komunikacji i zastępowalność centrów.	Czas przełączenia centrum kierowania.
Energia	Zasilanie obiektów krytycznych, black-start, mikrosieci.	Godziny autonomii i czas przywrócenia.
Łączność i informacja	Wielokanałowe ostrzeganie i łączność zapasowa.	Odsetek ludności osiągniętej w 10 minut.
Woda i żywność	Bezpieczne dostawy i dystrybucja do osób zależnych.	Dni pokrycia i czas uruchomienia punktów.
Zdrowie	Zdolność masowych zdarzeń, leki, e-zdrowie offline.	Czas zwiększenia pojemności systemu.
Transport i logistyka	Korytarze awaryjne, kolej, porty, paliwa i magazyny.	Czas przywrócenia kluczowego korytarza.
Finanse i płatności	Płatności awaryjne, gotówka, rozliczenia i ubezpieczenia.	Czas przejścia w tryb ciągłości.
Administracja i tożsamość	Obsługa podstawowych spraw i identyfikacja offline.	Odsetek usług dostępnych w trybie degradacji.
Cyberbezpieczeństwo	Detekcja, izolacja, odtworzenie i wymiana informacji.	MTTD / MTTR oraz wyniki ćwiczeń.
Produkcja strategiczna	Zdolność wytwarzania i naprawy komponentów krytycznych.	Czas skalowania 30/90/180 dni.
Porządek i ratownictwo	Zintegrowane działania służb i zasoby mobilne.	Czas dotarcia i dostępność rezerw.
Spójność społeczna	Wiarygodna komunikacja, pomoc lokalna, odporność poznawcza.	Zaufanie do komunikatów i udział w ćwiczeniach.

4.1. Osiem warstw infrastruktury odporności

Warstwy nie są hierarchią ważności, lecz **rekurencją sterowania**: pełna struktura regulacji powtarza się na każdym poziomie — obywatela, obiektu, gminy, regionu i państwa. Kolumna „warunek sterowności” wskazuje, co musi być spełnione, by warstwa w ogóle uczestniczyła w regulacji, a kolumna „odpowiednik w modelu systemu żywotnego” wiąże warstwę z uzasadnieniem cybernetycznym z rozdziału 2.2.

Warstwa	Treść	Warunek sterowności	Odpowiednik VSM
1. Obywatel	Kompetencje, przygotowanie domowe, prawa, wolontariat, Program 2G.	Prosty komunikat i realna rola.	S1 — operacje najniższego poziomu rekurencji
2. Schronienie i ratownictwo	Schrony, ukrycia, MDS, ewakuacja, medycyna i ochrona pożarowa.	Pojemność operacyjna i ćwiczenie.	S1 — operacje
3. Usługi podstawowe	Woda, żywność, zdrowie, ciepło, sanitariaty, płatności.	Minimalny standard i priorytety.	S1 — operacje
4. Energia	Źródła, sieci, magazyny, mikrosieci, paliwa, black-start.	Autonomia i redundancja.	Tor zasilający
5. Logistyka i produkcja	Transport, magazyny, części, serwis, przemysł dual-use.	Zdolność odtworzenia i skalowania.	Akumulator i alimentator
6. Dane i łączność	Rejestry, ostrzeganie, radio, satelity, chmura, kopie offline.	Interoperacyjność i plan wyjścia.	S2 — koordynacja; tor sterowniczy
7. AI i wiedza	RAG, graf zależności, symulacje, cyfrowy bliźniak, lessons learned.	Źródła, logi i human-in-command.	S4 — rozpoznanie
8. Państwo-regulator	Mandat, prawo, budżet, RACI, KPI/KRI, audyt i korekta.	Jeden właściciel wyniku oraz kontrola obywatelska.	S3 i S5 — zarządzanie, audyt, tożsamość

4.2. Standard minimalnej usługi i maksymalnego czasu przerwy

Funkcja krytyczna bez zdefiniowanego poziomu minimalnego jest deklaracją. Program wymaga, by dla każdej z dwunastu funkcji organ odpowiedzialny ustalił i opublikował cztery wartości; ich brak jest w rejestrze traktowany jak brak zdolności, a nie jak brak danych.

Parametr	Znaczenie	Sposób ustalenia
Minimalny poziom usługi	Co jeszcze musi działać, gdy nie może działać wszystko.	Decyzja organu po analizie skutków przerwania, jawna i uzasadniona.
Maksymalny czas przerwy	Po jakim czasie brak usługi staje się nieodwracalny.	Analiza wpływu na życie, zdrowie, prawa i ciągłość pozostałych funkcji.
Kolejność odtworzenia	Co uruchamiamy najpierw przy ograniczonych zasobach.	Wynika z grafu zależności: najpierw węzły, od których zależą inne.
Tryb degradacji	Jak funkcja działa bez informatyki, sieci i jednego budynku.	Procedura ręczna, przećwiczona co najmniej raz w roku.

5. KRAJOWY SYSTEM SCHRONÓW I BUDOWLI OCHRONNYCH



Rysunek 4. Schron jako pełna usługa ochronna: od ostrzeżenia do odtworzenia.

Krajowy system schronienia powinien być traktowany jako sieć usług ochronnych. Jego wynik nie wynika z liczby betonowych pomieszczeń, lecz z liczby sprawnych miejsc, czasu dojścia, adekwatności kategorii ochrony, autonomii instalacji, dostępności, gotowości obsługi i aktualności informacji dla mieszkańców.

Uzasadnienie sieciowe rozdziału. Schron nie jest obiektem samodzielnym, lecz węzłem w co najmniej czterech sieciach jednocześnie: dojścia pieszego, zasilania, łączności i zaopatrzenia. Jego wartość operacyjna równa się wartości najłabszej z tych czterech krawędzi, a nie klasie odporności konstrukcji.

5.1. Typologia prawna i funkcjonalna

Obiekt	Funkcja	Programowa zasada użycia
Schron	Hermetyczna budowla ochronna o najwyższym poziomie zabezpieczenia, z płaszczyzną ochrony i hermetyzacji.	Priorytet dla obszarów najwyższego ryzyka, funkcji krytycznych i dłuższego czasu ochrony.
Ukrycie	Budowla ochronna bez pełnej hermetyzacji, chroniąca m.in. przed odłamkami, gruzem i określonymi skutkami wybuchu.	Gęsta sieć blisko miejsc przebywania ludności.
Miejsce doraźnego schronienia	Przestrzeń przygotowana lub adaptowana na czas zagrożenia, o ograniczonym poziomie ochrony.	Szybkie zwiększenie pokrycia, bez wprowadzania w błąd co do poziomu ochrony.
Punkt schronienia	Miejsce zidentyfikowane jako doraźna możliwość ochrony, zgodnie z ramą po nowelizacji 2026.	Jasne oznakowanie, informacja o ograniczeniach i plan dalszego przemieszczenia.
Obiekt dual-use	Garaż, metro, hala, szkoła, magazyn lub inny obiekt z funkcją pokojową i ochronną.	Konwersja opisana, ćwiczona i możliwa w wymaganym czasie.

5.2. Kategorie i standard — proste objaśnienie

Rozporządzenie MSWiA z 4 listopada 2025 r. ustanowiło techniczne kategorie ukryć U-1, U-2, U-3 oraz schronów S-1, S-2, S-3. Wyższa kategoria oznacza większą odporność na skutki wybuchu i dodatkowe czynniki rażenia. Dokument programowy nie zastępuje projektu technicznego: kategorię dobiera uprawniony zespół na podstawie ryzyka, przeznaczenia, lokalizacji i obowiązujących wymagań.

Wymaganie z ramy 2025	Znaczenie dla programu
Maksymalna odległość planistyczna: 500 m w mieście i 1000 m poza miastem, z uwzględnieniem realnych dróg dojścia.	Mierzymy czas i dostępność, nie wyłącznie promień na mapie. Promień jest miarą euklidesową, a ludzie poruszają się po grafie ulic — różnica bywa dwukrotna.
Minimalna powierzchnia netto co do zasady nie mniejsza niż 1 m ² na osobę.	Pojemność formalna nie może ignorować warunków przebywania, obsługi i osób o ograniczonej mobilności.
Strefy ochronne: do 300 osób w ukryciu; do 1000/2000/3000 w schronach S-1/S-2/S-3.	Duże obiekty wymagają podziału ryzyka, zarządzania tłumem i redundancji instalacji — koncentracja jest ryzykiem topologicznym.
Odporność ogniowa: co najmniej REI 60 dla U-1, REI 120 dla U-2/U-3, REI 240 dla schronów.	Ochrona pożarowa jest częścią zdolności, nie dodatkiem; pożar wtórny jest najczęstszym mechanizmem strat po uderzeniu.
Wymogi dotyczące powietrza, tlenu, CO ₂ , wyjść, energii, wody i instalacji.	Testuje się cały system podtrzymania życia jako jedną całość, a nie pojedynczy komponent.
Uwzględnienie zagrożenia powodzią i wodami gruntowymi.	Mapa schronów musi być zintegrowana z Hydroportalem i lokalnym rozpoznaniem hydrologicznym — to zależność geograficzna w rozumieniu rozdziału 2.4.

5.3. Model docelowy sieci

1. Krajowa macierz zagrożenie — kategoria odporności — funkcja obiektu.
2. Warstwowa sieć: schrony hermetyczne, ukrycia, MDS, punkty schronienia i obiekty dual-use — pięć kategorii jako odpowiedź na pięć różnych klas zaburzeń, zgodnie z prawem wymaganej różnorodności.
3. Priorytetyzacja według ryzyka, gęstości populacji, czasu dojścia, dostępności, stanu technicznego i kosztu uzyskania sprawnego miejsca.
4. Dwa niezależne kierunki ewakuacji oraz analiza strefy zagruzowania tam, gdzie wymagają tego przepisy i projekt — zasada drugiej ścieżki w warstwie obiektu.
5. Filtrowentylacja, nadciśnienie, kontrola CO₂, woda, sanitariaty, energia, łączność i ochrona pożarowa testowane jako jeden system.
6. Centralna Ewidencja OZO z rozróżnieniem pojemności formalnej i operacyjnej, mapą offline oraz kontrolowanym zakresem danych wrażliwych.
7. Plan aktywacji, obsada, role, harmonogram przeglądów, zapasy, instrukcje i regularne ćwiczenia.
8. Projektowanie uniwersalne dla osób z niepełnosprawnościami, seniorów, dzieci i osób zależnych od urządzeń medycznych.
9. Oddzielenie cywilnych obiektów ochronnych od funkcji wojskowych i prawidłowe oznakowanie zgodnie z międzynarodowym prawem humanitarnym.
10. Jawne KPI: pokrycie operacyjne, czas dojścia, czas aktywacji, autonomia, dostępność, ważność przeglądu i koszt miejsca.

5.4. Kolejność budowy sieci: cztery kroki zamiast jednego celu liczbowego

Program świadomie nie stawia celu w postaci liczby schronów. Cel liczbowy przyjęty przed zbudowaniem modelu regulatora prowadzi do optymalizacji wskaźnika, a nie zdolności. Kolejność jest następująca i każdy krok ma bramę stop/go.

Krok	Zawartość	Brama wyjścia
1. Zobacz	Inwentaryzacja, weryfikacja terenowa, rozdzielenie pojemności formalnej i operacyjnej.	Baseline pokrycia operacyjnego z określonym marginesem błędu.
2. Utrzymaj	Przywrócenie sprawności obiektów istniejących: przeglądy, filtry, obsada, oznakowanie.	Odsetek obiektów z ważnym przeglądem i przeciwionizacyjną aktywacją.
3. Zagęść	Adaptacja obiektów dual-use i MDS tam, gdzie czas dojścia przekracza standard.	Mediana i 90. percentyl czasu dojścia w obszarze pilotażowym.
4. Zbuduj	Nowe budowle ochronne tam, gdzie adaptacja nie domyka ryzyka lub kategorii ochrony.	Koszt uzyskania sprawnego miejsca operacyjnego niższy niż wariant alternatywny.

Odwroćenie tej kolejnošci — rozpoczęcie od kroku czwartego — jest najczęstszą przyczyną, dla której programy schronowe w Europie kończyły się rozbudową ewidencji zamiast wzrostem zdolności. Nowy obiekt dodany do systemu, który nie potrafi utrzymać obiektów istniejących, powiększa dług utrzymaniowy zamiast go zmniejszać.

5.5. Paszport odporności obiektu

Paszport jest wersjonowaną kartą obiektu i jednocześnie **rekordem modelu regulatora**. Pola nie są dowolne: każde odpowiada jednej klasie informacji potrzebnej do sterowania. Pola oznaczone jako nowe w wydaniu drugim wynikają z uzasadnienia sieciowego.

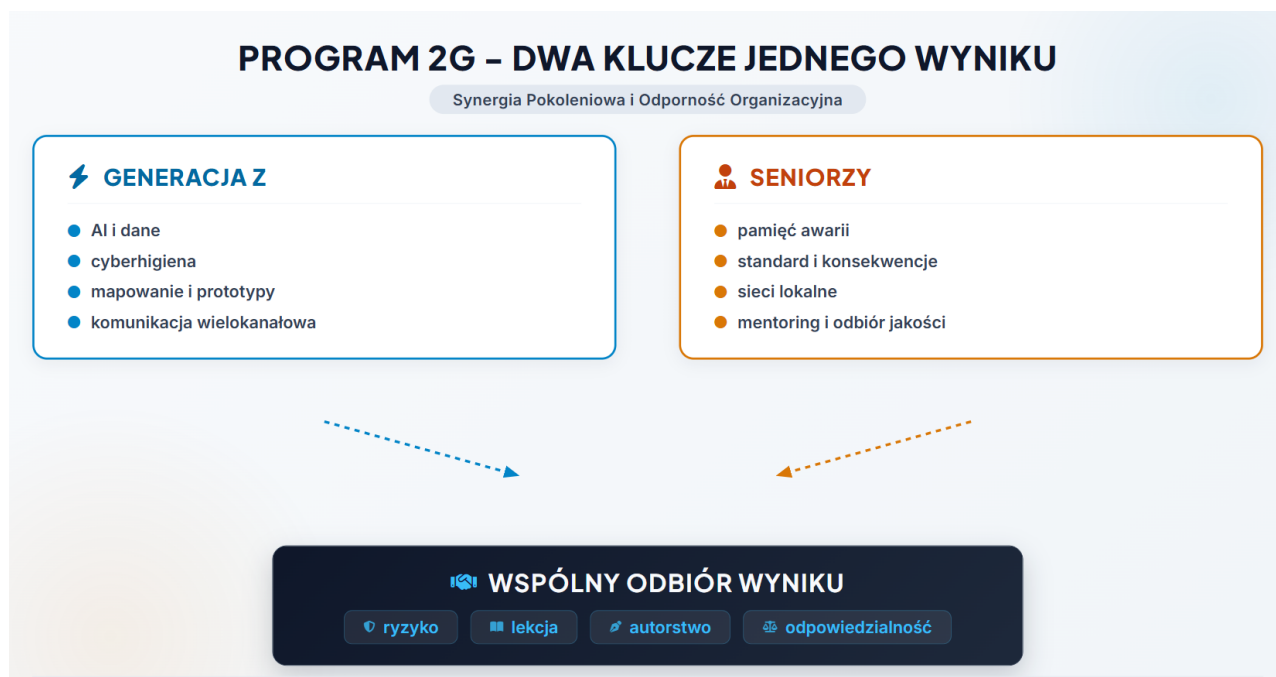
Pole obowiązkowe	Treść
Tożsamość	ID, lokalizacja, właściciel, zarządca, organ odpowiedzialny, kontakt i zastępca.
Funkcja i kategoria	Rodzaj obiektu, kategoria odporności, liczba miejsc formalnych i operacyjnych.
Ryzyko	Zagrożenia dominujące, strefa zalania, zagruzowanie, pożar, skażenie, zależności.
Zależności	Cztery typy zależności: fizyczna, cyfrowa, geograficzna i logiczna — z nazwą węzła, od którego obiekt zależy.
Druga ścieżka	Dla każdej zależności krytycznej: alternatywa, czas przełączenia i koszt uruchomienia.
Instalacje	Filtrowentylacja, energia, woda, sanitariaty, łączność, detekcja, ochrona pożarowa.
Gotowość	Czas aktywacji, obsada, ostatnie ćwiczenie, ważność przeglądu, braki krytyczne.
Dostępność	Trasy, bariery, wózki, osoby niesłyszące i niewidome, osoby zależne od urządzeń.
Cykl życia	CAPEX, OPEX, harmonogram serwisu, części krytyczne, dostawcy, plan wyjścia.
Ślad decyzji	Kto i kiedy potwierdził gotowość, źródła danych, zmiany wersji, działania naprawcze.

BEZ FAŁSZYWEGO BEZPIECZEŃSTWA

Mapa publiczna musi pokazywać poziom ochrony i aktualność danych. Miejsce doraźne nie może być komunikowane jak pełny schron, a obiekt niesprawny nie może zwiększać wskaźnika pokrycia operacyjnego.

Reguła pomiaru: obiekt bez ważnego przeglądu jest liczony jako zero, nie jako wartość poprzednia. Wskaźnik, który nie potrafi spaść, nie jest sprzężeniem zwrotnym.

6. SPOŁECZNA INFRASTRUKTURA ODPORNOŚCI I PROGRAM 2G



Rysunek 5. Program 2G: Generacja Z i seniorzy jako dwa klucze jednego wyniku.

Odporność nie powstaje w dniu alarmu. Powstaje w rodzinie, szkole, zakładzie pracy, wspólnocie mieszkaniowej, przychodni i lokalnej sieci pomocy. Infrastruktura społeczna to zaufanie, kompetencje, role, procedury współdziałania i zdolność dotarcia do osób, które nie poradzą sobie samodzielnie.

Uzasadnienie cybernetyczne rozdziału. Program 2G nie jest programem edukacyjnym ani akcją obywatelską. Jest **amplifikacją różnorodności regulatora**: włączenie obywateli, młodzieży i seniorów zwiększa repertuar odpowiedzi państwa o klasy zaburzeń, których administracja nie obsłuży własnymi kadrami w czasie krytycznym.

Rozstrzygnięcie strukturalne obowiązuje jednak równolegle i jest granicą tego rozdziału: udział obywateli **wzmacnia** zdolność publiczną i nigdy jej nie zastępuje. Odporność nie może stać się alibi dla wycofania państwa ani mechanizmem przerzucenia ryzyka na osoby, które mają najmniej zasobów, by je udźwignąć.

6.1. Powszechny standard przygotowania

- znajomość lokalnych sygnałów alarmowych, źródeł oficjalnych i zasad weryfikacji informacji;
- plan rodzinnego i sąsiedzkiego kontaktu, także bez internetu;
- podstawy pierwszej pomocy, bezpieczeństwa pożarowego i cyberhigieny;
- wiedza o najbliższym schronie, ukryciu, MDS i ograniczeniach danego miejsca;
- minimalna gotowość domowa zgodna z oficjalnymi zaleceniami i potrzebami zdrowotnymi;
- lista osób zależnych, urządzeń medycznych, transportu i punktów ładowania;
- uczestnictwo w lokalnym ćwiczeniu co najmniej raz w roku.

Standard przygotowania domowego przyjęty w Unii Europejskiej i państwach nordyckich opiera się na **minimum 72 godzin samowystarczalności**. Liczba ta nie jest arbitralna:

odpowiada typowemu czasowi, po którym zorganizowana pomoc dociera do większości obszarów po szoku o zasięgu regionalnym. Program przyjmuje ją jako punkt wyjścia, z dwoma zastrzeżeniami wynikającymi z polskiej struktury osadniczej: obszary o niskiej gęstości dróg i mostów wymagają dłuższego bufora, a osoby zależne od urządzeń medycznych i energii wymagają planu indywidualnego, nie standardu zbiorczego.

6.2. Role Generacji Z

- mapowanie danych, testy aplikacji i map offline;
- tworzenie prostych instrukcji multimedialnych i dostępnej komunikacji;
- AI, RAG, cyberhigiena, wykrywanie dezinformacji i analiza źródeł;
- prototypowanie czujników, dashboardów i rozwiązań low-cost;
- reverse mentoring dla seniorów i lokalnych organizacji.

6.3. Role seniorów

- pamięć awarii, procedur ręcznych i lokalnych zależności;
- mentoring techniczny i branżowy;
- ocena praktyczności instrukcji oraz skutków długiego trwania;
- sieci sąsiedzkie i identyfikacja osób wymagających wsparcia;
- audyt jakości, standard zawodowy i ochrona ciągłości wiedzy.

Obie grupy wnoszą do grafu odporności **różne zbiory słabych więzi**. Informację nową przenoszą kontakty spoza własnego środowiska, dlatego wartość Programu 2G nie leży w symbolicznej reprezentacji pokoleń, lecz w tym, że młodzież i seniorzy docierają do rozłącznych części społeczności lokalnej. Kapitał wiążący bez pomostowego utrwała izolację — miernikiem programu jest więc zasięg dotarcia do osób zależnych, a nie liczba uczestników szkoleń.

6.4. Standard dual-key

Zadanie wysokiego wpływu — mapa ryzyka, instrukcja aktywacji, karta obiektu, komunikat alarmowy — jest przygotowywane i odbierane przez co najmniej dwie perspektywy: twórcę lub prototypującego oraz doświadczonego mentora lub audytora. Rozbieżności są zapisywane, a decyzja ma właściciela.

Dual-key jest lokalną postacią zasady kontroli regulatora z rozdziału 2.2: obserwator zadania nie może być tożsamy z jego wykonawcą. Zasada ma trzy warunki praktyczne — rozbieżność musi być **zapisana, a nie uzgodniona w rozmowie**, decyzja musi mieć jedną osobę odpowiedzialną, a zapis rozbieżności wchodzi do pamięci instytucjonalnej nawet wtedy, gdy ostatecznie okazał się nie trafny.

6.5. Odporność poznawcza

Tor poznawczy jest w warunkach współczesnego kryzysu atakowany równolegle z torem fizycznym. Program przyjmuje trzy rozstrzygnięcia i jedną twardą granicę.

Rozstrzygnięcie	Treść	Dlaczego tak
Uodpornianie wyprzedzające zamiast prostowania po fakcie	Uprzedzające pokazanie mechanizmu manipulacji, ćwiczone i powtarzane.	Prewencja działa mierzalnie lepiej niż korekta, ale efekt zanika — konieczne są powtórzenia, nie jednorazowa kampania.
Wzmacnianie odbiorcy zamiast kontroli treści	Edukacja medialna, jawność źródła, pluralizm kanałów, protokół krytycznej oceny źródła.	Państwo, które definiuje prawdę, podważa zasadę, której broni; odporność buduje się po stronie odbiorcy.
Zaufanie warstwowo, nie hurtowo	Budowanie zaufania do instytucji i do źródeł, z jawnym wskazaniem niepewności.	Wysokie zaufanie uogólnione bywa w kryzysie czynnikiem podatności, bo rozluźnia ostrożność.

GRANICA OBRONY POZNAWCZEJ

Państwo ma obowiązek bronić toru poznawczego Narodu przed wrogą operacją wpływu i przed przechwyceniem przez prywatnego regulatora platformowego.

Państwu **nie wolno** stosować wobec własnych obywateli niejawnej manipulacji, której samo się broni. Ta granica oddziela odporność od propagandy państwowej i jest w programie regułą ustrojową.

HASŁO 2G

Młodzi przyspieszają rozpoznanie. Seniorzy chronią ciągłość i jakość. Wspólny wynik jest ważniejszy niż symboliczna reprezentacja pokoleń.

7. ENERGIA, WODA, ZDROWIE, ŻYWNOŚĆ, TRANSPORT I ŁĄCZNOŚĆ

Schron bez energii i wody, szpital bez leków, administracja bez łączności i przemysł bez komponentów tworzą pozór odporności. Dlatego obiekty ochronne muszą być wpięte w lokalne i regionalne ekosystemy usług podstawowych.

Uzasadnienie cybernetyczne rozdziału. Rozdział opisuje **tor zasilający** układu. Tor sterowniczy — dane, łączność, decyzja — jest przedmiotem rozdziału 9. Układ samodzielny traci samodzielność, gdy przerwany zostaje którykolwiek z torów; żaden nie jest ważniejszy, a inwestycja wyłącznie w jeden z nich nie zwiększa zdolności.

7.1. Cytadela odporności — węzeł dual-use

Moduł	Funkcja pokojowa	Funkcja kryzysowa
Mikrosieć	Lokalne bilansowanie, niższe koszty, elastyczność.	Wyspowe zasilanie centrum wsparcia i obiektów krytycznych.
BESS / magazyn	Usługi elastyczności i zarządzanie szczytem.	Autonomia i stabilizacja po zaniku sieci.
Źródło sterowalne	Ciepło, energia, usługa dla przemysłu.	Black-start i zasilanie priorytetowe.
Centrum danych / łączność	Usługi cyfrowe, edukacja, biznes i administracja.	Kopia krytycznych rejestrów, łączność zapasowa i tryb offline.
Budowla ochronna	Parking, sport, magazyn, edukacja.	Schronienie, centrum dowodzenia cywilnego, punkt pomocy.
Magazyn rotowany	Zwykła logistyka i rezerwa handlowa.	Woda, żywność, leki, filtry, części i środki higieny.
Warsztat / fablab	Naprawy, edukacja techniczna, prototypy.	Produkcja części, naprawy, drony ratownicze i łączność.

Cytadela jest odpowiedzią na ustalenie sieciowe: **praca wyspowa przerywa kaskadę**. Węzeł zdolny odciąć się od systemu nadrzędnego i utrzymać pięć funkcji lokalnie zamienia nagłe załamanie wzajemnej łączności w proces stopniowy i odwracalny. Z tego powodu kryterium lokalizacji cytadeli nie jest dostępność terenu, lecz **centralność pośrednictwa** w sieciach zasilania, łączności i logistyki regionu.

7.2. Minimalne zasady ciągłości

Domena	Zasada programu	Test
Energia	N+1 dla funkcji krytycznych; mikrosieć; paliwo; magazyn; ręczne obejścia.	Czy obiekt działa po utracie sieci i jednego generatora?
Woda	Źródło podstawowe, rezerwa, monitoring jakości, dystrybucja do osób zależnych.	Ile godzin i dni działa bez wodociągu?
Zdrowie	Triage, leki, tlen, dane offline, zasilanie urządzeń i transport pacjentów.	Jak szybko system zwiększa pojemność?
Żywność	Rotowane zapasy, umowy ramowe, alternatywne magazyny i transport.	Czy zapas jest aktualny i dystrybucja przewidziana?
Transport	Korytarze alternatywne, priorytet służb, paliwo, kolej i porty.	Czy istnieje sprawny objazd i plan utrzymania?
Łączność	Cell broadcast, radio, satelita, sieci lokalne, punkty fizyczne.	Czy komunikat dociera bez internetu i jednej sieci komórkowej?
Sanitariaty i higiena	Zaopatrzenie, odbiór nieczystości, środki higieniczne, rozwiązania bezwodne.	Czy obiekt utrzymuje warunki sanitarne przez zakładany czas przebywania?

Zasada N+1 jest w tym dokumencie rozumiana systemowo, a nie urządzeniowo. Drugi generator zasilany z tego samego zbiornika paliwa, tą samą trasą serwisową i przez tego samego dostawcę części nie jest redundancją, lecz **powieleniem tej samej zależności logicznej**. Test redundancji polega na wskazaniu, które ogniwo pozostaje wspólne dla obu ścieżek.

7.3. Odporność blisko mieszkańca

Każdy powiat powinien zidentyfikować węzły, które w kryzysie łączą minimum pięć funkcji: informację, zasilanie, wodę, pierwszą pomoc i schronienie. W mieście może to być szkoła z mikrosiecią i ukryciem; na obszarze wiejskim — remiza lub centrum usług z agregatem, radiem i zapasem wody; w regionie przemysłowym — cytadela energetyczno-cyfrowa z warsztatem i magazynem.

Wybór węzłów jest decyzją wielokryterialną i program zaleca prowadzenie jej jawnie, według ustalonej wcześniej listy kryteriów i wag, a nie w trybie uznaniowym. Minimalny zestaw kryteriów obejmuje: ryzyko dominujące, liczbę mieszkańców w zasięgu czasu dojścia, stan techniczny, koszt uzyskania sprawnego miejsca w cyklu życia, dostępność dla osób zależnych, odporność zasilania i istnienie właściciela zdolnego utrzymać obiekt. Jawność kryteriów i wag jest tu bezpiecznikiem antyzawłaszczeniowym: ranking oparty na jawnej formule jest weryfikowalny, ranking uznaniowy — nie.

7.4. Minimalne czasy autonomii — katalog startowy

Wartości są **punktem wyjścia do kalibracji regionalnej**, nie normą prawną. Organ odpowiedzialny ustala je dla konkretnego obiektu na podstawie ryzyka dominującego, liczby użytkowników i czasu dotarcia pomocy, a następnie publikuje wraz z uzasadnieniem.

Zasób	Punkt wyjścia dla węzła lokalnego	Punkt wyjścia dla cytadeli regionalnej
Zasilanie elektryczne	72 godziny bez uzupełnienia paliwa	7 dni z planem uzupełniania i zdolnością black-start
Woda pitna	72 godziny dla pojemności operacyjnej	7 dni z ujęciem własnym lub rezerwą wymienną
Łączność	dwa niezależne kanały, w tym jeden bez internetu	trzy niezależne kanały, w tym satelitarny
Zapasy medyczne	pierwsza pomoc i leki ratunkowe	zdolność triage i wsparcia zdarzenia masowego
Filtry i materiały eksploatacyjne	komplet wymienny na miejscu	zapas regionalny z rotacją i serwisem krajowym

8. GOSPODARKA ODPORNOŚCI I KRAJOWY PRZEMYSŁ DUAL-USE

Rynek sam nie finansuje pełnej redundancji, zapasów i zdolności, które ujawniają wartość dopiero w kryzysie. Państwo ma uzasadnioną rolę jako projektant standardów, pierwszy wymagający klient, operator rezerw i orkiestrator ekosystemu — pod warunkiem jawnego wyniku, konkurencji i ochrony przed przechwyceniem.

Uzasadnienie systemowe rozdziału. Redundancja jest dobrem publicznym: przedsiębiorstwo nie internalizuje społecznej korzyści z zapasu, którego samo nie użyje, dlatego rynek systematycznie niedodostarcza odporności. To jest tytuł do interwencji. Symetrycznie: nadmiar rezerw ma policzalny koszt fiskalny i zaburza rynek, więc **celem jest optymalny bufor pod policzone ryzyko, nie maksimum zapasów.**

8.1. Krajowy łańcuch dostaw infrastruktury odporności

Segment	Zdolności krajowe do rozwinięcia	Mechanizm popytu
Konstrukcje ochronne	Prefabrykaty, betony specjalne, drzwi, zamknięcia, elementy modułowe.	Typowe projekty, certyfikacja, zamówienia wieloletnie.
Filtrowentylacja CBRN	Filtry, wentylatory, zawory, sensory, detekcja i serwis.	Minimalny udział serwisu krajowego i zapas części.
Energia awaryjna	Agregaty, BESS, falowniki, mikrosieci, sterowanie i black-start.	Pilotaże w szkołach, szpitalach i obiektach OZO.
Łączność	Radio, satelita, mesh, syreny, cell broadcast, terminale offline.	Interoperacyjne standardy i testy wielokanałowe.
Woda i sanitariaty	Zbiorniki, uzdatnianie, pompy, toalety, monitoring jakości.	Zakupy ramowe i rotowane zapasy.
Dane i software	Rejestry OZO, GIS, RAG, cyfrowy bliźniak, cyberochrona.	Otwarte API, przenoszalność, kod krytyczny pod kontrolą.
Serwis i szkolenia	Inspektorzy, operatorzy, projektanci, instruktorzy i audytorzy.	Krajowy system kwalifikacji i utrzymania kompetencji.

Kryterium suwerenności w tym rozdziale nie oznacza autarkii. Oznacza **zdolność utrzymania i audytu warstwy** oraz realną możliwość zmiany dostawcy: dla każdego komponentu krytycznego musi istnieć albo producent krajowy, albo dwaj niezależni dostawcy sojusznicy, albo zapas pokrywający czas przebrojenia. Reshoring pełny tworzy nowe koncentracje i sam bywa źródłem ryzyka; dywersyfikacja z kwalifikowanym zapasem jest rozwiązaniem tańszym i odporniejszym.

8.2. Finansowanie według cyklu życia

- CAPEX nie może być przyznawany bez wieloletniego OPEX i właściciela utrzymania;
- koszt miejsca ochronnego liczy się wraz z serwisem, energią, przeglądami, ćwiczeniami i wymianą komponentów;
- dual-use może obniżać koszt netto, ale przychód pokojowy nie może uniemożliwiać szybkiej konwersji;

- finansowanie publiczne powinno być etapowe: koncepcja — projekt — test — odbiór — ćwiczenie — utrzymanie;
- projekty wysokiego ryzyka wymagają rezerwy kosztowej, ubezpieczenia i jawnej analizy wariantów;
- w zamówieniach strategicznych stosuje się plan wyjścia, interoperacyjność i ograniczenie vendor lock-in;
- transfer ryzyka jest planowany przed zdarzeniem, a nie po nim: warstwa buforów własnych, fundusz rezerwowy i instrument rynkowy dla ryzyk katastroficznych;
- bufor fiskalny buduje się w okresach dobrej koniunktury, ponieważ po szoku zdolność ich budowy spada wraz z potrzebą.

Sekwencja reformy finansowania jest w programie rozstrzygnięta i wynika z doświadczeń międzynarodowych: najpierw **dyscyplina agregatowa** (znany, przewidywalny strumień), potem **alokacja według priorytetów** (portfel misji zamiast rozproszonych zadań), a dopiero na końcu **efektywność operacyjna** (optymalizacja kosztu jednostkowego). Odwrócenie kolejności — zaczynanie od optymalizacji kosztu jednostkowego przy nieustalonym strumieniu — produkuje oszczędności pozorne i dług utrzymaniowy.

8.3. Zamówienie na wynik

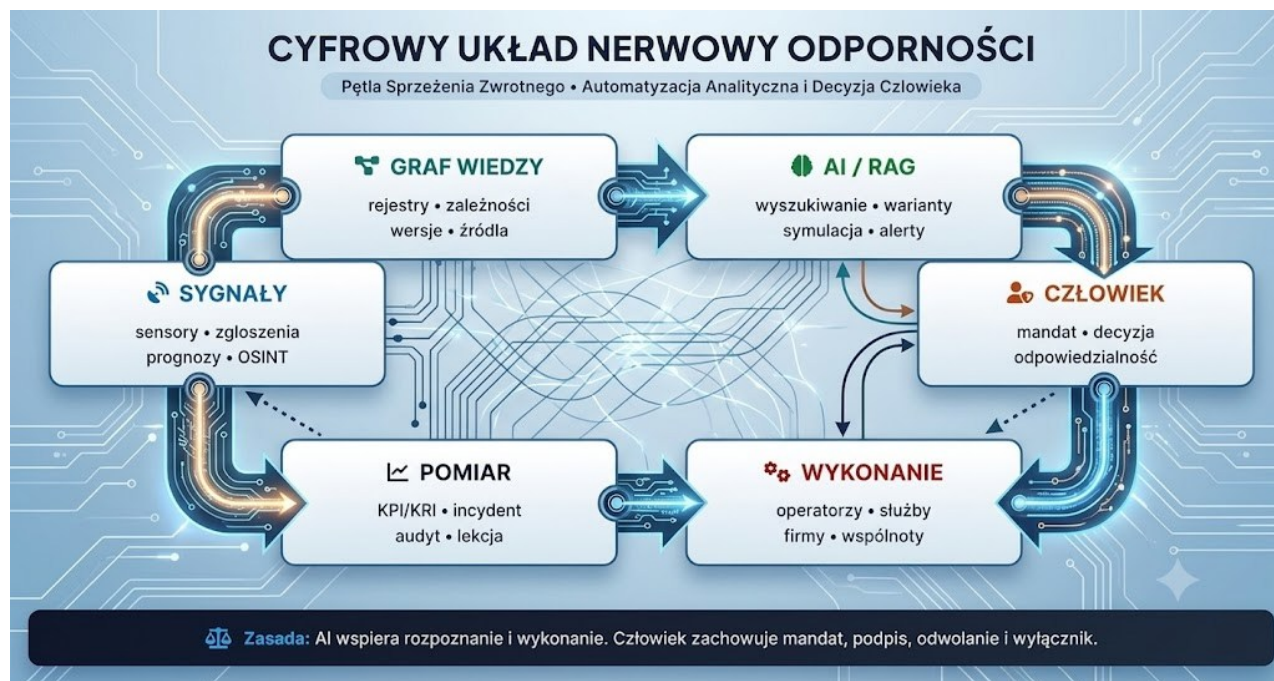
Nie kupujemy	Kupujemy
samej liczby urzędzeń	utrzymaną przez lata zdolność ochronną
samego remontu	obiekt gotowy, przećwiczony i serwisowalny
zamkniętego systemu IT	interoperacyjność, eksport danych i plan migracji
jednorazowego szkolenia	kompetencję potwierdzaną ćwiczeniem i aktualizacją
materiału promocyjnego	komunikat zrozumiały, dostępny i skuteczny w teście
samej pojemności nominalnej	pojemność operacyjną potwierdzoną audytem
deklaracji dostępności komponentu	zakwalifikowany drugi dostawca i zapas na czas przebrojenia

8.4. Bezpieczniki antyzawłaszczeniowe portfela

Wieloletni strumień zamówień na komponenty ochronne, serwis i oprogramowanie tworzy skoncentrowaną korzyść przy rozproszonym koszcie — czyli warunki sprzyjające przechwyceniu decydenta. Bezpieczniki muszą być elementem konstrukcji programu od pierwszego dnia.

Ryzyko	Bezpiecznik	Dowód wykonania
Przechwycenie standardu przez jednego producenta	Standard funkcjonalny zamiast produktowego; konsultacje jawne; okres przejściowy.	Publiczny rejestr uwag i uzasadnienie przyjęcia lub odrzucenia.
Uzależnienie od dostawcy technologii	Obowiązkowy plan wyjścia, eksport danych, test migracji w cyklu.	Wykonany test wyjścia z raportem i terminem powtórzenia.
Konflikt interesów w ocenie ofert	Rejestr konfliktu interesów, rotacja składów, rozdział oceny technicznej i decyzji.	Jawny skład, oświadczenia i ścieżka odwoławcza.
Kaptura regulacyjna przez eksperta	Pluralizm ekspercki, jawność opinii, obowiązek zdania odrębnego.	Publikacja opinii mniejszości wraz z decyzją.
Wydatek bez wyniku	Brama stop/go, powiązanie kolejnej transzy z potwierdzonym miernikiem.	Protokół bramy z decyzją i uzasadnieniem.

9. AI, RAG, CYFROWY BLIŹNIAK I PAMIĘĆ PAŃSTWA



Rysunek 6. Cyfrowy układ nerwowy odporności: sygnały, graf wiedzy, AI/RAG, decyzja człowieka, wykonanie i pomiar.

System odporności potrzebuje wspólnego modelu rzeczywistości. Dane o obiektach, dostawcach, energii, wodzie, ludności, zdrowiu, drogach, zapasach i incydentach muszą tworzyć aktualny graf zależności. AI może skracać pętlę rozpoznania, lecz nie otrzymuje samoistnego mandatu do ograniczania praw ani podejmowania decyzji wysokiego wpływu.

Uzasadnienie cybernetyczne rozdziału. Rozdział opisuje **tor sterowniczy** i jest bezpośrednim wykonaniem twierdzenia o dobrym regulatorze. Automatyzacja zwiększa wymaganą różnorodność regulatora **tylko wtedy, gdy pętla naprawcza nadąża za wolumenem**; w przeciwnym razie rośnie wyłącznie przepustowość błędu.

9.1. Narodowy Graf Odporności

- obiekty i funkcje krytyczne oraz ich właściciele;
- zależności w czterech typach: fizyczne, cyfrowe, geograficzne i logiczne — energia, woda, łączność, transport, dostawcy, serwis, kadry i dane;
- ryzyka geograficzne: powódź, pożar, przemysł, zagruzowanie, dostępność dróg;
- zasoby: miejsca ochronne, magazyny, agregaty, BESS, filtry, leki, pojazdy i kompetencje;
- miary topologiczne: centralność pośrednictwa węzła, istnienie drugiej ścieżki, przynależność do pary sieci o wysokim ryzyku kaskady;
- historia przeglądów, ćwiczeń, incydentów, napraw i zmian wersji;
- poziomy dostęp: informacja publiczna, operacyjna i chroniona.

Graf ma dwa zastosowania rozłączne i oba są obowiązkowe. **Zastosowanie planistyczne:** wskazanie od dwudziestu do pięćdziesięciu węzłów, których utrata kaskaduje na co najmniej dwie inne warstwy — i to one, a nie „ważne instytucje”, są przedmiotem ostony. **Zastosowanie operacyjne:** w czasie zdarzenia graf odpowiada na pytanie, co przestanie działać w następnej kolejności i w jakim czasie. Model nieodświeżany formalnie istnieje, lecz regulacja przestaje działać; przy dużej nieaktualności obserwacji korekta zaczyna wzmacniać odchylenie zamiast je znosić.

9.2. RAG — odpowiedź ze źródłem

Retrieval-Augmented Generation powinno odpowiadać wyłącznie na podstawie zatwierdzonego, wersjonowanego korpusu: ustaw, rozporządzeń, planów, instrukcji, kart obiektów i raportów z ćwiczeń. Każda odpowiedź pokazuje źródło, wersję, datę, zakres uprawnień i poziom niepewności. Rekomendacja bez wskazanego źródła nie może stanowić podstawy decyzji publicznej.

Korpus RAG jest zasobem o randze infrastruktury krytycznej i wymaga ochrony właściwej dla takiego zasobu: kontroli proveniencji dokumentu, izolacji pamięci, wykrywania zatrucia danych oraz modelu braku domyślnego zaufania w dostępie. Zatrucie korpusu jest atakiem na tor sterowniczy państwa i skutkuje nie błędem pojedynczej odpowiedzi, lecz systematycznym przesunięciem decyzji.

9.3. Minimalny standard agenta AI

Element	Wymaganie
Tożsamość	ID agenta, tożsamość maszynowa, właściciel, rola, zakres danych i narzędzi.
Mandat	Jasne zadanie, zakazane działania, poziom autonomii i termin przeglądu.
Uprawnienia minimalne	Dostęp wyłącznie do danych i narzędzi niezbędnych do zadania; brak uprawnień dziedziczonych.
Bezpieczeństwo	Segmentacja, sandbox, ochrona pamięci, testy odporności i red team.
Ślad	Log źródeł, zapytań, rekomendacji, decyzji człowieka i wykonania.
Human-in-command	Człowiek zatwierdza decyzje wysokiego wpływu i odpowiada za skutek.
Zatrzymanie	Kill switch, circuit breaker, tryb ręczny i plan działania bez modelu.
Odwwołanie	Prawo do wyjaśnienia, korekty danych i decyzji człowieka.
Plan wyjścia	Możliwość migracji, zastąpienia modelu i utrzymania funkcji krytycznej.

Zasada human-in-command jest definiowana przez **warunki, nie przez obecność człowieka w procedurze**. Warunki są trzy: odwracalność działania, symetria uzasadnienia (decyzja wsparta modelem jest uzasadniana tak samo jak decyzja wyłącznie ludzka) oraz zaskarżalność. Człowiek, który zatwierdza rekomendację bez możliwości jej zakwestionowania i bez czasu na ocenę, nie sprawuje kontroli — pełni funkcję podpisu.

9.4. Cyfrowy bliźniak

Cyfrowy bliźniak regionu lub funkcji krytycznej służy do testowania scenariuszy przed wdrożeniem: blackout z awarią telekomunikacji; uderzenie i pożar; powódź z utratą mostu; skażenie i ewakuacja; cyberatak na operatora. Model nie jest wyrocznią. Wyniki wymagają walidacji, analizy wrażliwości, red teamingu i decyzji odpowiedzialnego człowieka.

Wartość bliźniaka polega na czymś innym niż przewidywanie: pozwala **zidentyfikować założenia fałszywe zanim zweryfikuje je przeciwnik lub katastrofa**. Dlatego obowiązkowym produktem każdej symulacji jest nie rekomendacja, lecz lista założeń, których obalenie zmieniłoby wynik, wraz ze wskazaniem, jak te założenia sprawdzić w terenie.

9.5. Pamięć państwa

Siódma luka diagnozy — słaba pamięć instytucjonalna — jest rozwiązywana strukturalnie, nie technologicznie. Repozytorium wniosków ma trzy cechy obowiązkowe: **każdy wniosek ma właściciela i termin, zamknięcie wniosku wymaga ponownego testu, a wnioski nieudane są przechowywane na równi z udanymi**. Organizacja, która archiwizuje wyłącznie sukcesy, traci informację o tym, co nie działa, i powtarza ten sam błąd w kolejnym cyklu.

CZERWONA LINIA

Zakaz niejawnego profilowania politycznego, komercyjnego wykorzystywania danych kryzysowych, automatycznego ograniczania praw oraz uzależnienia funkcji krytycznej od jednego modelu, chmury lub dostawcy.

Zakaz obejmuje także **wtórne wykorzystanie danych kryzysowych** do celów niezwiązanych z zagrożeniem, dla którego zostały zebrane, oraz przekazanie takich danych podmiotowi, wobec którego państwo nie ma instrumentu egzekucji.

10. ZARZĄDZANIE, PRAWA OBYWATELSKIE I ODPOWIEDZIALNOŚĆ

Odporność bez praw może prowadzić do państwa nadzoru. Prawa bez zdolności prowadzą do państwa bezsilnego. Program łączy sprawczość z demokratycznymi i technicznymi bezpiecznikami.

Uzasadnienie strukturalne rozdziału. To jest miejsce, w którym domykają się obie pętle jednocześnie: pętla pierwsza — zdolność regulatora do sterowania; pętla druga — zdolność Narodu do kontrolowania regulatora. Program, który domyka tylko pierwszą, buduje państwo nadzoru; program, który domyka tylko drugą, buduje proceduralną wydmuszkę.

10.1. Struktura odpowiedzialności

Poziom	Rola w programie	Produkt obowiązkowy
Naród	Mandat, kontrola i korekta strategiczna.	Prawo do informacji, debaty i rozstrzygnięcia spraw fundamentalnych.
Prezydent / egzekutywa	Właściciel Narodowej Strategii Odporności i ciągłości państwa.	Portfel misji, budżet, właściciele funkcji i decyzje międzysektorowe.
Senat 100	Prawo, budżet, kontrola i wystuchanie publiczne.	Komisja odporności, jawny raport roczny, kontrola założeń.
Centrum Odporności i Ciągłości	Integracja ryzyk, danych, ćwiczeń i alarmów.	Rejestr ryzyk, dashboard, graf zależności, kanał alarmowy.
Administracja terenowa	Lokalne wykonanie i integracja służb.	Plan regionalny, mapa obiektów, SLA, ćwiczenia i działania naprawcze.
Sejmiki / wspólnoty	Lokalna wiedza i społeczna kontrola.	Opinia regionalna, lista ryzyk, zdanie odrębne, ocena dostępności.
Operatorzy i firmy	Utrzymanie infrastruktury i dostaw.	Plan ciągłości, paszport odporności, testy wyjścia i raport incydentów.
NGO, uczelnie, 2G	Współprodukcja kompetencji i niezależny sygnał zwrotny.	Pilotaże, szkolenia, audyty obywatelskie i repozytorium wiedzy.

Struktura jest odwzorowaniem modelu systemu żywego na poziomie państwa: Naród pełni funkcję organizatora zdolnego zmienić program układu, egzekutywa — zarządzania bieżącego, Senat i audyt — homeostatu odróżniającego zakłócenie od szumu, Centrum — rozpoznania i koordynacji, administracja terenowa i operatorzy — operacji. Usunięcie któregoś z poziomów nie przenosi jego funkcji na pozostałe: funkcja po prostu przestaje być wykonywana.

10.2. Karta praw obywatela w systemie odporności

- prawo do szybkiego, zrozumiałego i wielokanałowego ostrzeżenia;
- prawo do informacji o poziomie ochrony, aktualności danych i ograniczeniach obiektu;
- prawo do minimalnego standardu podstawowych usług także w trybie ograniczonym lub offline;
- prawo do równego dostępu, projektowania uniwersalnego i wsparcia osób zależnych;
- prawo do prywatności, minimalizacji danych i zakazu wtórnego wykorzystania niezgodnego z celem;
- prawo do wyjaśnienia udziału AI, danych, kryteriów i osoby zatwierdzającej;
- prawo do korekty danych, odwołania i niezależnego rozpatrzenia;
- prawo do wygaśnięcia środków nadzwyczajnych i jawnego uzasadnienia ich przedłużenia.

Ostatnie prawo jest bezpiecznikiem najważniejszym i najczęściej pomijanym. Środek nadzwyczajny wprowadzony bez daty wygaśnięcia nie wymaga decyzji o utrzymaniu — trwa domyślnie. Program wymaga konstrukcji odwrotnej: **każdy środek ograniczający prawa wygasa automatycznie, a jego przedłużenie wymaga jawnego uzasadnienia, wskazania organu i nowej decyzji.** To przeniesienie ciężaru dowodu jest technicznym wykonaniem zasady kontroli regulatora.

10.3. RACI dla obiektu i funkcji

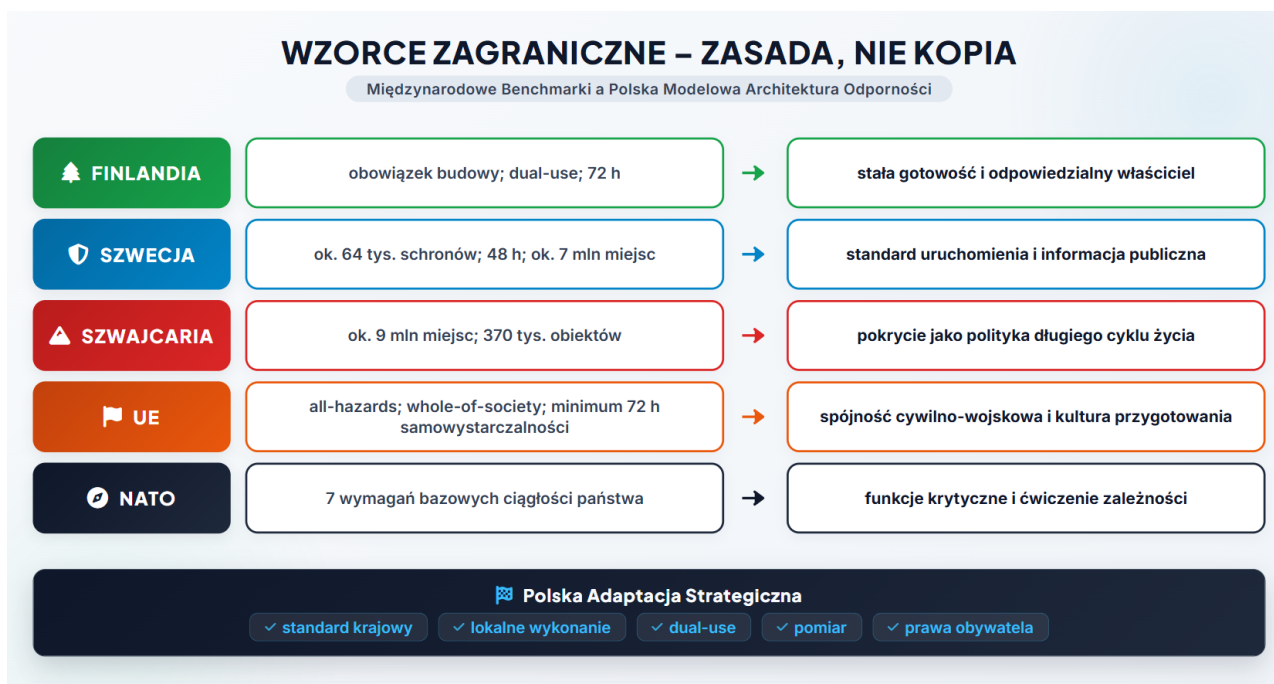
Rola	Znaczenie	Przykład
R — Responsible	Wykonuje zadanie i raportuje.	Zarządca obiektu, operator, służba, wykonawca.
A — Accountable	Jedna osoba lub organ odpowiada za wynik.	Właściciel funkcji krytycznej lub organ ochrony ludności.
C — Consulted	Dostarcza wiedzę i opinię.	Projektant, PSP, sanepid, operator energii, zespół 2G.
I — Informed	Otrzymuje informację o statusie i zmianach.	Mieszkańcy, użytkownicy, Senat, sejmik, media.

Reguła jest jedna i nie podlega negocjacji: **dla każdej funkcji krytycznej i każdego obiektu istnieje dokładnie jedna rola „A”, obsadzona osobą lub organem, nigdy zespołem.** Dwie osoby odpowiedzialne oznaczają zero osób odpowiedzialnych. Brak roli „A” na którymkolwiek poziomie przenosi odpowiedzialność w górę i zatrzymuje ją tam, gdzie nie ma już instrumentów wykonawczych.

10.4. Granica między sprawczością a nadzorem

Zdolność programu	Bezpiecznik równoważący	Kto go egzekwuje
Zbieranie danych o obiektach, zasobach i zależnościach	Minimalizacja danych, poziomy jawności, zakaz wtórnego użycia.	Organ ochrony danych, audyt niezależny, sąd.
Rejestr ludności zależnej i wsparcia indywidualnego	Zgoda, cel związany, termin usunięcia, dostęp rolami z logowaniem.	Organ prowadzący rejestr, audyt obywatelski.
Środki nadzwyczajne i ograniczenia praw	Automatyczne wygaśnięcie, jawne uzasadnienie przedłużenia.	Senat, sądy, kontrola konstytucyjna.
Systemy wspomagania decyzji i agencji AI	Rejestr algorytmów, ślad decyzji, human-in-command, zaskarżalność.	Organ nadzoru, audyt techniczny, obywatel w trybie odwołania.
Wieloletni portfel zamówień	Jawne kryteria, rejestr konfliktu interesów, plan wyjścia, rotacja.	Najwyższy organ kontroli, opinia publiczna, konkurenci rynkowi.

11. MODELE ZAGRANICZNE I POLSKA ADAPTACJA



Rysunek 7. Wzorce zagraniczne: zasady do adaptacji, a nie mechaniczne kopiowanie.

Modele zagraniczne pokazują, że infrastruktura odporności wymaga dziesięcioleci konsekwentnej polityki, jasnej odpowiedzialności właściciela, dual-use, regularnych przeglądów i wiarygodnej informacji publicznej. Polska powinna adaptować zasady do własnego prawa, geografii, zasobów i struktury osadniczej.

Model	Doświadczenie	Element do adaptacji w Polsce
Finlandia	Schrony często pełnią funkcje sportowe, parkingowe i magazynowe; muszą być możliwe do uruchomienia w 72 godziny. Obowiązek budowy jest szeroki i powiązany z nową zabudową. Model bezpieczeństwa kompleksowego opisuje siedem funkcji życiowych państwa.	Dual-use, odpowiedzialność właściciela, plan konwersji, regularna konserwacja i edukacja obywateli.
Szwecja	Okolo 64 tys. schronów i ok. 7 mln miejsc; gotowość w 48 godzin; publiczna mapa i jasne zasady korzystania; obrona totalna z jawnym komponentem informacyjnym.	Standard czasu aktywacji, publiczna informacja, obowiązki właściciela i test wyposażenia.
Szwajcaria	Okolo 9 mln miejsc w ok. 370 tys. obiektów; zasada miejsca dla mieszkańca przy lokalnych różnicach; nacisk na utrzymanie wartości istniejącej infrastruktury.	Długoterminowe pokrycie, finansowanie utrzymania, planowanie lokalnych luk i odpowiedzialność prywatnych właścicieli.
Singapur	Pięć filarów obrony totalnej z wyodrębnionym filarem psychologicznym.	Uznanie odporności poznawczej za osobną zdolność z własnym właścicielem i miernikiem.
UE — Unia Gotowości	Podjęcie all-hazards, whole-of-society i whole-of-government; wytyczne minimum 72 godzin samowystarczalności; infrastruktura dual-use i ćwiczenia.	Jedna architektura ryzyk, edukacja, partnerstwo publiczno-prywatne, standardy minimum i wspólne ćwiczenia.
NATO	Trzy funkcje: ciągłość rządzenia, podstawowych usług i wsparcie operacji wojskowych; siedem wymagań bazowych z oceną spełnienia.	Włączenie odporności cywilnej do planowania obronnego i testowanie zależności między sektorami.

Wspólny mianownik wszystkich sześciu modeli nie leży w liczbach, lecz w trzech zasadach: **właściciel obiektu odpowiada za jego gotowość, obiekt ma funkcję pokojową i spełnienie wymogu jest oceniane, a nie deklarowane**. Siedem wymagań bazowych NATO działa wyłącznie wtedy, gdy towarzyszy im pomiar spełnienia; bez niego lista funkcji staje się katalogiem intencji.

POLSKA DROGA

Nie kopiujemy liczby schronów ani jednego terminu. Budujemy własny standard oparty na ryzyku, prawie, gęstości ludności, dostępności, kosztach cyklu życia i realnych zdolnościach przemysłu.

Warunki brzegowe, których żadna adaptacja nie zmieni: położenie na osi zagrożenia bez naturalnej reduty na wschodzie, rozproszona struktura osadnicza, pozycja pomostowa między korytarzami północ-południe i wschód-zachód.

12. KPI, KRI, PUBLICZNY REJESTR I NIEZALEŻNY AUDYT

PUBLICZNY PULPIT ODPORNOŚCI - CO NAPRAWDĘ MIERZYM



Każdy KPI: definicja • źródło • właściciel • częstotliwość • próg ostrzegawczy • próg krytyczny • plan korekty.

Rysunek 8. Publiczny pulpit odporności: zdolność, nie aktywność administracyjna.

Pomiar jest w tym programie nie narzędziem sprawozdawczym, lecz **warunkiem istnienia sterowania**. Odporność nieopomiarowana pozostaje deklaracją; to jest treść tezy T1. Pomiar bez instrumentu zmiany decyzji nie jest jednak sprzężeniem zwrotnym, lecz jego imitacją — dlatego rozdział kończy się regułą domknięcia budżetowego.

12.1. KPI — mierniki wyniku

KPI	Definicja programowa	Częstotliwość
Pokrycie operacyjne	Odsetek ludności z dostępem do miejsca faktycznie sprawnego i możliwego do uruchomienia.	kwartalnie / rocznie
Czas dojścia	Mediana i 90. percentyl rzeczywistej trasy do właściwego obiektu.	rocznie + po zmianach
Czas aktywacji	Czas od polecenia do gotowości obiektu i obsady.	każde ćwiczenie
Autonomia	Godziny i dni działania energii, wody, sanitariatów, powietrza i łączności.	kwartalnie
Dostępność	Odsetek miejsc i tras zgodnych z potrzebami osób o ograniczonej mobilności i sensorycznymi.	rocznie
Aktualność danych	Odsetek obiektów z ważnym przeglądem, kartą i potwierdzoną lokalizacją.	miesięcznie
Odtworzenie funkcji	Rzeczywisty czas powrotu do minimalnej usługi po incydencie.	po incydencie
Krajowy serwis	Udział komponentów, części i serwisu dostępnych w Polsce lub w odpornym łańcuchu.	rocznie
Uczenie	Odsetek działań naprawczych wykonanych w terminie i ponownie przetestowanych.	kwartalnie
Druga ścieżka	Odsetek węzłów krytycznych z potwierdzoną alternatywą i zmierzonym czasem przełączenia.	półrocznie

12.2. KRI — wskaźniki ryzyka

Każdy KPI ma przypisany KRI, który wykrywa jego nadużycie. Jest to bezpośrednio wykonanie prawa Goodharta: miernik, który staje się celem, przestaje być dobrym miernikiem, więc obok każdej miary wyniku musi stać miara wykrywająca optymalizację samej miary.

KRI	Próg ostrzegawczy — przykład	Reakcja
Przegląd nieważny	poniżej 95% obiektów z aktualnym przeglądem.	Wstrzymanie liczenia do pokrycia operacyjnego; plan naprawczy.
Brak obsady	mniej niż 2 przeszkolonych zastępców dla funkcji.	Szkolenie i umowa wsparcia między jednostkami.
Vendor lock-in	Brak eksportu danych lub alternatywnego serwisu.	Test wyjścia, plan migracji, ograniczenie nowych zakupów.
Autonomia energii	Poniżej standardu dla danej funkcji lub obiektu.	Priorytet BESS, paliwa, mikrosieci i test black-start.
Niedostępna trasa	Wzrost czasu dojścia lub bariera dla osób zależnych.	Zmiana mapy, transport wspomagany, alternatywny obiekt.
Niezamknięte działania	powyżej 10% zaleceń krytycznych po terminie.	Eskalacja do właściciela i jawny status.
Niezgodność danych	Różnica pojemności formalnej i operacyjnej bez wyjaśnienia.	Audyt źródła, korekta rejestru i komunikatu.
Wzrost wskaźnika bez zmiany w terenie	Poprawa KPI niepotwierdzona kontrolą losową.	Test zaskoczenia i weryfikacja metody liczenia.
Koncentracja topologiczna	Rosnący udział jednego węzła w obsłudze funkcji.	Rozproszenie, budowa drugiej ścieżki, limit koncentracji.

12.3. Publiczny rejestr i poziomy jawności

Poziom	Co jest jawne	Co jest chronione
Publiczny	Lokalizacja i rodzaj obiektu, poziom ochrony, aktualność, dostępność, ogólna gotowość i instrukcja.	Szczegóły, których ujawnienie zwiększa ryzyko sabotażu.
Operacyjny	Obsada, kontakty, instalacje, zapasy, dostawcy, działania naprawcze.	Dostęp rolami, logowanie, potrzeba wiedzy.
Chroniony	Szczegóły wrażliwe bezpieczeństwa, odporności konstrukcji, systemów i procedur.	Szyfrowanie, segmentacja, kontrola dostępu i audyt.

Podział jawności jest rozstrzygnięciem, a nie kompromisem między przejrzystością a bezpieczeństwem. Obywatel potrzebuje wiedzieć **gdzie, jaki poziom ochrony i jak aktualne dane** — bez tego mapa publiczna produkuje fałszywe poczucie bezpieczeństwa. Przeciwnik szuka natomiast **szczegółów konstrukcyjnych, obsady i zależności serwisowych**. Te dwa zbiory są w znacznej mierze rozłączne i program korzysta z tej rozłączności zamiast wybierać między jawnością a ochroną.

12.4. Niezależny audyt

- audyt techniczny obiektu i instalacji;
- audyt organizacyjny: role, obsada, umowy, procedury i ćwiczenia;
- audyt danych i cyberbezpieczeństwa;
- audyt dostępności i praw obywatelskich;
- audyt finansowy pełnego cyklu życia;
- audyt topologiczny: weryfikacja drugiej ścieżki i koncentracji zależności;
- red team i test zaskoczenia;
- jawny raport wniosków, z wyjątkiem informacji chronionych;
- obowiązek zamknięcia zaleceń i ponownego testu.

12.5. Narodowy Indeks Odporności

Indeks jest rocznym, jawnym zestawieniem zdolności państwa. Program przyjmuje trzy zasady jego konstrukcji, wynikające z doświadczeń międzynarodowych z indeksami odporności.

Zasada	Treść	Dlaczego
Nierankingowość	Indeks pokazuje mocne i słabe strony jednostki, nie miejsce w tabeli.	Ranking uruchamia optymalizację pozycji zamiast zdolności.
Rozdzielenie dwóch prędkości	Osobno mierzona zdolność odbicia i zdolność przeskoku naprzód.	System dobry w powrocie do normy bywa bezradny wobec szoku trwałego.
Najstabsze ogniwo, nie średnia	Wynik funkcji równa się wynikowi jej najstabszej warstwy.	Średnia ukrywa pojedynczy punkt awarii, który decyduje o realnej zdolności.

13. MAPA DROGOWA: 100 DNI — 10 LAT



Rysunek 9. Mapa drogowa: etapowanie, bramy stop/go i skalowanie po potwierdzeniu wyniku.

Kolejność etapów wynika z prawa Conwaya i z zasady domknięcia pętli: **mandat przed systemem, model przed inwestycją, pomiar przed skalowaniem**. Odwrócenie tej kolejności jest najczęstszą przyczyną, dla której programy odporności kończą się rozbudową ewidencji zamiast wzrostem zdolności.

13.1. Pierwsze 100 dni

- powołanie właściciela programu i Prezydenckiego Centrum Odporności i Ciągłości;
- przyjęcie 12 funkcji krytycznych oraz jednolitego słownika KPI/KRI;
- uruchomienie Krajowego Rejestru Ryzyk z podziałem na ryzyka ostre i chroniczne oraz mapy 50 największych podatności kaskadowych;
- inwentaryzacja danych o OZO, energii, wodzie, zdrowiu, łączności i logistyce;
- wybór trzech pilotaży: metropolia, powiat średni i obszar wiejski lub przygraniczny;
- baseline: pokrycie operacyjne, czas aktywacji, autonomia i aktualność danych;
- karta praw obywatela i standard jawności informacji;
- uruchomienie kanału sygnału pilnego z progami, oknem czasowym i skutkiem uzgodnionym przed kryzysem.

13.2. Dwanaście miesięcy

- pierwszy Narodowy Indeks Odporności i publiczny dashboard;
- paszporty odporności dla obiektów pilotażowych, z polami zależności i drugiej ścieżki;
- Narodowy Graf Odporności i źródłowy RAG;
- pierwsze ćwiczenie wielosektorowe z utratą energii i łączności;
- Program 2G w każdym pilotażu;
- pilotaże mikrosieci, łączności zapasowej, map offline i konwersji dual-use;
- program krajowych kwalifikacji dla projektantów, inspektorów, zarządców i operatorów.

13.3. Trzy lata

- przećwiczone plany regionalne i mapa realnego pokrycia;
- aktualne paszporty odporności dla priorytetowych obiektów;
- wielokanałowe ostrzeganie i test dostępności;
- rotowane rezerwy i umowy uruchamiane w kryzysie;
- krajowe łańcuchy serwisu filtrowentylacji, energii awaryjnej i łączności;
- coroczne ćwiczenia lokalne i krajowe oraz audyt działań naprawczych.

13.4. Pięć lat

- sieć mikrosieci, magazynów energii i zdolności black-start dla funkcji krytycznych;
- redundantne centra danych i suwerenna infrastruktura dla rejestrów krytycznych;
- cytadele odporności w każdym regionie;
- program modernizacji i budowy OZO według ryzyka i kosztu miejsca operacyjnego;
- finansowanie cyklu życia i ubezpieczenia ryzyka infrastruktury;
- pełne testy wyjścia od dostawców krytycznych.

13.5. Dziesięć lat

- Polska jako regionalne centrum infrastruktury odporności, energii, logistyki, cyberbezpieczeństwa, AI i produkcji dual-use;
- pokrycie operacyjne zgodne z przyjętymi standardami ryzyka i dostępności;
- krajowy przemysł komponentów ochronnych i serwisu eksportujący do regionu Europy Środkowej;
- żywy system wiedzy i wniosków z ćwiczeń, awarii i odbudowy;
- społeczeństwo regularnie ćwiczące przygotowanie bez militaryzacji życia codziennego.

BRAMA STOP/GO

Każdy etap kończy się decyzją opartą na wyniku, kosztach pełnego cyklu życia, bezpieczeństwie, prawach obywatela i zdolności utrzymania rozwiązania. Pilotaż bez potwierdzonego wyniku nie jest automatycznie skalowany.

Domknięcie budżetowe: rozstrzygnięcie programu bez pozycji w planie finansowym, bez terminu i bez właściciela rezultatu nie jest rozstrzygnięciem, lecz opinią.

14. PORTFEL PROJEKTÓW PILOTAŻOWYCH

Pilotaż	Zakres	Wynik po 12 miesiącach
Metropolia 2G	Mapa OZO i czasu dojścia, metro i garaże dual-use, komunikacja dostępna, zespół Gen Z-seniorzy.	Zweryfikowane pokrycie operacyjne, mapa offline, ćwiczenie i plan inwestycji.
Powiat odporności	Węzeł: remiza, szkoła lub przychodnia, mikrosieć, łączność, magazyn, punkt medyczny.	Minimalna usługa przez określony czas po utracie sieci i internetu.
Cytadela energetyczno-cyfrowa	Podziemny lub wzmocniony obiekt, energia, BESS, centrum danych, łączność, centrum kryzysowe, warsztat.	Test black-start, ciągłość rejestrów, plan wsparcia regionu.
Fabryka odporności	Konsorcjum produkcji drzwi, filtrów, zaworów, sensorów, BESS i oprogramowania.	Kwalifikacja komponentów, serwis krajowy i plan skali 30/90/180 dni.
RAG Ochrony Ludności	Wersjonowany korpus prawny i operacyjny, wyszukiwarka źródłowa, tryb offline.	Odpowiedzi ze źródłem, logiem i testem błędów; brak decyzji autonomicznych.
Szkoła gotowości	Program edukacyjny, ćwiczenia, pierwsza pomoc, cyberhigiena, mapowanie lokalne.	Przećwiczona społeczność, dostępne instrukcje i sieć wsparcia osób zależnych.
Audyt obywatelski	Publiczny dashboard, rejestr działań naprawczych, losowe testy zaskoczenia.	Wiarygodność danych i zamknięcie zaleceń krytycznych.
Mapa zależności regionu	Graf węzłów i krawędzi, symulacja kaskad, lista węzłów o najwyższej centralności.	Lista 20–50 węzłów krytycznych z planem drugiej ścieżki i kosztem.

14.1. Karta projektu pilotażowego

Pole	Wymaganie
Problem	Jednoznaczna podatność lub funkcja do utrzymania.
Właściciel	Jedna osoba lub organ odpowiedzialny za wynik.
Użytkownicy	Mieszkańcy, osoby zależne, operatorzy, służby i odbiorcy.
Baseline	Stan przed projektem: czas, pokrycie, autonomia, ryzyko, koszt.
Rezultat	Mierzalna zdolność po projekcie.
KPI/KRI	Definicje, źródła danych, progi i częstotliwość.
Wariant zerowy	Co się stanie, jeżeli projekt nie zostanie zrealizowany — jawnie opisany i wyceniony.
Bezpieczniki	Prawa, prywatność, dostępność, cyber, human-in-command.
Cykl życia	CAPEX, OPEX, serwis, kadry, zapasy i wymiana komponentów.
Bramy	Koncepcja, test, odbiór, ćwiczenie, utrzymanie, skalowanie.
Lekcja	Co zmieniono po błędzie i kto zatwierdził nową wersję.

15. TEST GOTOWOŚCI ORGANIZACJI I WSPÓLNOTY

Test ma charakter edukacyjny. Nie zastępuje audytu, projektu technicznego, wymogów prawa ani instrukcji służb. Jego celem jest wykrycie pierwszej luki, którą można naprawić.

Pytanie	Tak / częściowo / nie	Dowód
Czy każda funkcja krytyczna ma właściciela i zastępcę?		Imię, mandat, kontakt, procedura zastępstwa.
Czy określono minimalny poziom usługi i maksymalny czas przerwy?		SLA ciągłości i priorytety odtworzenia.
Czy system działa bez internetu, jednego budynku i jednej kluczowej osoby?		Wynik ćwiczenia lub testu.
Czy znamy dostawców krytycznych, części, zapasy i alternatywy?		Mapa zależności i umowy.
Czy dla każdej zależności krytycznej istnieje druga ścieżka i znany czas przełączenia?		Zapis w paszporcie obiektu i wynik testu przełączenia.
Czy dane są aktualne, wersjonowane i dostępne offline?		Raport jakości i kopia testowa.

Pytanie	Tak / częściowo / nie	Dowód
Czy komunikat jest zrozumiały dla Gen Z, seniorów i osób z niepełnosprawnościami?		Test użytkowników 2G i dostępności.
Czy obiekt ochronny ma aktualny paszport, obsadę i plan aktywacji?		Przegląd, instrukcja, lista obsady.
Czy po ostatnim incydencie lub ćwiczeniu zamknięto działania naprawcze?		Rejestr zaleceń i ponowny test.
Czy istnieje plan wyjścia od dostawcy technologii lub chmury?		Eksport danych, alternatywa, termin migracji.
Czy wynik pomiaru wraca do decyzji o zasobach w następnym cyklu?		Pozycja w planie finansowym powiązana z miernikiem.
Czy obywatel zna status, źródło, właściciela i drogę odwołania?		Publiczny interfejs i procedura odwołania.

15.1. Interpretacja

Wynik	Znaczenie	Pierwszy krok
A — większość „tak”	Podstawy istnieją, lecz wymagają testu zaskoczenia.	Ćwiczenie wielosektorowe i audyt działań naprawczych.
B — wiele „częściowo”	Zdolność jest niepełna lub nieudokumentowana.	Przypisz właścicieli, standardy, terminy i dowody.
C — wiele „nie”	Wysoka podatność i ryzyko fałszywego bezpieczeństwa.	Wybierz jedną funkcję krytyczną i zbuduj minimalny plan ciągłości.

PIERWSZY KROK

Jedno źródło. Jedna mapa zależności. Jedna poprawiona procedura. Jedno ćwiczenie. Państwo odporne powstaje przez tysiące zamkniętych pętli korekty, nie przez jedną kampanię.

16. TEST ZGODNOŚCI Z FORMUŁĄ NACZELNĄ I NAPIĘCIA NIEROZSTRZYGNIE

Rozdział zamyka pętlę dokumentu: sprawdza, czy rozstrzygnięcia przyjęte w rozdziałach 1–15 są zgodne z formułą naczelną, i wskazuje jawnie te napięcia, których wydanie drugie nie rozstrzyga. Jawne wskazanie nierozstrzygnięć jest w tym programie warunkiem wiarygodności, a nie przyznaniem się do braku.

16.1. Test zgodności rozdziałów z formułą

Rozdział	Który człon formuły realizuje	Dowód zgodności
1. Definicja i sens	Wszystkie cztery systemy	Cztery rodzaje infrastruktury jako warunki konieczne, nie klasyfikacja.
2. Cztery drogi dowodowe	Koherencja systemów	Test czterech uzasadnień dla każdego mechanizmu programu.
3. Diagnoza	Tworzą odporność — zdolność, nie deklarację	Luki opisane jako miejsca otwarcia pętli regulacji.
4. Architektura	System polityczny i technologiczny	Dwanaście funkcji z właścicielem, standardem i miernikiem.
5. Schrony	Służą codziennie	Dual-use jako reguła projektowa; kolejność zobacz–utrzymaj–zagęść–zbuduj.
6. Program 2G	System społeczny	Amplifikacja różnorodności regulatora z bezpiecznikiem antyneoliberalnym.
7. Usługi podstawowe	Tor zasilający czterech systemów	Zasady ciągłości z testem dla każdej domeny.
8. Gospodarka odporności	System gospodarczy	Redundancja jako dobro publiczne z jawnym kosztem cyklu życia.
9. AI i pamięć państwa	System technologiczny	Model regulatora z human-in-command i czerwonymi liniami.
10. Zarządzanie i prawa	System polityczny	Domknięcie obu pętli: sterowania i kontroli nad regulatorem.
11. Modele zagraniczne	Służą codziennie	Trzy wspólne zasady wzorców zamiast kopiowania liczb.
12. Mierniki i audyt	Tworzą odporność	KPI z przypisanym KRI i regułą domknięcia budżetowego.
13.–15. Wykonanie	Do działania w sytuacjach kryzysowych	Bramy stop/go, karta projektu, test gotowości z dowodem.

16.2. Napięcia nierozstrzygnięte

Napięcie	Stan w dokumencie
Centralizacja standardu a autonomia wykonania	Rozstrzygnięte: centrum ustala standard minimalny, finansuje i audytuje; wykonanie po stronie samorządu, operatora i wspólnoty.
Jawność mapy obiektów a ryzyko sabotażu	Rozstrzygnięte: trzy poziomy jawności oparte na rozłączności zbiorów informacji potrzebnej obywatelowi i przeciwnikowi.
Odporność obywatelska a obowiązek państwa	Rozstrzygnięte: wzmocnienie, nigdy substytut; zobowiązanie dwunaste.
Automatyzacja decyzji a odpowiedzialność człowieka	Rozstrzygnięte: human-in-command definiowany przez odwracalność, symetrię uzasadnienia i zaskarżalność.
Skala dual-use a gwarancja szybkiej konwersji	Nierozstrzygnięte: brak polskich danych o realnym czasie konwersji obiektów; wymaga pomiaru w trzech pilotażach przed przyjęciem standardu czasu.
Wysokość optymalnego bufora rezerw	Nierozstrzygnięte: wymaga jawnej wyceny kosztu utrzymania i policzonego ryzyka dla każdej kategorii zapasu osobno.
Tempo programu a zdolność absorpcyjna administracji i przemysłu	Nierozstrzygnięte: wymaga oceny zdolności wykonawczej przed skalowaniem; ryzyko wydatku bez wyniku.
Premia za suwerenność komponentu a koszt inwestycji	Nierozstrzygnięte: wymaga jawnej wyceny premii dla każdej kategorii komponentu krytycznego.
Docelowy poziom pokrycia operacyjnego	Świadomie nieustalony: cel liczbowy przyjęty przed zbudowaniem modelu regulatora prowadzi do optymalizacji wskaźnika zamiast zdolności.

16.3. Warunki, przy których program należałoby zmienić

- gdyby pomiar w pilotażach wykazał, że koszt uzyskania sprawnego miejsca w obiekcie dual-use przewyższa koszt obiektu dedykowanego w pełnym cyklu życia;
- gdyby czas konwersji obiektów dual-use okazał się systematycznie dłuższy niż czas ostrzegania właściwy dla polskiego położenia;
- gdyby publiczna mapa obiektów wykazała mierzalny wzrost ryzyka sabotażu przewyższający korzyść informacyjną dla mieszkańców;
- gdyby indeks odporności okazał się sterowany metodą liczenia, a nie stanem terenu — co wykryje test zaskoczenia i kontrola losowa;
- gdyby zdolność absorpcyjna administracji i przemysłu nie pozwalała wykonać portfela bez obniżenia jakości poniżej standardu minimalnego.

Program, który nie wskazuje warunków własnej zmiany, nie jest doktryną sprawdzalną, lecz deklaracją. Powyższe pięć warunków jest przedmiotem corocznego sprawozdania i wchodzi do agendy przeglądu strategii.

ANEKS A. SŁOWNIK POJĘĆ, TERMINÓW I SKRÓTÓW

Słownik obejmuje 132 hasła w sześciu grupach. Objasnienia podano w znaczeniu, jakie termin ma **w tym dokumencie**; tam, gdzie pojęcie ma definicję ustawową, znaczenie programowe jej nie zastępuje i nie modyfikuje.

A.1. Skróty, akronimy i oznaczenia

Skrót	Rozwinięcie	Znaczenie w dokumencie
AI	Artificial Intelligence — sztuczna inteligencja	Narzędzie skracania pętli rozpoznania; nigdy samodzielny podmiot decyzji wysokiego wpływu.
BESS	Battery Energy Storage System	Akumulatorowy magazyn energii; w pokoju usługa elastyczności, w kryzysie autonomia obiektu.
CAPEX	Capital Expenditure	Nakład inwestycyjny; w programie nieprzyszwany bez zapewnionego OPEX i właściciela utrzymania.
CBRN	Chemical, Biological, Radiological, Nuclear	Zagrożenia chemiczne, biologiczne, radiologiczne i nuklearne; przedmiot filtrowentylacji i detekcji.
CER	Critical Entities Resilience (dyrektywa UE 2022/2557)	Rama odporności podmiotów krytycznych obejmująca wprost adaptację i odtworzenie po incydencie.
CEOZO	Centralna Ewidencja Obiektów Zbiorowej Ochrony	Rejestr obiektów ochronnych; w programie z rozdzieleniem pojemności formalnej i operacyjnej.
CO ₂	Dwutlenek węgla	Parametr kontrolowany w budowlach ochronnych jako miara jakości powietrza i obciążenia.
DC	Data Center — centrum danych	Węzeł ciągłości rejestrów i usług cyfrowych; w cytadeli moduł dual-use.
Dual-use	Podwójne zastosowanie	Rozwiązanie służące funkcjom cywilnym i ochronnym; w programie reguła projektowa, nie oszczędność.
FIMI	Foreign Information Manipulation and Interference	Zagraniczna manipulacja informacyjna i ingerencja — atak na tor poznawczy państwa.
GIS	Geographic Information System	System informacji geograficznej; podstawa analizy czasu dojścia i stref ryzyka.
Human-in-command	Człowiek w dowodzeniu	Człowiek zachowuje mandat, kontrolę i odpowiedzialność; warunkiem są odwracalność, symetria uzasadnienia i zaskarżalność.
KPI	Key Performance Indicator	Miernik wyniku i zdolności, z właścicielem, definicją i częstotliwością.

Skrót	Rozwinięcie	Znaczenie w dokumencie
KRI	Key Risk Indicator	Wskaźnik ryzyka z progiem alarmowym; przypisany do KPI jako bezpiecznik przed nadużyciem miary.
KSE	Krajowy System Elektroenergetyczny	Najwyższy poziom bilansowania energii; punkt odniesienia dla pracy wyspowej.
MDS	Miejsce doraźnego schronienia	Przestrzeń przygotowana lub adaptowana na czas zagrożenia, o ograniczonym poziomie ochrony.
MTTD	Mean Time to Detect	Średni czas wykrycia incydentu; miernik warstwy cyberbezpieczeństwa.
MTTR	Mean Time to Recover / Repair	Średni czas odtworzenia lub naprawy; miernik zdolności regeneracyjnej.
NIS2	Network and Information Security 2 (dyrektywa UE 2022/2555)	Rama wysokiego wspólnego poziomu cyberbezpieczeństwa; warstwa cyfrowa odporności.
N+1	Redundancja jednostkowa	Jedna jednostka zapasowa ponad zapotrzebowanie; w programie liczona systemowo, nie urządzeniowo.
OPEX	Operating Expenditure	Koszt utrzymania w cyklu życia: serwis, energia, przeglądy, ćwiczenia, wymiana komponentów.
OZO	Obiekt zbiorowej ochrony	Zbiorcza nazwa budowli ochronnych i miejsc schronienia w polskiej ramie prawnej.
PKB	Produkt Krajowy Brutto	Odniesienie dla ustawowego poziomu finansowania ochrony ludności.
RACI	Responsible, Accountable, Consulted, Informed	Macierz ról; reguła programu: dokładnie jedna rola „A” dla funkcji i obiektu.
RAG	Retrieval-Augmented Generation	Generowanie odpowiedzi wyłącznie na podstawie wskazanych, wersjonowanych źródeł.
RCB	Rządowe Centrum Bezpieczeństwa	Organ koordynacyjno-doradczy zarządzania kryzysowego; punkt odniesienia dla Centrum Odporności i Ciągłości.
REI	Nośność, szczelność, izolacyjność ogniowa	Klasa odporności ogniowej elementu budowlanego, wyrażona w minutach.
S-1 / S-2 / S-3	Kategorie schronów	Techniczne kategorie schronów według polskich przepisów; wyższa oznacza większą odporność.
SLA	Service Level Agreement	Mierzalny standard usługi i czasu; w programie zapis minimalnego poziomu i maksymalnej przerwy.

Skrót	Rozwinięcie	Znaczenie w dokumencie
U-1 / U-2 / U-3	Kategorie ukryć	Techniczne kategorie ukryć według polskich przepisów.
VSM	Viable System Model — model systemu żywotnego	Model Beera: pięć podsystemów koniecznych do przeżycia organizacji na każdym poziomie rekurencji.
Zero trust	Brak domyślnego zaufania	Model bezpieczeństwa: ciągła weryfikacja tożsamości i uprawnień, także wewnątrz sieci.
2G	Generacja Z i seniorzy	Program współpracy dwóch pokoleń jako amplifikator różnorodności regulatora.
3A	Antycypacja — Absorpcja — Adaptacja	Model porządkujący TechnoSanacji; trzy pytania testujące każdy element systemu.

A.2. Pojęcia cybernetyczne

Pojęcie	Znaczenie w dokumencie
Cybernetyka	Nauka o sterowaniu i komunikacji w układach złożonych. W dokumencie: język opisu odporności jako układu regulacyjnego.
Regulator	Podsystem utrzymujący wybrane zmienne układu w wyznaczonych granicach mimo zakłóceń. Tu: państwo w funkcji sterowania odpornością.
Twierdzenie o dobrym regulatorze	Conant–Ashby: każdy dobry regulator układu musi być modelem tego układu. Podstawa obowiązku posiadania aktualnego grafu zależności i paszportów obiektów.
Prawo wymaganej różnorodności	Ashby: tylko różnorodność może pochłoniąć różnorodność. Repertuar odpowiedzi regulatora nie może być mniejszy niż repertuar zagrożeń.
Amplifikacja różnorodności	Zwiększanie repertuaru regulatora przez włączenie obywateli, samorządów i przedsiębiorstw. Uzasadnienie Programu 2G.
Atenuacja różnorodności	Zmniejszanie strumienia informacji wejściowej przez agregację. Dopuszczalna wobec danych o systemie, zakazana wobec profilowania obywateli.
Cybernetyka drugiego rzędu	Ujęcie, w którym obserwator jest częścią obserwowanego systemu. Przenosi problem z „jak sterować lepiej” na „kto pilnuje sterującego”.
Układ samodzielny	Układ zdolny przeciwdziałać utracie zdolności sterowania; składa się z receptora, korelatora, efektora, homeostatu, akumulatora i alimentatora.
Receptor	Blok poboru informacji. Tu: czujniki, rejestry, obserwacja obywatelska, meldunki służb, dane operatorów.
Korelator	Blok przetwarzania informacji w decyzje wraz z pamięcią norm. Tu: centrum kryzysowe, analiza, RAG, cyfrowy bliźniak.

Pojęcie	Znaczenie w dokumencie
Efektor	Blok wykonania oddziaływań. Tu: służby, zarządcy obiektów, operatorzy, wykonawcy, wspólnoty.
Homeostat	Blok samokorekty odróżniający zakłócenie od szumu. Tu: audyt niezależny, kontrola parlamentarna, sądy, audyt obywatelski.
Akumulator i alimentator	Bloki gromadzenia i zasilania energomaterią. Tu: magazyny rotowane, paliwa, BESS, łańcuch dostaw i serwis.
Organizator	Organ zdolny zmienić program własnego układu. W państwie: władza ustrojodawcza i Naród, nie egzekutywa.
Tor sterowniczy	Kanał informacji, którym układ steruje: dane, łączność, modele, przekaz publiczny.
Tor zasilający	Kanał energomaterii umożliwiający wykonanie: energia, woda, paliwa, części, leki, żywność.
Moc swobodna	Zasób, którym układ dysponuje na działanie samodzielne. Tu: niezaangażowana rezerwa zdolności, zapasów i mocy wytwórczych.
Czas decyzyjny	Czas od zarejestrowania bodźca do wykonania odpowiedzi. Struktura ma go minimalizować, a nie chronić hierarchię.
Sygnał algedoniczny	Kanał alarmowy omijający hierarchię, przenoszący informację o zdarzeniu krytycznym, dla którego nie przewidziano wskaźnika.
Model systemu żywotnego	Pięć podsystemów Beera: operacje, koordynacja, zarządzanie z audytem, rozpoznanie przyszłości, tożsamość i reguła nadrzędna.
Rekurencja	Powtarzalność pełnej struktury sterowania na kolejnych poziomach: obiekt, gmina, powiat, region, państwo.
Sprzężenie zwrotne	Powrót informacji o wyniku w postaci zdolnej zmienić następną decyzję. Sprawozdanie bez instrumentu zmiany nie jest sprzężeniem.
Domknięcie pętli na alokacji	Warunek, w którym wynik pomiaru wraca do decyzji o zasobach w następnym cyklu budżetowym.
Pętla decyzyjna	Cykl obserwacji, orientacji, decyzji i działania. Przewagę uzyskuje strona domykająca cykl szybciej.
Inwersja epistemiczna	Stan, w którym model jest na tyle nieaktualny, że korekta zaczyna wzmacniać odchylenie zamiast je znosić.
Pojemność kanału	Maksymalna ilość informacji przenoszona przez kanał. Każdy zbędny szczebel pośredni wprowadza opóźnienie i szum.
Sterowanie pośrednie	Przejęcie nie organów, lecz programu w korelatorze — przez standardy, oprogramowanie, ekspertów i przekaz.
Suwerenność cyfrowa	Zdolność utrzymania i audytu warstwy technologicznej pod kontrolą krajową; nie autarkia, lecz sterowność.

A.3. Pojęcia systemowe i odpornościowe

Pojęcie	Znaczenie w dokumencie
Odporność	Zdolność utrzymania funkcji krytycznych mimo zakłócenia oraz powrotu do stanu zdatności z zachowaniem tożsamości i sterowności.
Odporność inżynierska	Ujęcie zakładające jedną równowagę i mierzone czasem powrotu do niej. Niewystarczające wobec szoków trwałych.
Odporność ekologiczna	Utrzymanie tożsamości układu przy zmianie stanu; ujęcie przyjęte w programie.
Zdolność adaptacyjna	Zdolność przejścia do nowego, lepszego stanu po szoku trwałym — „przeskok naprzód”.
Zdolność transformacji	Zdolność zmiany samej struktury systemu, gdy dotychczasowa przestała być wykonalna.
Cykl adaptacyjny	Sprzężenie trwałości i zmiany: szok jest oknem reorganizacji, nie wyłącznie stratą.
Absorpcja	Zdolność przyjęcia zakłócenia bez utraty funkcji krytycznej.
Antycypacja	Zdolność rozpoznania zakłócenia zanim wystąpi; warstwa rozpoznania i wczesnego ostrzegania.
Model 3A	Antycypacja, absorpcja, adaptacja — trzy pytania testujące każdy element systemu odporności.
Awaria normalna	Teza, wedle której w układach złożonych i ściśle sprzężonych awarie są własnością konstrukcji, a nie odchyleniem.
Ściśle sprzężenie	Stan, w którym elementy zależą od siebie bez zapasu czasu i zasobu; zakłócenie rozchodzi się szybciej, niż da się je zrozumieć.
Luz systemowy	Celowy nadmiar zasobu, czasu lub przepustowości, pochtaniający zakłócenie zamiast przenosić je dalej.
Redundancja	Powielenie funkcji krytycznej w niezależnych elementach; niezależność, nie sama liczba, decyduje o jej wartości.
Degradacja łagodna	Projektowanie systemu tak, by pod obciążeniem tracił zdolności stopniowo i w kontrolowanej kolejności.
Pułapka sztywności	Stan nadmiernej centralnej kontroli, w którym system traci zdolność adaptacji i załamuje się katastrofalnie.
Pułapka ubóstwa	Stan niedomiaru zasobów i koordynacji, w którym system nie jest w stanie wyjść z niskiego poziomu zdolności.
Optymalne pasmo odporności	Rozstrzygnięcie programu: odporność ma optimum, nie maksimum; nadmiar rezerw i kontroli też są patologią.
Antykruchość	Własność układu, który poprawia się wskutek obciążenia; wymaga zapasu na przeżycie pierwszego wstrząsu.

Pojęcie	Znaczenie w dokumencie
Punkt dźwigni	Miejsce, w którym mała interwencja daje dużą zmianę. Reguła jest silniejszym punktem dźwigni niż parametr budżetowy.
Prawo Goodharta	Miernik, który staje się celem, przestaje być dobrym miernikiem. Podstawa obowiązku przypisania KRI do każdego KPI.
Granica systemu	Zakres elementów objętych analizą; jej wybór przesądza wynik porównania wariantów inwestycyjnych.
Koszt systemowy	Pełny koszt zdolności: budowa, serwis, energia, obsada, ćwiczenia, wymiana i koszt niedostarczonej usługi.
Koszt miejsca operacyjnego	Koszt uzyskania jednego sprawnego, gotowego miejsca ochronnego w pełnym cyklu życia.
Wariant zerowy	Jawnie opisany i wyceniony skutek niezrealizowania projektu; obowiązkowe pole karty pilotażu.
Pojemność formalna	Liczba miejsc wynikająca z ewidencji i parametrów projektowych obiektu.
Pojemność operacyjna	Liczba miejsc rzeczywiście dostępnych w obiekcie sprawnym, obsadzonym i gotowym do uruchomienia.
Paszport odporności	Wersjonowana karta funkcji, ryzyk, zależności, instalacji, gotowości, kosztów i odpowiedzialności obiektu.
Ciągłość działania	Zdolność nieprzerwanego wykonywania funkcji krytycznych mimo utraty siedzib, systemów lub zasilania.
Tryb degradacji	Sposób działania funkcji bez informatyki, sieci i jednego budynku; wymaga procedury ręcznej i ćwiczenia.
Brama stop/go	Decyzja kończąca etap, oparta na potwierdzonym wyniku, koszcie cyklu życia i zdolności utrzymania.
Test zaskoczenia	Sprawdzenie gotowości bez uprzedzenia; jedyny wiarygodny sposób pomiaru czasu aktywacji.
Red teaming	Celowa krytyka własnych planów z perspektywy przeciwnika; instytucjonalny mechanizm sprzężenia negatywnego.
Krajowy Rejestr Ryzyk	Jawny wykaz ryzyk ostrych i chronicznych z właścicielem, wskaźnikiem wczesnego ostrzegania i wariantem awaryjnym.
Horizon scanning	Stała funkcja rozpoznawania zagrożeń wschodzących, zanim staną się przedmiotem planu.

A.4. Pojęcia sieciowe

Pojęcie	Znaczenie w dokumencie
Graf zależności	Reprezentacja państwa jako sieci: węzły to obiekty i funkcje, krawędzie to zależności czterech typów.
Sieć bezskalowa	Sieć o silnie nierównomiernym rozkładzie liczby połączeń, z nielicznymi węzłami o bardzo wielu powiązaniach.
Odporna, lecz krucha	Własność takich sieci: znoszą awarie losowe, rozpadają się przy uderzeniu celowanym w węzeł centralny.
Hub	Węzeł o nieproporcjonalnie dużej liczbie połączeń; cel pierwszorzędny racjonalnego przeciwnika.
Centralność pośrednictwa	Miara liczby najkrótszych ścieżek przechodzących przez węzeł; wskazuje wąskie gardła niezależnie od wielkości obiektu.
Węzeł krytyczny	Węzeł, którego utrata kaskaduje na co najmniej dwie inne warstwy. Nie jest tożsamy z węzłem dużym.
Most / punkt artykulacji	Element, którego usunięcie rozcina sieć na niepołączone części.
Sieci współzależne	Dwie lub więcej sieci, w których działanie jednej warunkuje działanie drugiej — typowo energia i telekomunikacja.
Kaskada awarii	Przenoszenie się uszkodzenia między sieciami współzależnymi, prowadzące do rozpadu skokowego poniżej progu pojedynczej sieci.
Perkolacja	Model przejścia sieci ze stanu spójnego do rozpadu przy usuwaniu węzłów lub krawędzi.
Zależność fizyczna	Wyjście jednego węzła jest wejściem drugiego — np. zasilanie schronu z sieci elektroenergetycznej.
Zależność cyfrowa	Zależność przez stan informacji i sterowanie — np. pompa sterowana systemem zewnętrznego operatora.
Zależność geograficzna	Wspólne położenie powodujące wspólną podatność na to samo zdarzenie niszczące.
Zależność logiczna	Zależność przez rynek, umowę, regulację lub decyzję — np. jeden dostawca filtrów dla całego kraju.
Druga ścieżka	Alternatywna trasa przepływu dla węzła krytycznego, o określonym koszcie uruchomienia i czasie przełączenia.
Pojedynczy punkt awarii	Element, którego utrata usuwa funkcję całego systemu, ponieważ nie istnieje uruchamialna druga ścieżka.
Praca wyspowa	Zdolność fragmentu sieci do samodzielnej pracy po odłączeniu od systemu; mechanizm przerywania kaskady.
Black-start	Zdolność uruchomienia zasilania od zera, bez wsparcia sieci zewnętrznej; warunek odbudowy po rozległym zaniku.

Pojęcie	Znaczenie w dokumencie
Ryzyko topologiczne	Ryzyko wynikające z rozmieszczenia zasobów w sieci, nie z ich wielkości — np. koncentracja pojemności w jednym węźle.
Kapitał wiążący	Więzi wewnątrz własnej grupy; bez kapitału pomostowego utrwala izolację wspólnoty.
Kapitał pomostowy	Więzi między grupami; nośnik informacji nowej i warunek dotarcia pomocy do osób spoza sieci sąsiedzkich.
Siła słabych więzi	Teza, wedle której informację nową przenoszą kontakty spoza własnego środowiska; uzasadnienie struktury Programu 2G.
Odporność kognitywna	Zdolność społeczeństwa do rozpoznania manipulacji i utrzymania spójności poznawczej pod presją informacyjną.
Uodpornianie wyprzedzające	Uprzedzające ujawnienie mechanizmu manipulacji, uodporniające odbiorcę bez kontroli treści.

A.5. Pojęcia strukturalne, prawne i operacyjne

Pojęcie	Znaczenie w dokumencie
Zdolność państwa	Zdolność organizacji do domknięcia zadania od zamiaru do zweryfikowanego wyniku; problem organizacyjny, nie budżetowy.
Właściciel wyniku	Jedna osoba lub organ odpowiadający za rezultat funkcji lub obiektu; rola „A” w macierzy RACI.
Współodpowiedzialność bez odpowiedzialnego	Patologia struktur, w których zadanie ma wielu wykonawców i żadnej roli rozliczanej z wyniku.
Prawo Conwaya	Struktura budowanego systemu odwzorowuje strukturę komunikacyjną organizacji, która go tworzy.
Subsydiarność operacyjna	Centrum ustala standard minimalny, finansuje i audytuje; wykonanie należy do samorządu, operatora i wspólnoty.
Jednostka dostarczania	Wyodrębniony zespół rozliczany z wykonania priorytetu, z twardym miernikiem i bezpośrednim dostępem do decydenta.
Przechwycenie regulatora	Stan, w którym organ regulujący działa w interesie podmiotu regulowanego; ryzyko rosnące ze skalą strumienia zamówień.
Antyzawłaszczanie	Zestaw bezpieczników: jawność kryteriów, rejestr konfliktu interesów, rotacja, plan wyjścia, audyt niezależny.
Uzależnienie od dostawcy	Stan, w którym zmiana dostawcy technologii jest niemożliwa lub nieopłacalna; w ujęciu sieciowym oddanie huba.
Plan wyjścia	Udokumentowana i przetestowana możliwość migracji do innego dostawcy, modelu lub technologii.
Zamówienie na wynik	Kontraktowanie utrzymanej zdolności zamiast dostawy rzeczy; z miernikiem, bramą etapową i okresem utrzymania.

Pojęcie	Znaczenie w dokumencie
Budżet cyklu życia	Wieloletnie ujęcie kosztu obejmujące CAPEX, OPEX, serwis, kadry, zapasy i wymianę komponentów.
Domknięcie budżetowe	Zasada: rozstrzygnięcie bez pozycji w planie finansowym, terminu i właściciela rezultatu jest opinią, nie rozstrzygnięciem.
Bezpiecznik antyneoliberalny	Zasada: odporność obywatelska wzmacnia zdolność publiczną i nigdy jej nie zastępuje.
Budowla ochronna	Obiekt budowlany lub jego część spełniający kryteria uznania za budowlę ochronną w rozumieniu przepisów.
Schron	Hermetyczna budowla ochronna o najwyższym poziomie zabezpieczenia, z płaszczyzną ochrony i hermetyzacji.
Ukrycie	Budowla ochronna bez pełnej hermetyzacji, chroniąca m.in. przed odłamkami, gruzem i określonymi skutkami wybuchu.
Punkt schronienia	Miejsce zidentyfikowane jako doraźna możliwość ochrony, zgodnie z ramą po nowelizacji z 2026 r.
Filtrowentylacja	Układ oczyszczania i tłoczenia powietrza utrzymujący nadciśnienie i parametry atmosfery w budowlu ochronnej.
Strefa zagruzowania	Obszar możliwego zawalenia i zasypania wokół budynku, wpływający na trasy ewakuacji i dostęp ratownictwa.
Projektowanie uniwersalne	Projektowanie umożliwiające korzystanie z obiektu przez osoby o różnych możliwościach bez adaptacji dodatkowej.
Ochrona ludności	Zadanie publiczne obejmujące ostrzeganie, schronienie, ewakuację, ratownictwo i zaspokojenie potrzeb podstawowych.
Obrona cywilna	Wyodrębniona forma ochrony ludności w czasie konfliktu zbrojnego, chroniona międzynarodowym prawem humanitarnym.
Whole-of-society	Podejście angażujące obywateli, biznes, organizacje i samorząd obok administracji, przy zachowaniu odpowiedzialności państwa.
Whole-of-government	Podejście wymagające współdziałania wszystkich resortów i szczebli wokół wspólnego wyniku, nie wokół kompetencji.
Siedem wymagań bazowych	Zestaw funkcji odporności przyjęty w NATO: ciągłość rządzenia, energia, przemieszczenia masowe, żywność i woda, zdarzenia masowe, łączność, transport.
Cytadela odporności	Wielomodułowy węzeł dual-use łączący energię, dane, schronienie, zapasy i warsztat na poziomie regionu.
Węzeł pięciu funkcji	Obiekt lokalny łączący w kryzysie informację, zasilanie, wodę, pierwszą pomoc i schronienie.
Rezerwa rotowana	Zapas utrzymywany przez bieżące zużycie i uzupełnianie, dzięki czemu nie traci ważności i nie generuje kosztu martwego.

Pojęcie	Znaczenie w dokumencie
Narodowy Indeks Odporności	Roczne, jawne, nierankingujące zestawienie zdolności państwa w dwóch prędkościach odporności.
Formuła naczelna	Zdanie definiujące przedmiot dokumentu przez wskazanie miar i warunków koniecznych; podlega uzasadnieniu i falsyfikacji.
Warunek falsyfikacji	Twierdzenie, którego prawdziwość obalałaby program; jego wskazanie odróżnia doktrynę sprawdzalną od deklaracji.

A.6. Pojęcia ustrojowe i programowe TechnoSanacji

Pojęcie	Znaczenie w dokumencie
TechnoSanacja	Droga naprawy państwa: metoda przejścia od diagnozy do sprawczości, oparta na cybernetycznym ujęciu instytucji.
TechnoRepublika	Cel ustrojowy: państwo sprawcze, przewidujące i rozliczalne wobec obywatela, sterowane w oparciu o dane i odpowiedzialność.
Cztery koherentne systemy	Polityczny, społeczny, gospodarczy i technologiczny — przedmiot formuły naczelnej i kryterium spójności programu.
Centrum Odporności i Ciągłości	Organ integracji ryzyk, danych, ćwiczeń i alarmów; właściciel rejestru ryzyk, grafu i kanału pilnego.
Narodowa Strategia Odporności	Dokument nadrzędny z portfelem misji, właścicielami funkcji i budżetem; własność egzekutywy.
Narodowy Graf Odporności	Model zależności państwa: węzły, krawędzie, miary topologiczne, historia i poziomy dostęp.
Program 2G	Program współpracy Generacji Z i seniorów jako amplifikator różnorodności regulatora.
Standard dual-key	Wymóg, by zadanie wysokiego wpływu przygotowywały i odbierały dwie różne perspektywy, z zapisem rozbieżności.
Karta praw obywatela w systemie odporności	Katalog ośmiu praw równoważących zdolności programu; podstawa kontroli regulatora.
Sejmik samorządowy	Regionalne forum kształtowania polityk bez własnej biurokracji; w programie źródło opinii, listy ryzyk i zdania odrębnego.
Senat 100	Izba kontroli i legislacji; w programie właściciel komisji odporności i jawnego raportu rocznego.
Audyt obywatelski	Niezależny od administracji mechanizm weryfikacji danych i zamknięcia zaleceń, z dostępem do publicznego pulpitu.
Czerwona linia	Zakaz bezwarunkowy programu, niepodlegający ważeniu z korzyścią operacyjną.

ANEKS B. BIBLIOGRAFIA I BAZA DOWODOWA

Aneks obejmuje 206 pozycji w piętnastu klastrach tematycznych. Źródła podzielono na klasykę teoretyczną (klastry B.1–B.5), korpus analityczny i normatywny (B.6–B.11), polskie akty prawne i programy publiczne (B.12), oficjalne wzorce międzynarodowe (B.13), dokumenty programowe TechnoSanacji i destylaty bibliotek operacyjnych (B.14) oraz adresy źródeł internetowych (B.15). Wdrożenie wymaga każdorazowej weryfikacji aktualnego tekstu prawa, norm, wytycznych technicznych i danych operacyjnych.

B.1. Cybernetyka, teoria sterowania i regulacji

1. Wiener, N. (1948), *Cybernetics: or Control and Communication in the Animal and the Machine*, MIT Press, Cambridge MA.
2. Wiener, N. (1950), *The Human Use of Human Beings: Cybernetics and Society*, Houghton Mifflin, Boston.
3. Ashby, W.R. (1956), *An Introduction to Cybernetics*, Chapman & Hall, Londyn.
4. Ashby, W.R. (1958), *Requisite Variety and Its Implications for the Control of Complex Systems*, „Cybernetica” 1(2), s. 83–99.
5. Conant, R.C., Ashby, W.R. (1970), *Every Good Regulator of a System Must Be a Model of That System*, „International Journal of Systems Science” 1(2), s. 89–97.
6. Shannon, C.E. (1948), *A Mathematical Theory of Communication*, „The Bell System Technical Journal” 27(3), s. 379–423 oraz 27(4), s. 623–656.
7. Beer, S. (1972), *Brain of the Firm: The Managerial Cybernetics of Organization*, Allen Lane, Londyn.
8. Beer, S. (1979), *The Heart of Enterprise*, John Wiley & Sons, Chichester.
9. Beer, S. (1985), *Diagnosing the System for Organizations*, John Wiley & Sons, Chichester.
10. Beer, S. (1974), *Designing Freedom*, Canadian Broadcasting Corporation, Toronto.
11. Espejo, R., Reyes, A. (2011), *Organizational Systems: Managing Complexity with the Viable System Model*, Springer, Berlin–Heidelberg.
12. Schwaninger, M. (2006), *Intelligent Organizations: Powerful Models for Systemic Management*, Springer, Berlin.
13. von Foerster, H. (2003), *Understanding Understanding: Essays on Cybernetics and Cognition*, Springer, Nowy Jork.
14. Luhmann, N. (1984), *Soziale Systeme: Grundriß einer allgemeinen Theorie*, Suhrkamp, Frankfurt nad Menem.
15. Medina, E. (2011), *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*, MIT Press, Cambridge MA.
16. Forrester, J.W. (1961), *Industrial Dynamics*, MIT Press, Cambridge MA.
17. Sterman, J.D. (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin/McGraw-Hill, Boston.

18. Deutsch, K.W. (1963), *The Nerves of Government: Models of Political Communication and Control*, Free Press, Nowy Jork.
19. Easton, D. (1965), *A Systems Analysis of Political Life*, John Wiley & Sons, Nowy Jork.
20. Powers, W.T. (1973), *Behavior: The Control of Perception*, Aldine, Chicago.

B.2. Polska szkoła cybernetyki: układy samodzielne i tory sterowania

21. Mazur, M. (1966), *Cybernetyczna teoria układów samodzielnych*, Państwowe Wydawnictwo Naukowe, Warszawa.
22. Mazur, M. (1970), *Jakościowa teoria informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa.
23. Mazur, M. (1976), *Cybernetyka i charakter*, Państwowy Instytut Wydawniczy, Warszawa.
24. Kossecki, J. (1981), *Cybernetyka społeczna*, Państwowe Wydawnictwo Naukowe, Warszawa (wyd. 1: 1975).
25. Kossecki, J. (1984), *Cybernetyka kultury*, Państwowy Instytut Wydawniczy, Warszawa.
26. Kossecki, J. (2001), *Wzajemne oddziaływania państw jako układów sterowniczych*, Wydawnictwo Akademii Świętokrzyskiej, Kielce.
27. Kossecki, J. (2005), *Metacybernetyka*, Kielce–Warszawa.
28. Wilsz, J. (2005), *Samosterowność jako właściwość układu autonomicznego*, Wydawnictwo Wyższej Szkoły Pedagogicznej, Częstochowa.
29. Lange, O. (1965), *Wstęp do cybernetyki ekonomicznej*, Państwowe Wydawnictwo Naukowe, Warszawa.
30. Greniewski, H. (1959), *Cybernetyka niematematyczna*, Państwowe Wydawnictwo Naukowe, Warszawa.

B.3. Teoria systemów, niezawodność i inżynieria odporności

31. Bertalanffy, L. von (1968), *General System Theory: Foundations, Development, Applications*, George Braziller, Nowy Jork.
32. Simon, H.A. (1962), *The Architecture of Complexity*, „Proceedings of the American Philosophical Society” 106(6), s. 467–482.
33. Simon, H.A. (1996), *The Sciences of the Artificial*, wyd. 3, MIT Press, Cambridge MA.
34. Perrow, C. (1984), *Normal Accidents: Living with High-Risk Technologies*, Basic Books, Nowy Jork.
35. Weick, K.E., Sutcliffe, K.M. (2007), *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, Jossey-Bass, San Francisco.
36. Hollnagel, E., Woods, D.D., Leveson, N. (red.) (2006), *Resilience Engineering: Concepts and Precepts*, Ashgate, Aldershot.
37. Hollnagel, E. (2011), *Resilience Engineering in Practice: A Guidebook*, Ashgate, Farnham.
38. Reason, J. (1997), *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot.

39. Leveson, N. (2011), *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge MA.
40. Holling, C.S. (1973), *Resilience and Stability of Ecological Systems*, „Annual Review of Ecology and Systematics” 4, s. 1–23.
41. Gunderson, L.H., Holling, C.S. (red.) (2002), *Panarchy: Understanding Transformations in Human and Natural Systems*, Island Press, Waszyngton.
42. Walker, B. i in. (2002), *Resilience Management in Social-Ecological Systems*, „Conservation Ecology” 6(1), art. 14.
43. Folke, C. i in. (2010), *Resilience Thinking: Integrating Resilience, Adaptability and Transformability*, „Ecology and Society” 15(4), art. 20.
44. Carpenter, S.R., Brock, W.A. (2008), *Adaptive Capacity and Traps*, „Ecology and Society” 13(2), art. 40.
45. Scheffer, M. i in. (2012), *Anticipating Critical Transitions*, „Science” 338(6105), s. 344–348.
46. Meadows, D.H. (1999), *Leverage Points: Places to Intervene in a System*, The Sustainability Institute, Hartland.
47. Meadows, D.H. (2008), *Thinking in Systems: A Primer*, Chelsea Green Publishing, White River Junction.
48. Taleb, N.N. (2012), *Antifragile: Things That Gain from Disorder*, Random House, Nowy Jork.
49. Taleb, N.N. (2007), *The Black Swan: The Impact of the Highly Improbable*, Random House, Nowy Jork.
50. Goodhart, C.A.E. (1975), *Problems of Monetary Management: The UK Experience*, Papers in Monetary Economics, Reserve Bank of Australia.
51. Scott, J.C. (1998), *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven.
52. Snowden, D.J., Boone, M.E. (2007), *A Leader's Framework for Decision Making*, „Harvard Business Review” 85(11), s. 68–76.

B.4. Teoria sieci i odporność infrastruktury krytycznej

53. Barabási, A.-L., Albert, R. (1999), *Emergence of Scaling in Random Networks*, „Science” 286(5439), s. 509–512.
54. Albert, R., Jeong, H., Barabási, A.-L. (2000), *Error and Attack Tolerance of Complex Networks*, „Nature” 406, s. 378–382.
55. Barabási, A.-L. (2016), *Network Science*, Cambridge University Press, Cambridge.
56. Watts, D.J., Strogatz, S.H. (1998), *Collective Dynamics of 'Small-World' Networks*, „Nature” 393, s. 440–442.
57. Newman, M.E.J. (2018), *Networks*, wyd. 2, Oxford University Press, Oksford.
58. Freeman, L.C. (1979), *Centrality in Social Networks: Conceptual Clarification*, „Social Networks” 1(3), s. 215–239.

59. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S. (2010), *Catastrophic Cascade of Failures in Interdependent Networks*, „Nature” 464, s. 1025–1028.
60. Vespignani, A. (2010), *The Fragility of Interdependency*, „Nature” 464, s. 984–985.
61. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001), *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, „IEEE Control Systems Magazine” 21(6), s. 11–25.
62. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J. (2000), *Network Robustness and Fragility: Percolation on Random Graphs*, „Physical Review Letters” 85(25), s. 5468–5471.
63. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S. (2001), *Breakdown of the Internet under Intentional Attack*, „Physical Review Letters” 86(16), s. 3682–3685.
64. Argonne National Laboratory (2015), *Critical Infrastructure Dependencies and Interdependencies*, Argonne IL.
65. Argonne National Laboratory (2013), *Resilience Index for Critical Infrastructure*, Argonne IL.
66. Granovetter, M.S. (1973), *The Strength of Weak Ties*, „American Journal of Sociology” 78(6), s. 1360–1380.
67. Burt, R.S. (1992), *Structural Holes: The Social Structure of Competition*, Harvard University Press, Cambridge MA.
68. Conway, M.E. (1968), *How Do Committees Invent?*, „Datamation” 14(4), s. 28–31.
69. Castells, M. (1996), *The Rise of the Network Society*, Blackwell, Oksford.
70. Joint Research Centre (2021–2025), *analizy odporności infrastruktury krytycznej i współzależności sektorowych*, JRC, Ispra.

B.5. Zdolność państwa, organizacja i antyzawłaszczanie

71. Fukuyama, F. (2013), *What Is Governance?*, „Governance” 26(3), s. 347–368.
72. Besley, T., Persson, T. (2011), *Pillars of Prosperity: The Political Economics of Development Clusters*, Princeton University Press, Princeton.
73. Ting, M.M. (2011), *An Organizational Theory of State Capacity*, „Journal of Theoretical Politics”.
74. National Bureau of Economic Research (2023), *State Capacity as an Organizational Problem*, NBER Working Paper w31591, Cambridge MA.
75. National Bureau of Economic Research (2018–2024), *Personnel Economics of the State oraz Productivity of Bureaucrats*, NBER, Cambridge MA.
76. Mazzucato, M. (2021), *Mission Economy: A Moonshot Guide to Changing Capitalism*, Allen Lane, Londyn.
77. OECD (2020–2025), *Steering from the Centre in Times of Complexity*, OECD Publishing, Paryż.

78. Institute for Government (2021–2024), *Power with Purpose: Final Report of the Commission on the Centre of Government*, IfG, Londyn.
79. OECD (2009–2025), *Government at a Glance*, kolejne edycje, OECD Publishing, Paryż.
80. Bank Światowy (2010–2025), korpus operacyjny zarządzania finansami publicznymi: przeglądy wydatków publicznych, MTEF, budżet zadaniowy, GovTech Maturity Index, Waszyngton.
81. Michels, R. (1911), *Zur Soziologie des Parteiwesens in der modernen Demokratie*, Klinkhardt, Lipsk.
82. Mills, C.W. (1956), *The Power Elite*, Oxford University Press, Nowy Jork.
83. Stigler, G.J. (1971), *The Theory of Economic Regulation*, „The Bell Journal of Economics and Management Science” 2(1), s. 3–21.
84. Mann, M. (1984), *The Autonomous Power of the State: Its Origins, Mechanisms and Results*, „European Journal of Sociology” 25(2), s. 185–213.
85. Transparency International (2020–2026), analizy przechwycenia państwa, jawności beneficjentów rzeczywistych i regulacji lobbingu, Berlin.
86. INTOSAI (2019–2025), standardy najwyższych organów kontroli i niezależności audytu publicznego, Wiedeń.
87. Bovens, M. (2007), *Analysing and Assessing Accountability: A Conceptual Framework*, „European Law Journal” 13(4), s. 447–468.
88. Komisja Wenecka (2016), *Rule of Law Checklist*, CDL-AD(2016)007, Strasburg.
89. Komisja Wenecka (2020), *Respect for Democracy, Human Rights and the Rule of Law during States of Emergency*, CDL-AD(2020)014, Strasburg.

B.6. Odporność jako polityka publiczna: ramy, pomiar i krytyka

90. RAND Corporation (2021–2025), *A Method for Assessing Societal Resilience for National Security*, RAND, Santa Monica.
91. NIST (2023–2025), *Resilience Indicators*, NIST SP 2300-01, Gaithersburg.
92. NIST (2021), *Developing Cyber-Resilient Systems*, NIST SP 800-160 Vol. 2 Rev. 1, Gaithersburg.
93. NIST (2023), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, Gaithersburg.
94. NIST (2020), *Zero Trust Architecture*, NIST SP 800-207, Gaithersburg.
95. OECD (2024–2025), *Vulnerability Indicators oraz Strategic Foresight Toolkit*, OECD Publishing, Paryż.
96. OECD (2020–2024), *Towards Anticipatory Governance i Framework on Emerging Critical Risks*, OECD Publishing, Paryż.
97. Arup, Rockefeller Foundation (2015), *City Resilience Index*, Londyn–Nowy Jork.

98. Cutter, S.L. i in. (2014–2024), *Baseline Resilience Indicators for Communities (BRIC)* wraz z przeglądami metodologicznymi.
99. Komisja Europejska (2021), *EU Resilience Dashboards*, Bruksela.
100. University of Notre Dame (2024), *ND-GAIN Country Index Technical Report*, Notre Dame IN.
101. UNDRR (2025), *Global Assessment Report: Resilience Pays*, Genewa.
102. UNDRR, WMO (2024), *Multi-Hazard Early Warning Systems Checklist*, Genewa.
103. Briguglio, L. i in. (2009), *Economic Vulnerability and Resilience: Concepts and Measurements*, „Oxford Development Studies” 37(3).
104. Chandler, D. (2014), *Resilience: The Governance of Complexity*, Routledge, Londyn (krytyka pojęcia odporności).
105. Joseph, J. (2013), *Resilience as Embedded Neoliberalism: A Governmentality Approach*, „Resilience” 1(1), s. 38–52.
106. Welsh, M. (2014), *Resilience and Responsibility: Governing Uncertainty in a Complex World*, „The Geographical Journal” 180(1).
107. World Economic Forum (2020–2026), *Global Risks Report*, kolejne edycje, Genewa.

B.7. Ochrona ludności, obrona cywilna i obrona totalna

108. Niinistö, S. (2024), *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, raport dla Komisji Europejskiej, Bruksela.
109. Komisja Europejska (2025), *Preparedness Union Strategy*, COM(2025)637, Bruksela.
110. Komisja Europejska (2025), *Strategic Foresight Report: Resilience 2.0*, Bruksela.
111. NATO (2016–2026), *Resilience, Civil Preparedness and Article 3* wraz z siedmioma wymaganiami bazowymi, Bruksela.
112. NATO (2021–2025), *AJP-3.19 Allied Joint Doctrine for Civil-Military Cooperation*, NSO, Bruksela.
113. Finnish Security Committee (2017, akt. 2024), *The Security Strategy for Society*, Helsinki.
114. Ministry of the Interior of Finland (2024–2026), *Civil Defence Shelters* — wytyczne i informacja publiczna, Helsinki.
115. Finnish Ministry of the Interior (2025), *72 Hours Home Preparedness*, Helsinki.
116. Myndigheten för samhällsskydd och beredskap (2024), *Om krisen eller kriget kommer*, MSB, Sztokholm.
117. Swedish Civil Defence Authority (2025), *Good to Know about Civil Defence Shelters*, Sztokholm.
118. Swiss Federal Office for Civil Protection (2024–2026), *Shelters for the Population*, Berno.
119. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2020–2025), materiały Zivilschutz i poradniki gotowości, Bonn.

120. ZOES-Bund (2020–2025), *Grünbücher* o bezpieczeństwie publicznym, ochronie ludności, ZMZ 4.0 i obrazie sytuacyjnym w czasie rzeczywistym, Berlin.
121. Ministry of Defence of Singapore (2023–2025), *Total Defence: Five Pillars*, Singapur.
122. International Institute for Strategic Studies (2024–2025), *Civil Defence in Europe*, IISS, Londyn.
123. International Committee of the Red Cross (2020–2025), ochrona ludności cywilnej i międzynarodowy znak obrony cywilnej, MKCK, Genewa.
124. Konwencje genewskie z 12 sierpnia 1949 r. wraz z Protokołami dodatkowymi z 1977 r., w szczególności art. 61 Protokołu I.
125. UK Cabinet Office (2023–2025), *National Risk Register*, Londyn.
126. Ośrodek Studiów Wschodnich (2024–2026), analizy nowych koncepcji obrony totalnej w regionie, OSW, Warszawa.

B.8. Infrastruktura krytyczna, cyberodporność i suwerenność technologiczna

127. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych, Dz.U. UE L 333/164.
128. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (NIS 2), Dz.U. UE L 333/80.
129. ENISA (2024–2026), *Threat Landscape*, kolejne edycje, Ateny.
130. ENISA (2024), *NIS360* oraz *Foresight 2030 Threats*, Ateny.
131. CISA (2021–2025), *Zero Trust Maturity Model* oraz wytyczne ochrony infrastruktury krytycznej, Waszyngton.
132. Department of Homeland Security (2023–2025), *National Critical Functions* i *Strategic Guidance for Critical Infrastructure*, Waszyngton.
133. ISO 22301, *Security and resilience — Business continuity management systems*.
134. ISO 22316, *Security and resilience — Organizational resilience*.
135. ISO 22320, *Security and resilience — Emergency management*.
136. ISO 31000, *Risk management — Guidelines*.
137. NIST (2024), *Cybersecurity Framework 2.0*, Gaithersburg.
138. NIST (2022), *Integrating Cybersecurity and Enterprise Risk Management*, NIST IR 8286, Gaithersburg.
139. NASK (2023–2025), opracowania wdrożeniowe dyrektyw CER i NIS 2 w warunkach polskich, Warszawa.
140. European Parliament (2024–2026), *Technological Sovereignty and Digital Infrastructure*, EPRS, Bruksela.

141. Joint Research Centre (2023–2025), *Reexports and Strategic Dependencies* — mapa zależności importowych UE, Ispra.
142. Zuboff, S. (2019), *The Age of Surveillance Capitalism*, PublicAffairs, Nowy Jork.

B.9. Energia, woda, żywność i zdrowie jako tor zasilający

143. International Energy Agency (2024–2026), *Electricity Security* oraz analizy elastyczności i magazynowania energii, IEA, Paryż.
144. International Energy Agency (2025), *Energy System Resilience: Lessons from Ukraine*, IEA, Paryż.
145. ENTSO-E (2024–2026), *European Resource Adequacy Assessment* oraz procedury odbudowy zasilania, Bruksela.
146. Sandia National Laboratories (2020–2025), analizy mikrosieci i odporności energetycznej obiektów krytycznych, Albuquerque.
147. Polskie Sieci Elektroenergetyczne (2024–2026), materiały o bezpieczeństwie pracy krajowego systemu elektroenergetycznego, Konstancin-Jeziorna.
148. Bouzarovski, S. (2018), *Energy Poverty: (Dis)Assembling Europe's Infrastructural Divide*, Palgrave Macmillan, Cham.
149. FAO (2021), *The State of Food and Agriculture: Making Agrifood Systems More Resilient to Shocks and Stresses*, Rzym.
150. FAO (2022), *Public Food Stockholding: A Review of Policies and Practices*, Rzym.
151. Bank Światowy (2022–2024), *Strengthening Strategic Grain Reserves*, Waszyngton.
152. WHO (2021–2025), *Health Systems Resilience: Concepts and Strategies* oraz wskaźniki odporności systemów zdrowia, Genewa.
153. Bank Światowy (2023–2025), *Pandemic Prevention, Preparedness and Response*, Waszyngton.
154. OECD (2025), *Supply Chain Resilience Review*, OECD Publishing, Paryż.
155. National Bureau of Economic Research (2024), *Efficiently Resilient* (Capponi, Du, Stiglitz), NBER Working Paper w32221, Cambridge MA.
156. National Bureau of Economic Research (2021), *Risks and Global Supply Chains*, NBER Working Paper w29444, Cambridge MA.
157. Bank Światowy (2020–2024), *Financial Protection Against Natural Disasters* oraz analizy warstwowania ryzyka katastroficznego, Waszyngton.
158. European Investment Bank (2022), *Scarring Effects of Crises on Public Finances*, Working Paper 2022/14, Luksemburg.

B.10. Odporność społeczna, zaufanie i odporność poznawcza

159. Sztompka, P. (2007), *Zaufanie. Fundament społeczeństwa*, Znak, Kraków.
160. Putnam, R.D. (2000), *Bowling Alone: The Collapse and Revival of American Community*, Simon & Schuster, Nowy Jork.

161. Aldrich, D.P. (2012), *Building Resilience: Social Capital in Post-Disaster Recovery*, University of Chicago Press, Chicago.
162. Aldrich, D.P. (2019), *Black Wave: How Networks and Governance Shaped Japan's 3/11 Disasters*, University of Chicago Press, Chicago.
163. OECD (2024), *Drivers of Trust in Public Institutions*, OECD Publishing, Paryż.
164. van der Linden, S. (2023), *Foolproof: Why Misinformation Infects Our Minds and How to Build Immunity*, W.W. Norton, Nowy Jork.
165. Roozenbeek, J., van der Linden, S. (2019), *Fake News Game Confers Psychological Resistance Against Online Misinformation*, „Palgrave Communications” 5, art. 65.
166. Lewandowsky, S. i in. (2020), *The Debunking Handbook 2020*, George Mason University, Fairfax.
167. FOI (2024), *Societal Security and Psychological Defence*, Memo 8613, Sztokholm.
168. European External Action Service (2023–2026), *FIMI Threat Reports*, kolejne edycje, Bruksela.
169. NATO Strategic Communications Centre of Excellence (2020–2026), analizy operacji informacyjnych i manipulacji w mediach społecznościowych, Ryga.
170. Hybrid CoE (2023), *CORE: Comprehensive Resilience Ecosystem*, Helsinki.
171. Hybrid CoE (2024–2026), *Countering Hybrid Threats oraz AI and FIMI*, Helsinki.
172. Fundacja im. Stefana Batorego (2024–2026), *Gotowi na kryzys? — badania świadomości i przygotowania Polaków*, Warszawa.
173. UNFPA (2024), *Demographic Resilience Programme*, Nowy Jork.

B.11. Sztuczna inteligencja, systemy wieloagentowe i nadzór algorytmiczny

174. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji, Dz.U. UE L 2024/1689.
175. Rada Europy (2024), *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CETS nr 225, Wilno.
176. OECD (2024–2026), *Governing with AI oraz The Agentic AI Landscape*, OECD Publishing, Paryż.
177. European Data Protection Supervisor (2021–2025), opinie o zautomatyzowanym podejmowaniu decyzji i znaczącej kontroli człowieka, Bruksela.
178. UK Government (2022–2025), *Algorithmic Transparency Recording Standard*, Londyn.
179. Russell, S. (2019), *Human Compatible: Artificial Intelligence and the Problem of Control*, Viking, Nowy Jork.
180. O'Neil, C. (2016), *Weapons of Math Destruction*, Crown, Nowy Jork.
181. Pasquale, F. (2015), *The Black Box Society*, Harvard University Press, Cambridge MA.
182. OWASP (2025), *Agentic AI Threats and Mitigations*, Fundacja OWASP.

- 183. Cloud Security Alliance (2025), *MAESTRO: Multi-Agent Security Threat Modelling*, Seattle.
- 184. Anthropic (2024–2026), *Model Context Protocol* — specyfikacja interoperacyjności narzędzi i agentów.
- 185. Google (2024–2026), *Agent2Agent Protocol* — specyfikacja komunikacji między agentami.
- 186. Karp, A.C., Zamiska, N.W. (2025), *The Technological Republic: Hard Power, Soft Belief, and the Future of the West*, Crown Currency, Nowy Jork.

B.12. Polska — prawo i programy publiczne

- 187. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483, z późn. zm.).
- 188. [P1] Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, Dz.U. 2024 poz. 1907; wejście w życie zasadniczo 1 stycznia 2025 r.
- 189. [P2] Ustawa z dnia 17 kwietnia 2026 r. o zmianie ustawy o ochronie ludności i obronie cywilnej oraz niektórych innych ustaw, Dz.U. 2026 poz. 646.
- 190. [P3] Rozporządzenie MSWiA z dnia 21 lutego 2025 r. w sprawie kryteriów uznawania obiektów budowlanych albo ich części za budowle ochronne, Dz.U. 2025 poz. 235.
- 191. [P4] Rozporządzenie dotyczące Centralnej Ewidencji Obiektów Zbiorowej Ochrony, Dz.U. 2025 poz. 922.
- 192. [P5] Rozporządzenie dotyczące przygotowania i użytkowania miejsc doraźnego schronienia, Dz.U. 2025 poz. 933.
- 193. [P6] 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.
- 194. [P7] Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026 — 16,7 mld zł w 2025 r. i 17,2 mld zł w 2026 r.
- 195. [P8] Gov.pl, komunikat z 20 marca 2026 r.: w 2026 r. priorytetem są nowe schrony, ukrycia, MDS i adaptacja istniejących obiektów.
- 196. [P9] Najwyższa Izba Kontroli (2019–2026), kontrole budowli ochronnych, miejsc ukrycia i przygotowania struktur obrony cywilnej, NIK, Warszawa.
- 197. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590, z późn. zm.).
- 198. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. 2022 poz. 655, z późn. zm.).

B.13. Dokumenty programowe TechnoSanacji i destylaty bibliotek operacyjnych

- 199. Węgrzyn, A. (2026), *Budowanie odporności społecznej, gospodarczej i technologicznej państwa. Program odporności TechnoRepubliki Polskiej*, TechnoSanacja, Warszawa (lipiec 2026).

200. Węgrzyn, A. (2026), *Infrastruktura odporności państwa*, wydanie pierwsze, TechnoSanacja, Warszawa (5 sierpnia 2026).
201. Węgrzyn, A. (2026), *Przewodnik TechnoSanacji. Idea, pojęcia, definicje, indeksy*, wersja 1.1, TechnoSanacja, Warszawa (2 sierpnia 2026).
202. Destylat RES (2026), *Odporność społeczna, gospodarcza i technologiczna TechnoRepubliki* — synteza korpusu 1725 publikacji, TechnoSanacja.
203. Destylat SYS (2026), *Analiza systemowa państwa* — synteza korpusu 3231 publikacji w sześciu klastrach, TechnoSanacja.
204. Destylat CybControl (2026), *Cybernetyka państwa, narodu i organizacji politycznej* — synteza korpusu 623 publikacji, TechnoSanacja.
205. Destylat MultiAgent (2026), *TechnoRepublika — system multiagentowy* — synteza korpusu 622 publikacji, TechnoSanacja.
206. Destylat AHP (2026), *Wielokryterialny proces decyzyjny* — synteza korpusu 990 publikacji, TechnoSanacja.

B.14. Adresy źródeł internetowych

<https://technosanacja.pl/>

<https://technosanacja.pl/rezyliencja/>

<https://technorepublika.pl/>

<https://eli.gov.pl/eli/DU/2024/1907/ogl>

<https://eli.gov.pl/eli/DU/2025/235/ogl>

<https://eli.gov.pl/eli/DU/2025/1548/ogl>

<https://www.gov.pl/web/kgpsp/rzad-przyjal-program-ochrony-ludnosci-i-obrony-cywilnej-na-lata-2025-2026>

<https://www.gov.pl/web/uw-podlaski/program-ochrony-ludnosci-i-obrony-cywilnej-w-tym-roku-priorytetem-miejsca-schronienia>

https://commission.europa.eu/topics/preparedness_en

<https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3>

<https://intermin.fi/en/rescue-services/preparedness/civil-defence-shelters>

<https://www.mcf.se/en/advice-for-individuals/civil-defence-shelters-evacuation-and-warning-systems/good-to-know-about-civil-defence-shelters/>

<https://www.babs.admin.ch/en/shelters-for-the-population>

B.15. Nota o źródłach

Pozycje klasyczne (klastry B.1–B.5) podano z pełnym adresem bibliograficznym. Pozycje analityczne instytucji badawczych i organizacji międzynarodowych (B.6–B.11) pochodzą z korpusu źródłowego TechnoSanacji i podano je na poziomie instytucji, tytułu serii lub raportu

oraz roku wydania; przed publikacją zewnętrzną zaleca się uzupełnienie ich o dokładne daty wydania, numery raportów i adresy elektroniczne. Akty prawne przywołano według stanu na wrzesień 2026 r. i przed zastosowaniem wymagają weryfikacji w tekście jednolitym. Dane liczbowe dotyczące programów publicznych i wzorców zagranicznych podano w brzmieniu z momentu publikacji źródła.

ZASTRZEŻENIE KOŃCOWE

Dokument zwiększa świadomość i porządkuje program. Nie zastępuje oficjalnych komunikatów alarmowych, decyzji organów ochrony ludności, projektu budowlanego, opinii prawnej, ekspertyzy konstrukcyjnej ani instrukcji służb.

Bezpieczeństwo wymaga zgodności rzeczywistych praktyk z prawem, normami i wynikami ćwiczeń.

NIE BUNKIER ZAMIAST PRZYSZŁOŚCI.

INFRASTRUKTURA, KTÓRA SŁUŻY CODZIENNIE I RATUJE W KRYZYSIE.

Dokument • debata • pierwsze zadanie • pomiar • korekta



Polska, wrzesień 2026 r. Materiał udostępniony na licencji Creative Commons — Uznanie autorstwa.