

Narodowa Strategia Bezpieczeństwa



Tom 1. Ogólna strategia bezpieczeństwa:

cybernetyczna pętla przetrwania, odporności, odstraszania i sprawczości państwa

NARODOWA STRATEGIA BEZPIECZEŃSTWA  **TechnoRepublika**

4 FUNDAMENTY INTERESU NARODOWEGO 	6 TORÓW WSPÓŁCZESNEJ SUWERENNOŚCI <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td> DANE</td> <td> ENERGIA</td> <td> SOFTWARE</td> </tr> <tr> <td> PRODUKCJA</td> <td> OBRONA</td> <td> DECYZJE</td> </tr> </table>	 DANE	 ENERGIA	 SOFTWARE	 PRODUKCJA	 OBRONA	 DECYZJE	DIME+T: INSTRUMENTY SIŁY PAŃSTWA DIME+T     +  Dyplomacja Informacja Wojsko Gospodarka TECHNOLOGIA TECHNOLOGIA jako kluczowy mnożnik sprawczości.
 DANE	 ENERGIA	 SOFTWARE						
 PRODUKCJA	 OBRONA	 DECYZJE						



OD PROCEDUR DO WYNIKÓW

Transformacja opisów w realną zdolność działania i skrócenie pętli decyzyjnej.

FORMUŁA NACZELNA

Narodowa Strategia Bezpieczeństwa TechnoRepubliki
to cybernetyczna architektura przetrwania, odporności, odstraszania,
suwerenności technologicznej i sprawczości państwa



Mapa dokumentu:

Część	Rozdział	Zakres i funkcja	Str.
Tom 1 – strategia ogólna			
0	Streszczenie strategiczne	Teza dokumentu, nadrzędność strategii i cztery komunikaty polityczne	5
1	Interes narodowy	Hierarchia interesów i kryterium bezpieczeństwa reform	7
2	Środowisko strategiczne 2026–2035	Pozycja Polski, geopolityka i narracja narodowa	9
3	Mapa Oddziaływań Geopolitycznych	Model MOG, elementy i relacje,	11
4	Prezydenckie Centrum Strategiczne	Mandat, architektura i produkty centrum decyzyjnego	13
5	Teatry aktywności PCS	Wschód, Bałtyk, Trójmorze, Transatlantyk i aktorzy globalni	15
6	Instrumenty siły: DIME+T+L	Dyplomacja, informacja, wojsko, gospodarka, technologia i prawo	32
7	Scenariusze i warianty decyzji	Scenariusze S1–S12, warianty oraz rejestr założeń krytycznych	36
A1	Słownik Tomu 1	Pojęcia strategiczne, MOG, skróty i symbole użyte w rozdziałach 0–7	40
Ż1	Baza źródłowa Tomu 1	Źródła i inspiracje wykorzystane w strategii ogólnej	49
Tom 2 – standardy wdrożeniowe			
8	Standardy bezpieczeństwa programów	Certyfikacja i macierz dziewięciu programów TechnoRepubliki	Tom 2
9	Wdrożenie i mierniki wyniku	Horyzonty wdrożenia, pulpit KPI i pakiet legislacyjny	Tom 2
10	Protokół decyzji strategicznej	Sekwencja decyzji i karta decyzji strategicznej	Tom 2
11	Karty sektorowe	Standard bezpieczeństwa i reguły wspólne programów	Tom 2
12	Narracja strategiczna	Marketing polityczny i bank zdań komunikacji publicznej	Tom 2
13	Powiązania systemowe	Relacje strategii z programami sektorowymi i architekturą państwa	Tom 2
14	Ryzyka wdrożenia	Ryzyka reformy oraz zabezpieczenia instytucjonalne	Tom 2
A2	Słownik Tomu 2	Terminy wdrożeniowe, sektorowe, legislacyjne i metryki wykonawcze	Tom 2
Ż2	Baza źródłowa Tomu 2	Źródła i standardy wdrożeniowe dla rozdziałów 8–14	Tom 2

Architektura strategii: adaptacja wzorców do TechnoRepubliki

Sekwencja strategiczna: interes → środowisko → regiony → instrumenty → warianty → odpowiedź



Formuła naczelna

Narodowa Strategia Bezpieczeństwa to nadrzędna architektura decyzji państwa, która łączy geopolitykę, obronę, dane, energię, gospodarkę, zdrowie, społeczeństwo i technologię w jeden system odporności i sprawczości. Jej celem jest przekształcenie położenia Polski z ryzyka frontowego w przewagę państwa centralnego Europy Środkowej: suwerennego w danych, energii, oprogramowaniu, produkcji, obronie i decyzji.

Relacja do Obrony Narodowej

Strategia bezpieczeństwa jest dokumentem nadrzędnym. Obrona Narodowa pozostaje dokumentem wykonawczym w domenie militarno-obronnej: rozwija odstraszenie, wojsko nowego wzoru, obywatelski system obrony i produkcję dual-use. Strategia bezpieczeństwa obejmuje natomiast pełne pole bezpieczeństwa narodowego: militarne, informacyjne, energetyczne, gospodarcze, zdrowotne, społeczne, technologiczne i kognitywne.

Klauzula legalnej transformacji

W obecnym porządku prawnym Prezydenckie Centrum Strategiczne może funkcjonować jako centrum analityczno-koordynacyjne i zaplecze foresightu strategicznego przy legalnych organach państwa. Docelowo, po przyjęciu Konstytucji TechnoRepubliki, staje się centrum egzekutywy odpowiedzialnym za mapę oddziaływań, pulpit KPI, red teaming, scenariusze i audyt wykonania strategii. Każdy etap wymaga jawnej podstawy prawnej, kontroli demokratycznej i rozliczalności za wynik.

Standard KPI

Każdy miernik strategii w wariantcie cybernetycznym musi mieć definicję, źródło danych, właściciela, częstotliwość aktualizacji, próg ostrzegawczy, próg krytyczny oraz przypisany wariant awaryjny. KPI bez progu i właściciela jest informacją opisową, a nie instrumentem sterowania państwem.

Dokument Narodowa Strategia Bezpieczeństwa jest nadrzędną strategią bezpieczeństwa i sprawczości państwa dla projektu TechnoRepubliki. Jego funkcją nie jest opis świata, lecz ustanowienie systemu decyzji: kto widzi zmianę, kto liczy ryzyko, kto proponuje warianty, kto odpowiada za wykonanie i według jakich mierników jest rozliczany wynik. Strategia bezpieczeństwa jest dokumentem nadrzędnym. Obrona Narodowa jest dokumentem sektorowym dla domeny obronnej i militarnej.

Streszczenie strategiczne

TEZA DOKUMENTU

TechnoRepublika będzie państwem, które ma widzieć własne środowisko strategiczne w czasie bliskim rzeczywistemu, rozumieć je przez modele i AI, podejmować decyzje przez legalne centrum egzekutywy oraz wykonywać je przez agencje, ekosystemy i obywateli. Bez takiego regulatora Polska pozostaje peryferią cudzych strategii.

Strategie amerykańskie wyznaczają formalną architekturę dokumentów bezpieczeństwa narodowego: interes narodowy, środowisko strategiczne, regiony, instrumenty siły, warianty decyzji i odpowiedź strategiczną. Nie przejmuje jednak treści amerykańskiej strategii. Polska nie jest mocarstwem globalnym; jest państwem centralnym Europy Środkowej, krajem frontowym NATO i węzłem między Bałtykiem, Karpatami, Białorusią, Ukrainą, Niemcami, Trójmorzem oraz łańcuchami technologii przyszłości. Dokument korzysta z architektury NSS, lecz nie przejmuje treści strategii amerykańskiej.

Strategie amerykańskie są użytecznym wzorcem formalnym, ponieważ porządkują myślenie wokół czterech interesów: ochrony narodu, dobrobytu, pokoju przez siłę i wpływu państwa. Strategia ta jest użyteczna jako ostrzeżenie: sojusze są coraz bardziej transakcyjne, ciężar obrony Europy będzie przesuwany na europejskich sojuszników, a każdy średni podmiot musi posiadać własną bazę zdolności. Wniosek dla Polski jest prosty: sojusze są konieczne, ale nie zastępują własnych danych, energii, software, produkcji, obrony i decyzji.

Narodowa Strategia Bezpieczeństwa wyznacza najwyższy standard ochrony dla wszystkich pozostałych programów TechnoSanacji. Każdy program - obrona, zdrowie, innowacje, system informacyjny, energetyka, gospodarka, polityka społeczna, kadry i seniorzy - musi odpowiedzieć na to samo pytanie: czy zmniejsza podatność państwa, skraca pętlę decyzyjną, zwiększa produkcję strategiczną, wzmacnia odporność obywateli i podnosi centralność Polski w sieciach relacji?

Strategię, ze względu na objętość, podzielono na dwa tomy. Tom 1 – strategia ogólna – zawiera definicję interesu narodowego, analizę środowiska strategicznego, model MOG, teatry aktywności, instrumenty siły oraz scenariusze. Tom 2 – standardy wdrożeniowe – rozwija model pomiarowy MOG, mierniki, protokoły decyzji, karty sektorowe, wdrożenie i ryzyka realizacyjne.

Cele strategiczne	Znaczenie
I. Przetrwanie	ciągłość państwa, integralność terytorialna, obrona ludności, odporność infrastruktury
II. Suwerenność	kontrola danych, compute, energii, software, produkcji, kadr i decyzji
III. Odporność społeczna	spójność wspólnoty, gotowość obywatelska, odporność poznawcza, zdrowie psychiczne i zdolność społeczeństwa do działania w kryzysie
IV. Dobrobyt technologiczny	gospodarka ekosystemów, przemysł dual-use, eksport technologii, kapitał cierpliwy
V. Pozycja i wpływ	wiarygodność sojusznicza, przywództwo Trójmorza, marka państwa użytecznego dla Europy

Cztery komunikaty geopolityczne strategii

1. Nie flanka i peryferium, lecz państwo centralne Europy. Polska musi przestać opisywać się językiem bufora i zacząć projektować swoją niezbędną.
2. Nie procedura i nakład, lecz wynik. Bezpieczeństwo jest mierzone zdolnością do działania pod presją, a nie budżetem, liczbą dokumentów i instytucji.
3. Nie zależność technologiczna, lecz własne tory sterowania. Dane, energia, software, produkcja i decyzja są współczesnymi granicami suwerenności.
4. Nie samo odstraszenie deklaratywne, lecz odstraszenie przez odmowę, odporność i produkcję. Państwo, którego nie da się szybko złamać, zmienia kalkulację przeciwnika.

1. Interes narodowy

Interes narodowy ma układ hierarchiczny. Najpierw państwo musi przeżyć, utrzymać integralność terytorialną, ochronić ludność i zapewnić ciągłość decyzji. Następnie musi odzyskać suwerenność w torach sterowania: danych, energii, software'u, compute, produkcji, finansów, kadr i narracji. Trzecim poziomem jest odporność społeczna, czyli zdolność wspólnoty do absorpcji szoku, obrony przed dezinformacją, zachowania zaufania, samoorganizacji i szybkiego powrotu do działania po kryzysie. Dopiero na tej podstawie państwo może budować dobrobyt technologiczny, wpływ i przywództwo.

Odwrócenie tej kolejności tworzy państwo widowiskowe: ma narrację, ale nie ma zdolności; ma sojusze, ale nie ma własnego wkładu; ma strategię, ale nie ma wykonania; ma instytucje, ale nie ma odpornego społeczeństwa zdolnego utrzymać państwo w warunkach presji, wojny informacyjnej i kryzysu.

Poziom	Treść interesu	Miernik strategiczny
Przetrwanie	integralność terytorialna, ciągłość konstytucyjna, ochrona ludności, odporność miast i infrastruktury	minimalizacja ryzyka: prawdopodobieństwo × ekspozycja × podatność × konsekwencje × (1 – zabezpieczenia)
Suwerenność	decyzje, dane, energia, software, compute, produkcja, kadry, finanse i narracja	redukcja podatności i zależności jednostronnych
Odporność	spójność społeczna, zaufanie, odporność poznawcza, zdrowie psychiczne, gotowość obywatelska, obrona cywilna i zdolność wspólnot lokalnych do działania w kryzysie	maksymalizacja zdolności absorpcji szoku i powrotu do działania: zaufanie × gotowość × kompetencje kryzysowe × odporność informacyjna / czas dezorganizacji
Dobrobyt	produktywność, reindustrializacja, eksport high-tech, przemysł dual-use, kapitał cierpliwy	wzrost centralności Polski w sieciach handlu, wiedzy i logistyki
Wpływ	pozycja w NATO, UE, Trójmorzu, B9, relacje z USA i państwami globalnymi	wzrost intensywności i trwałości relacji dodatnich oraz niezbędności Polski

1.1. Zasada krytyczna: każda reforma musi wzmacniać bezpieczeństwo

Strategia ustanawia jedną regułę nadrzędną: żaden program publiczny nie jest neutralny strategicznie. Reforma zdrowia wpływa na odporność populacji. Reforma energii decyduje o przetrwaniu centrów danych i przemysłu. Reforma gospodarcza decyduje o zdolności produkcji dronów, leków, sensorów i komponentów. Polityka kadrowa decyduje, czy państwo będzie posiadało ludzi zdolnych do kontrolowania AI, energetyki, obrony i finansów. Polityka senioralna decyduje o legitymizacji i pamięci instytucjonalnej transformacji. Dlatego Narodowa Strategia nie jest dodatkiem do programów sektorowych; jest ich wspólną normą bezpieczeństwa.

KRYTERIUM ZGODNOŚCI PROGRAMU Z NARODOWĄ STRATEGIĄ BEZPIECZEŃSTWA

Program jest strategiczny tylko wtedy, gdy jednocześnie: zmniejsza podatność państwa, zwiększa zdolności wykonawcze, skraca czas decyzji, wzmacnia odporność społeczną i buduje polską własność technologii albo danych.

2. Środowisko strategiczne 2026-2035

Środowisko strategiczne nie jest stabilnym łańcem prawa międzynarodowego, lecz złożonym polem oddziaływań. Państwa, korporacje technologiczne, platformy, rynki energii, łańcuchy dostaw, modele AI, systemy płatnicze i narracje medialne działają jak wzajemnie sprzężone regulatory. Polska musi posiadać własny model tego pola, ponieważ państwo bez modelu działa według cudzej mapy. Mapa Oddziaływań Geopolitycznych stanie się podstawowym narzędziem analitycznym oraz instrumentem zarządzania strategicznego.

2.1. Polska jako państwo centralne Europy

Polska nie powinna definiować się jako peryferia Zachodu ani bufor między cudzymi imperiami. Jej realna pozycja wynika z geometrii kontynentu: Bałtyk, Karpaty, Nizina Środkowoeuropejska, przesmyk suwalski, Ukraina, Niemcy, Czechy, Słowacja, Litwa i Morze Czarne tworzą układ, w którym Polska jest państwem przejścia, odporności i produkcji. Ta centralność jest zagrożeniem tylko wtedy, gdy państwo nie ma sterowności.

Dla TechnoRepubliki centralność staje się aktywem: pozwala pobierać rentę geostrategiczną za bezpieczeństwo, logistykę, energię, obronę, przemysł i informacje. Centralność nie oznacza samotności strategicznej. Polska buduje własną sprawczość w ramach NATO, UE, B9 i Trójmorza, zwiększając swój wkład sojuszniczy i redukując własne podatności.

Kluczowy cel geopolityczny brzmi: uczynić Polskę mniej substytuowalną dla sojuszników i trudniejszą do sparaliżowania dla przeciwników. To nie jest hasło prestiżowe. To algorytm pozycji strategicznej: zwiększać centralność dodatnich relacji i zmniejszać podatność na relacje wrogie.

2.2. Strategiczny sens narracji narodowej

W epoce permanentnego kryzysu państwo rywalizuje nie tylko zdolnościami, ale także narracją. Naród, który potrafi przekonująco odpowiedzieć na pytanie, po co istnieje w systemie międzynarodowym, uzyskuje kapitał narracyjny: przyciąga sojuszników, inwestorów, talenty i uwagę. TechnoRepublika powinna budować narrację państwa, które czyni Europę bezpieczniejszą, bardziej odporną technologicznie i mniej zależną od cudzych platform. To jest Polski Cel Strategiczny (Greater Global Purpose): Polska nie tylko broni własnej granicy, lecz zabezpiecza rdzeń odporności Europy Środkowej.

Cyberkulturowa wizja łączy polskie dziedzictwo, język i wspólnotową tożsamość z kompetencjami cyfrowymi, sztuczną inteligencją oraz suwerenną infrastrukturą informacyjną. Jej znaczenie polega na przekształceniu kultury w źródło odporności i soft power — zdolności obrony własnej narracji, przyciągania partnerów oraz współtworzenia standardów technologicznych. Dzięki niej TechnoRepublika nie tylko adaptuje cudze rozwiązania, lecz projektuje własny model nowoczesności, w którym technologia wzmacnia obywatela, ciągłość kulturową i podmiotowość państwa.

2.3. Globalne trendy geostrategiczne

Środowisko geostrategiczne lat 2026–2035 będzie kształtowane przez wielobiegunową rywalizację, warunkowość sojuszy oraz rosnące wykorzystanie technologii, gospodarki i informacji jako instrumentów siły. Poniższa tabela przedstawia najważniejsze trendy oraz wynikające z nich konsekwencje dla polskiej suwerenności, odporności i zdolności do samodzielnego działania.

Trend	Opis	Wnioski
Wielobiegunowość i rywalizacja mocarstw	Rosja, Chiny, USA, UE, Indie, Turcja i Zatoka prowadzą politykę transakcyjną i selektywną.	Polska musi budować własną zdolność negocjacyjną i niezbędność regionalną.
Warunkowość gwarancji sojusznich	Burden-sharing i burden-shifting oznaczają presję na Europę, aby płaciła i produkowała więcej zdolności.	Sojusz z USA pozostaje kluczowy, ale nie może zastępować polskiej produkcji i odporności.
Powrót geoekonomii	Sankcje, kontrola eksportu, chokepoints, surowce krytyczne i zależności energetyczne są instrumentami presji.	Dywersyfikacja i własne węzły są tak samo ważne jak klasyczna dyplomacja.
Technologia jako hard power	AI, compute, półprzewodniki, kosmos, cyber, data centers i software decydują o przewadze państw.	Suwerenny system informacyjny i gospodarka compute stają się podstawą bezpieczeństwa.
Wojna kognitywna i dezinformacja	Przeciwnik uderza w zaufanie, percepcję i wolę społeczną równie mocno jak w infrastrukturę.	Ochrona narracji narodowej jest elementem obrony, a nie zadaniem PR.
Taksonomia zagrożeń 2026-2035	konwencjonalne, nuklearne, hybrydowe, cyber, energetyczne, gospodarcze, zdrowotne, kognitywne, platformowe.	Bezpieczeństwo musi być zarządzane systemowo: wojsko, cyber, energia, zdrowie, gospodarka, informacja i platformy cyfrowe jako jedna mapa ryzyk i jedna pętla decyzji.

3. Mapa Oddziaływań Geopolitycznych

Strategia opiera się na cybernetycznym modelu wspomagania decyzji geostrategicznych. Główna przewaga tej autorskiej koncepcji polega na tym, że nie traktuje geopolityki jako zbioru impresji politycznych odniesionych do przestrzeni, lecz przedstawia środowisko bezpieczeństwa jako dynamiczny, skierowany i wielowarstwowy graf. Pozwala to opisywać nie tylko państwa, lecz również przedsiębiorstwa technologiczne, organizacje międzynarodowe, platformy cyfrowe, infrastrukturę krytyczną i łańcuchy dostaw.

Formalnie można zapisać Mapę Oddziaływań Geopolitycznych:

$$G_MOG(t) = \{V, E_1(t), E_2(t), ..., E_L(t)\}$$

gdzie:

- V — zbiór aktorów i zasobów strategicznych,
- $E_l(t)$ — relacje w warstwie l , np. militarnej, energetycznej, gospodarczej lub informacyjnej,
- t — czas,
- każda relacja $i \rightarrow j$ posiada kierunek, znak, intensywność, prawdopodobieństwo, podatność i niepewność pomiaru.

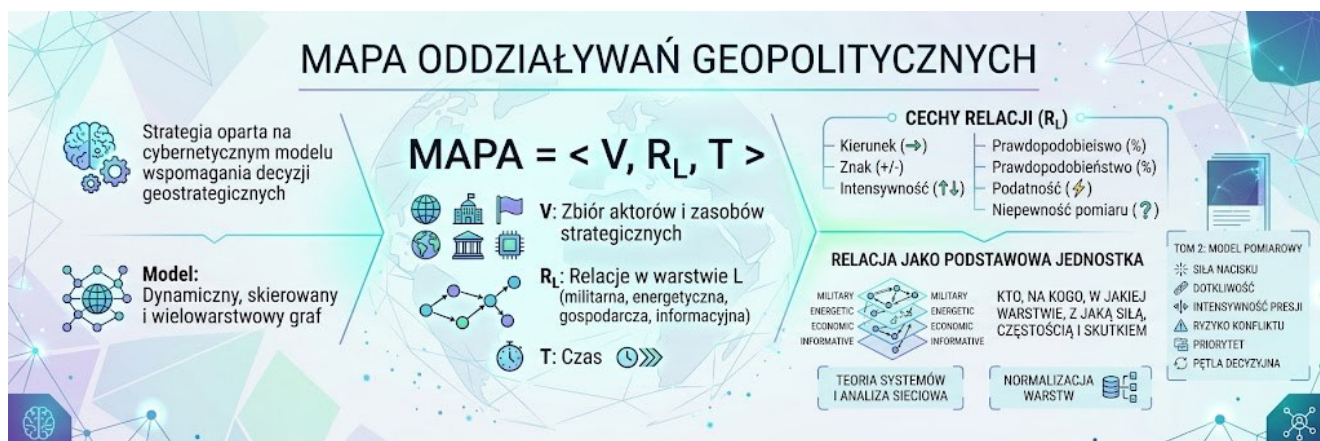
To podejście jest zgodne z teorią systemów i analizą sieciową. Należy zastrzec, że redukcja wszystkich warstw do jednego wyniku wymaga wcześniejszej normalizacji: wielkości handlu, liczby cyberataków, presji militarnej i oddziaływania informacyjnego. Nie można bezpośrednio dodawać ani mnożyć poszczególnych wartości.

Podstawową jednostką nie jest więc samo państwo, lecz relacja: kto oddziałuje, na kogo, w jakiej warstwie, w jakim kierunku i znaku, z jaką dotkliwością, jak gwałtownie, jak często i z jakim skutkiem. W tej logice mapa strategiczna jest ważonym, dynamicznym, skierowanym i wielowarstwowym grafem relacji geopolitycznych.

Narzędzia informatyczne pomagają w modelowaniu i symulacji grafów relacji. Tom 1 definiuje wspólny język MOG, natomiast Tom 2 przedstawia pełny model pomiarowy i zasady kalibracji. Model rozwija pojęcia: dotkliwość pojedynczego oddziaływania, gwałtowność, częstotliwość, intensywność presji, prawdopodobieństwo, ekspozycja, podatność, konsekwencje, zabezpieczenia, ryzyko, niepewność, pilność, priorytet decyzyjny i pętla decyzyjna.

Mapa Oddziaływań Geopolitycznych wymaga rozwijania następujących elementów:

- 1) Słownik zmiennych, ich skal i źródeł danych.
- 2) Osobne modele dla poszczególnych warstw bezpieczeństwa.
- 3) Przedziały ufności lub rozkłady prawdopodobieństwa (zamiast ocen punktowych).
- 4) Analizę korelacji, kaskad i zależności między warstwami.
- 5) Testy historyczne, analizę wrażliwości i symulacje Monte Carlo.
- 6) Kalibrację progów ostrzegawczych oraz pomiar fałszywych alarmów.
- 7) Oznaczanie jakości, aktualności i pochodzenia danych.
- 8) Niezależny audyt, red teaming i możliwość zakwestionowania rekomendacji modelu.
- 9) Zakaz autonomicznego podejmowania przez AI decyzji dotyczących eskalacji militarnej.
- 10) Modele alternatywne, aby MOG nie stała się źródłem błędów systemowych.



4. Prezydenckie Centrum Strategiczne

Prezydenckie Centrum Strategiczne (PCS) powinno być instytucjonalnym mózgiem Narodowej Strategii Bezpieczeństwa. Jego zadaniem będzie utrzymywanie aktualnej mapy oddziaływań, wyznaczanie wektorów relacji z podmiotami państwowymi i niepaństwowymi, tworzenie scenariuszy strategicznych, przygotowywanie wariantów dyplomatycznych, informacyjnych, gospodarczych i wojskowych oraz modelowanie sytuacji kryzysowych i wojennych.

Centrum nie zastępuje Rady Ministrów, resortów, służb, Sił Zbrojnych ani organów konstytucyjnych państwa. Jego funkcją jest integracja poznawcza i decyzyjna: nadanie instytucjom wspólnego modelu sytuacji, wspólnego języka decyzji, wspólnej mapy ryzyk oraz wspólnego systemu mierników. Prezydenckie Centrum Strategiczne ma skracać czas od sygnału ostrzegawczego do decyzji i wykonania przez właściwego właściciela zadania.

Klauzula prawno-ustrojowa

W obecnym porządku konstytucyjnym Prezydenckie Centrum Strategiczne może funkcjonować wyłącznie jako organ analityczno-doradczy i koordynacyjny przy Prezydencie Rzeczypospolitej Polskiej, działający w granicach obowiązującej Konstytucji, ustaw oraz kompetencji Prezydenta, Rady Ministrów, ministrów, Sił Zbrojnych, służb specjalnych i administracji publicznej. W tym trybie Centrum nie przejmuje kompetencji wykonawczych rządu ani resortów. Przygotowuje analizy, scenariusze, rekomendacje, mapy ryzyka, warianty decyzji oraz raporty strategiczne dla organów państwa.

W trybie przejściowym Centrum powinno zostać ustanowione na podstawie aktu organizacyjnego Prezydenta oraz współdziałać z Biurem Bezpieczeństwa Narodowego, Radą Bezpieczeństwa Narodowego, właściwymi ministerstwami, Rządowym Centrum Bezpieczeństwa, Siłami Zbrojnymi, służbami i operatorami infrastruktury krytycznej. Jego mandat powinien obejmować analizę strategiczną, integrację danych jawnych i niejawnych w granicach prawa, foresight, red teaming, wargaming, ocenę odporności państwa oraz przygotowywanie rekomendacji dla legalnie umocowanych organów decyzyjnych.

W docelowym modelu TechnoRepubliki Polskiej Prezydenckie Centrum Strategiczne staje się konstytucyjnie lub ustawowo umocowanym centrum sterowania strategicznego państwa,

podporządkowanym Prezydentowi jako głowie państwa i właścicielowi długookresowej strategii bezpieczeństwa.

W tym modelu Centrum nie jest superresortem, lecz metasystemem państwa: utrzymuje mapę sytuacyjną, definiuje mierniki, prowadzi scenariusze, wskazuje właścicieli misji, monitoruje wykonanie i uruchamia procedury eskalacyjne. Decyzje wykonawcze pozostają po stronie właściwych agencji, resortów i dowództw, ale są prowadzone według jednolitej mapy strategicznej, wspólnych KPI i jasnej odpowiedzialności za wynik.

Tak rozumiane Prezydenckie Centrum Strategiczne nie oznacza skoku ustrojowego poza prawo. Jest rozwiązaniem dwuetapowym: najpierw działa jako legalne centrum analityczno-koordynacyjne w obecnym porządku konstytucyjnym, a dopiero po przyjęciu docelowych zmian ustrojowych staje się pełnym centrum strategicznego sterowania TechnoRepubliki.

Komponent	Skład / kompetencje	Funkcja
Rada Strategii Narodowej	Prezydent, kluczowi sekretarze stanu, dowództwo, przedstawiciele agencji i eksperci	ustala priorytety, zatwierdza założenia krytyczne i warianty gry
Centrum Mapy Oddziaływań Geopolitycznych	analitycy relacji, data science, AI, ekonomia, geopolityka	utrzymuje graf relacji; mierzy intensywność presji, ryzyko, podatność, niepewność i centralność
Biuro Foresightu i Wargamingu	scenariusze, red team, gry strategiczne, symulacje agentowe	testuje warianty decyzji i obala fałszywe założenia
Dyrektoriat Informacyjny	narracja, FIMI, kognitywne bezpieczeństwo, OSINT	chroni wolę społeczną i kapitał narracyjny państwa
Komórka Geoeconomii	łańcuchy dostaw, surowce, energia, przemysł, sankcje, inwestycje	projektuje dźwignie gospodarcze i redukcję podatności
Pulpit KPI Państwa	dane resortów, agencji, administracji i ekosystemów	monitoruje wykonanie strategii w czasie bliskim rzeczywistemu

4.1. Produkty Prezydenckiego Centrum Strategicznego

Produkt	Opis
Mapa relacji 360°	aktualny graf podmiotów państwowych, korporacyjnych i sieciowych w otoczeniu Polski
Rejestr założeń krytycznych	jawna i okresowo testowana lista warunków, od których zależy poprawność strategii
Karta ryzyka państwa	ranking ryzyk według prawdopodobieństwa, ekspozycji, podatności, konsekwencji i skuteczności zabezpieczeń; priorytety redukcji ryzyka
Scenariusze dyplomatyczne	warianty negocjacji, koalicji, neutralizacji nacisków i budowy relacji dodatnich
Scenariusze informacyjne	narracje, kontrnarracje, kampanie odporności poznawczej, reakcje na dezinformację
Scenariusze wojenne	warianty kryzysów, eskalacji, mobilizacji, przerwania infrastruktury i uderzeń hybrydowych
Wytyczne dla programów	standardy bezpieczeństwa i KPI dla programów portalu TechnoSanacja.pl/programy

ZASADA HUMAN-IN-COMMAND

AI wspiera rozpoznanie, symulacje, ranking ryzyk i analizę wariantów.
Decyzje wysokiego ryzyka pozostają w ręku człowieka i konstytucyjnych organów państwa.
AI ma skracać pętlę poznania, nie przejmować odpowiedzialność polityczną.

5. Teatry aktywności PCS

Aktywność Prezydenta i PCS objawia się w wybranych obszarach strategicznych. Analiza relacji państwa ma układ warstwowy i domenowy. Nie obejmuje wyłącznie geografii klasycznej, lecz także przestrzeń danych, energii, zdrowia, infrastruktury, łańcuchów dostaw i odporności poznawczej społeczeństwa. Bezpieczeństwo państwa nie rozgrywa się już tylko na granicy i polu walki. Rozgrywa się jednocześnie w systemie energetycznym, cyberprzestrzeni, logistyce, platformach cyfrowych, narracji publicznej, dostępności leków, produkcji amunicji, przepływach kapitału i zdolności społeczeństwa do zachowania spójności w kryzysie.

Teatry geograficzne i relacyjne

1. Wschód i sąsiedzi graniczni. Obejmuje Rosję, Białoruś, Ukrainę, Litwę, przesmyk suwalski oraz całą infrastrukturę przygraniczną. Jest to teatr egzystencjalny: decyduje o przetrwaniu, integralności terytorialnej, odstraszeniu przez odmowę, ochronie granicy, obronie warstwowej, fortyfikacji, drone wall, rozpoznaniu i odporności na presję hybrydową.

2. Bałtyk. Obejmuje porty, stocznie, morską energetykę wiatrową, gazociągi, kable podmorskie, terminale LNG, infrastrukturę offshore oraz bezpieczeństwo dna morskiego. Bałtyk jest dla TechnoRepubliki nie tylko akwenem, ale strategicznym systemem dostępu: do energii, handlu, transportu, danych i projekcji siły sojuszniczej.

3. Trójmorze i głębia regionalna. Obejmuje Europę Środkową, Bukaresztańską Dziewiątkę, Via Carpatia, Rail Baltica, korytarze północ-południe, mobilność wojskową, logistykę dual-use i regionalne systemy odporności. Celem TechnoRepubliki jest przekształcenie Polski z państwa frontowego w państwo centralne: węzeł logistyczny, energetyczny, cyfrowy, wojskowy i przemysłowy regionu.

4. Transatlantyk. Obejmuje relacje z USA, NATO, Kanadą i Wielką Brytanią, pozostające podstawą odstraszenia oraz dostępu do technologii, rozpoznania i zdolności sojuszniczych. Wobec warunkowości gwarancji, presji na burden-sharing i przesunięcia uwagi USA na Indo-Pacyfik Polska powinna wzmacniać swoją wiarygodność przez wydatki obronne, wkład produkcyjny i rozwój własnych zdolności.

5. Europa Zachodnia. Obejmuje Niemcy, Francję i instytucje Unii Europejskiej jako przestrzeń rynku, regulacji, kapitału, technologii i współpracy przemysłowej. Zadaniem PCS jest budowanie koalicji projektowych, wpływanie na europejskie standardy oraz ograniczanie ryzyka asymetrii interesów, spowolnienia regulacyjnego i marginalizacji polskiego przemysłu obronnego.

6. Aktorzy globalni i korporacyjni. Obejmuje Chiny, Indie, Turcję, państwa Zatoki, globalne fundusze oraz korporacje kontrolujące platformy, dane, półprzewodniki, moc obliczeniową i cyfrowe punkty dostępu. Polska powinna prowadzić selektywne partnerstwa, dywersyfikować zależności, chronić suwerenność danych i platform oraz wykorzystywać kapitał strategiczny bez oddawania prywatnym bramkarzom kontroli nad infrastrukturą krytyczną.

Teatry funkcjonalne

7. Infrastruktura krytyczna. Obejmuje sieci energetyczne, gazowe, wodne, kolejowe, drogowe, portowe, telekomunikacyjne, data centers, szpitale, magazyny, systemy płatnicze i administrację cyfrową. W tym teatrze przeciwnik może nie przekraczać granicy państwa, lecz paraliżować jego funkcje przez sabotaż, cyberatak, awarię łańcuchową lub operację wpływu.

8. Cyberprzestrzeń, AI i system informacyjny państwa. Obejmuje dane, modele AI, compute, chmurę państwową, kryptografię, systemy dowodzenia, agentów AI, cyberbezpieczeństwo i cyfrowego bliźniaka państwa. W tym teatrze rozstrzyga się szybkość decyzji, odporność administracji, ochrona tajemnic państwowych, bezpieczeństwo wyborów, zdolność rozpoznania i przewaga informacyjna.

9. Energia. Obejmuje elektroenergetykę, paliwa, gaz, wodór, atom, OZE, magazyny energii, lokalne bilansowanie, ciepłownictwo, rezerwy strategiczne i zasilanie infrastruktury krytycznej. Energia jest torowiskiem suwerenności: bez odpornego zasilania nie działa wojsko, AI, przemysł, ochrona zdrowia, transport ani administracja.

10. Zdrowie i bezpieczeństwo biologiczne. Obejmuje system ochrony zdrowia, dostępność leków, rezerwy medyczne, diagnostykę, biotechnologię, pandemie, zdrowie psychiczne i zdolność państwa do utrzymania populacji w stanie sprawności. W wersji bezpieczeństwa zdrowie nie jest wyłącznie polityką społeczną, lecz elementem odporności narodowej.

11. Społeczeństwo, kognityka i wojna informacyjna. Obejmuje odporność poznawczą, zaufanie społeczne, narrację narodową, edukację obywatelską, odporność na dezinformację, mobilizację społeczną, obronę cywilną i gotowość lokalnych wspólnot do działania. Przeciwnik uderza tu w wolę oporu, percepcję rzeczywistości, zaufanie do państwa i zdolność społeczeństwa do zachowania spójności.

12. Łańcuchy dostaw i geoekonomia. Obejmuje surowce krytyczne, chipy, leki, amunicję, komponenty przemysłowe, żywność, finansowanie, technologie dual-use, transport i zależność od platform globalnych. Celem TechnoRepubliki jest redukcja podatności na szantaż, dywersyfikacja dostaw, friend-shoring, budowa rezerw oraz rozwój krajowej produkcji strategicznej.

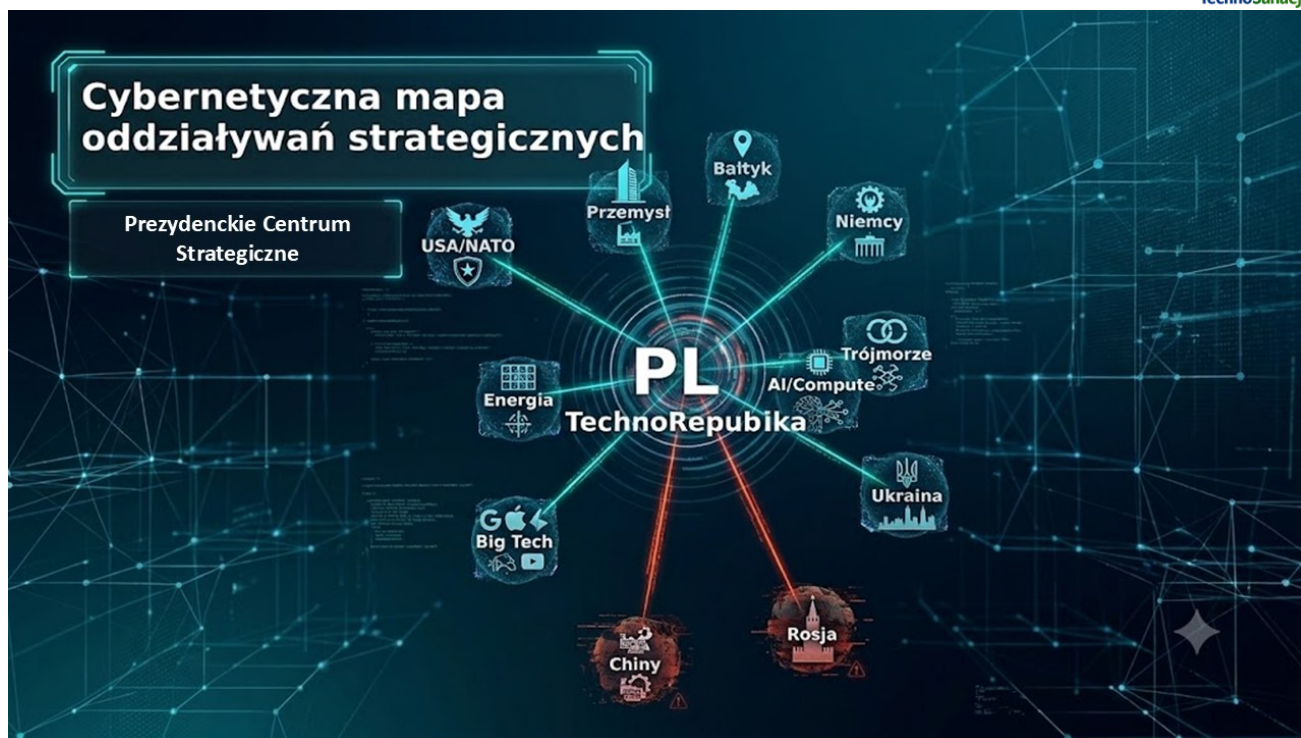
W tej typologii główne teatry geograficzne — Wschód, Bałtyk i Trójmorze - łączą się z teatrami funkcjonalnymi: infrastrukturą krytyczną, cyber/AI, energią, zdrowiem, społeczeństwem i łańcuchami dostaw. Dopiero ich wspólna analiza pozwala państwu widzieć realne pole walki XXI wieku. TechnoRepublika musi zatem prowadzić strategię nie jako zbiór resortowych polityk, lecz jako jeden system bezpieczeństwa, w którym każdy teatr ma właściciela, KPI, progi ostrzegawcze, warianty awaryjne i jasną ścieżkę eskalacji.

W wyniku analiz powstaje na bieżąco wizualizacja w formie cybernetycznej mapy oddziaływań strategicznych, która jest komplementarnym mechanizmem do Mapy Oddziaływań Geopolitycznych. TechnoRepublika występuje jako węzeł centralny reagujący na presję zewnętrzną, który aktywnie monitoruje, modeluje i steruje relacjami z otoczeniem. Zielone wektory mogą oznaczać relacje wzmacniające potencjał państwa: sojusze, energetykę, przemysł, AI/compute, Bałtyk i Trójmorze. Czerwone wektory mogą wskazywać relacje wysokiego ryzyka: Rosję i Chiny jako źródła presji militarnej, technologicznej, informacyjnej i geoeconomicznej. Rolą Prezydenckiego Centrum Strategicznego jest utrzymywanie aktualnej mapy strategicznej aktorów, ryzyk i zależności oraz przekładanie jej na decyzje: dyplomatyczne, obronne, przemysłowe, energetyczne i informacyjne.

Najważniejszy wniosek:

Cybernetyczna mapa oddziaływań strategicznych nie jest ilustracją geopolityczną, lecz narzędziem decyzyjnym.

Każdy teatr powinien mieć własne mierniki ryzyka, właściciela instytucjonalnego, scenariusze eskalacyjne i pakiet odpowiedzi strategicznej.



Teatr	Zakres	Ryzyko	Odpowiedź
Wschód i sąsiedzi graniczni	Rosja, Białoruś, Ukraina, Litwa, przesmyk suwalski	A2AD, presja hybrydowa, migracja instrumentalizowana, wojna na Ukrainie	odstraszanie przez odmowę, fortyfikacja, drone wall, obrona warstwowa
Bałtyk	porty, kable, gazociągi, offshore, dno morskie	sabotaż podmorski, paraliż portów, wojna na dnie morskim	dozór, redundancja kabli, odporność portów, siły morskie i powietrzne
Europa Środkowa / Trójmorze	Via Carpatia, Rail Baltica, B9, energetyka i logistyka	fragmentacja, opóźnienia infrastrukturalne, brak wspólnej narracji	korytarze odporności, wspólne zakupy, wspólne standardy i projekty dual-use
Transatlantyk	USA, NATO, Kanada, Wielka Brytania	warunkowość gwarancji, burden-shifting, priorytet Indo-Pacific	wkład produkcyjny, wydatki obronne, wiarygodność i zdolności własne
Europa Zachodnia	Niemcy, Francja, UE, przemysł, regulacje	ryzyko regulacyjnego spowolnienia i asymetrii interesów	koalicje projektowe, standardy, rynek, de-risking, obrona przemysłowa
Aktorzy globalni i korporacyjni	Chiny, Indie, Turcja, Zatoka, Big Tech, fundusze, platformy	chokepoints technologiczne, prywatni bramkarze, zależności danych	suwerenne dane, kontrola platform, partnerstwa selektywne, kapitał strategiczny

5.1. Wschód — strefa bliskiego oddziaływania

Najwyższy priorytet bezpieczeństwa TechnoRepubliki Polskiej otrzymuje Wschód, czyli przestrzeń, w której czas decyzji jest najkrótszy, a skutki błędu mogą być egzystencjalne. Teatr wschodni obejmuje:

Rosję, Białoruś, Ukrainę, Litwę, Przesmyk Suwalski, Obwód Kaliningradzki, granicę państwową, infrastrukturę przygraniczną oraz zaplecze logistyczne wschodniej flanki NATO.

Wschód nie jest jednym kierunkiem geograficznym, lecz układem powiązanych zagrożeń: presji militarnej, A2AD, działań hybrydowych, instrumentalizacji migracji, dywersji, sabotażu infrastruktury, operacji informacyjnych, cyberataków, rozpoznania przeciwnika oraz testowania odporności państwa. W tej strefie każda godzina zwłoki może stać się przewagą przeciwnika, dlatego państwo musi działać według logiki stałego rozpoznania, szybkiej decyzji i natychmiastowego wykonania.

Rosja pozostaje głównym źródłem ryzyka militarnego, nuklearnego, cybernetycznego, energetycznego i informacyjnego. Jej celem strategicznym jest osłabienie spójności NATO, testowanie determinacji państw granicznych, zastraszanie społeczeństw oraz rozbijanie zdolności decyzyjnej przeciwnika poniżej progu otwartej wojny.

Białoruś pełni funkcję wysuniętej platformy operacyjnej Rosji. Jest źródłem presji granicznej, instrumentalizacji migracji, prowokacji, rozpoznania, operacji psychologicznych oraz potencjalnego rozwinięcia wojskowego przeciwko Polsce, Litwie i Ukrainie.

Ukraina jest strategiczną głębią bezpieczeństwa Polski. Jej doświadczenia wojenne są dla TechnoRepubliki podstawowym laboratorium przyszłej obrony: drony, amunicja krążąca, obrona warstwowa, rozpoznanie satelitarne i taktyczne, walka radioelektroniczna, rozproszenie dowodzenia, szybka produkcja, odporność społeczeństwa i znaczenie zapasów amunicji muszą zostać przełożone na polski system obronny.

Litwa i Przesmyk Suwalski stanowią krytyczny węzeł spójności NATO między Polską a państwami bałtyckimi. Przesmyk Suwalski nie może być traktowany wyłącznie jako punkt na mapie, lecz jako zintegrowany system: obrona terytorialna, mobilność wojskowa, drogi, kolej, łączność, magazyny, obrona powietrzna, counter-UAS, logistyka, ochrona ludności i wspólne planowanie z Litwą oraz sojusznikami.

Kaliningrad i system A2AD tworzą stałe zagrożenie dla swobody działania Polski i NATO w regionie. TechnoRepublika musi traktować Kaliningrad jako źródło presji rakietowej, powietrznej, morskiej, elektronicznej, cybernetycznej i informacyjnej. Odpowiedzią nie jest pojedynczy system uzbrojenia, lecz odporna architektura: rozpoznanie, obrona powietrzna, rozproszenie infrastruktury, zapasowe centra dowodzenia, redundancja łączności i zdolność działania mimo zakłóceń.

Stałymi zadaniami PCS na teatrze wschodnim są:

Element	Ryzyko	Odpowiedź TechnoRepubliki
Rosja	presja militarna, nuklearna, cyber, informacyjna	odstraszanie przez odmowę, obrona warstwowa, gotowość sojusznicza, własna produkcja obronna
Białoruś	migracja instrumentalizowana, prowokacje, rozpoznanie, platforma Rosji	wzmocniona granica, szybka reakcja SG i wojska, odporność prawna, komunikacja strategiczna
Ukraina	długotrwała wojna, ryzyko eskalacji, presja logistyczna	strategiczna głębia, wsparcie odporności, transfer lekcji wojennych do polskiej doktryny
Litwa i Przesmyk Suwalski	przecięcie spójności NATO, paraliż mobilności	wspólne planowanie, infrastruktura dual-use, obrona korytarza, ćwiczenia z Litwą i NATO
Kaliningrad/A2AD	blokowanie swobody działania, presja rakietowa i radioelektroniczna	rozpoznanie, OPL, counter-UAS, redundancja dowodzenia, rozproszenie infrastruktury
Infrastruktura przygraniczna	dywersja, sabotaż, cyberatak, awaria łańcuchowa	ochrona fizyczna i cyfrowa, monitoring, rezerwy, szybka naprawa, lokalne centra kryzysowe
Spółeczeństwo przygraniczne	panika, dezinformacja, zmęczenie kryzysem	obrona cywilna, edukacja kryzysowa, komunikaty państwa, odporność poznawcza

Strategia dla Wschodu wymaga stałego obrazu sytuacji w czasie bliskim rzeczywistości. Obejmuje to rozpoznanie wielodomenowe, monitoring granicy, analizę OSINT, dane sojusznicze, kontrolę infrastruktury krytycznej, śledzenie operacji informacyjnych oraz ocenę gotowości lokalnej administracji. Każdy incydent na granicy, w cyberprzestrzeni, logistyce, energetyce lub przestrzeni informacyjnej musi być przypisany do właściciela reakcji i rozliczony w pętli:

sygnał — analiza — decyzja — wykonanie — informacja zwrotna.

Lekcje z wojny na Ukrainie wskazują, że przewagę uzyskuje państwo, które szybciej widzi, szybciej decyduje, szybciej produkuje i szybciej adaptuje taktykę. Dlatego teatr wschodni wymaga nie tylko silnej armii, ale także: zapasów amunicji, dronów i counter-UAS, mobilnej obrony powietrznej, walki radioelektronicznej, fortyfikacji, odpornych miast, lokalnych rezerw, rozproszonej energetyki, zapasowej łączności oraz administracji zdolnej do działania bez komfortu pokoju.

Celem TechnoRepubliki na Wschodzie jest odstraszanie przez odmowę: przeciwnik ma wiedzieć, że presja militarna, hybrydowa, migracyjna, cybernetyczna lub sabotażowa nie sparaliżuje państwa, nie złamie społeczeństwa i nie doprowadzi do opóźnienia decyzji. Wschód musi być zarządzany jako stały teatr operacyjny państwa, a nie jako seria incydentów obsługiwanych po fakcie.

5.2. Bałtyk — morski teatr infrastruktury krytycznej

Bałtyk jest dla Polski osobnym teatrem bezpieczeństwa, ponieważ łączy w jednej przestrzeni handel, energię, dane, logistykę, projekcję siły NATO, porty, offshore wind, gazociągi, kable podmorskie i infrastrukturę dna morskiego. Nie jest to wyłącznie akwen morski ani zaplecze gospodarki morskiej. Jest to system krytyczny, którego zakłócenie może uderzyć jednocześnie w energetykę, łączność, transport, gospodarkę, wojsko i odporność społeczną.

W logice TechnoRepubliki Bałtyk należy traktować jako morską przestrzeń sterowania państwem. Przeciwnik nie musi dokonywać klasycznego ataku militarnego, aby wywołać efekt strategiczny. Wystarczy uszkodzenie kabla podmorskiego, sabotaż gazociągu, blokada portu, awaria terminalu LNG, zakłócenie pracy farm offshore, cyberatak na operatora logistycznego albo operacja dezinformacyjna dotycząca bezpieczeństwa infrastruktury. Dlatego strategia Bałtyku musi przejść od modelu reaktywnego — „naprawiamy po sabotażu” — do modelu ciągłego dozoru, redundancji i odstraszania przez wykrywalność.

Zakres aktywności dla teatru bałtyckiego

Obszar	Znaczenie dla TechnoRepubliki	Główne ryzyko	Odpowiedź strategiczna
Kable podmorskie	łączność, dane, finanse, administracja, systemy wojskowe	przecięcie, podsłuch, sabotaż, zakłócenie transmisji	redundancja tras, monitoring pasywny, szybka naprawa, ochrona fizyczna i cyber
Gazociągi i infrastruktura energetyczna	bezpieczeństwo energetyczne, zasilanie gospodarki i przemysłu	sabotaż, eksplozja, presja energetyczna, awaria łańcuchowa	monitoring, rezerwy, dywersyfikacja dostaw, plany ciągłości działania
Porty	handel, logistyka wojskowa, import surowców, eksport przemysłowy	blokada, cyberatak, sabotaż, paraliż przeładunków	ochrona portów, logistyka dual-use, zapasowe trasy, integracja z NATO
Offshore wind	energia, przemysł morski, transformacja energetyczna	sabotaż turbin, kabli eksportowych i stacji elektroenergetycznych	dozór morski, redundancja przyłączy, ochrona infrastruktury offshore
Dno morskie	przestrzeń przebiegu kabli, gazociągów, sensorów i infrastruktury	działania podprogowe, operacje specjalne, minowanie, ukryte urządzenia	mapa dna, sensory, monitoring pasywny, współpraca z marynarką i operatorami
Łączność morska i satelitarna	dowodzenie, ratownictwo, żegluga, wojsko, porty	zakłócanie, spoofing, cyberatak, utrata sygnału	redundancja łączności, kanały zapasowe, integracja z systemami NATO
Żegluga i szlaki handlowe	dostęp do rynków, ciągłość dostaw, mobilność wojskowa	blokada, prowokacje, presja militarna, incydenty hybrydowe	rozpoznanie, eskortowanie, plany awaryjne, współpraca sojusznicza

Logika infrastruktury podmorskiej

Najważniejszą zmianą w podejściu do Bałtyku jest uznanie, że dno morskie stało się przestrzenią strategiczną. Kable podmorskie i gazociągi są dziś odpowiednikiem arterii państwa. Przenoszą dane, energię i sterowanie, a ich uszkodzenie może wywołać skutki większe niż klasyczny atak na pojedynczy obiekt lądowy.

Dlatego TechnoRepublika powinna aktualizować **Bałtycką Mapę Infrastruktury Podmorskiej**, obejmującą przebieg kabli, gazociągów, przyłączy energetycznych, stacji offshore, punktów lądowania kabli, węzłów portowych, torów podejściowych, sensorów, akwenów szczególnie wrażliwych oraz potencjalnych miejsc sabotażu. Mapa ta powinna być aktualizowana w czasie bliskim rzeczywistości i połączona z systemem ostrzegania państwa.

Monitoring i dozór Bałtyku

Bałtyk wymaga stałego dozoru wielowarstwowego. Obejmuje on:

- monitoring pasywny — nasłuch akustyczny, analiza anomalii ruchu statków, wykrywanie nietypowej aktywności w pobliżu kabli, gazociągów i farm offshore;
- monitoring aktywny — patrole morskie, drony nawodne, podwodne i powietrzne, inspekcje infrastruktury, satelitarne śledzenie jednostek, współpraca z operatorami komercyjnymi;
- monitoring cybernetyczny — ochrona systemów portowych, energetycznych, logistycznych, terminalowych, telekomunikacyjnych i operatorskich;
- monitoring informacyjny — wykrywanie narracji dezinformacyjnych dotyczących awarii, skażeń, rzekomych zaniedbań państwa, kosztów energetyki offshore lub bezpieczeństwa portów.

Celem nie jest pełna kontrola każdego metra dna morskiego, lecz zbudowanie takiego systemu wykrywania anomalii, aby przeciwnik wiedział, że działania sabotażowe będą trudne do ukrycia, szybko przypisane i objęte odpowiedzialnością państwa oraz sojuszników.

Redundancja i ciągłość działania

Każda infrastruktura krytyczna na Bałtyku musi mieć wariant awaryjny. Oznacza to, że strategia nie może zakładać nienaruszalności kabli, gazociągów, portów czy farm offshore. Musi zakładać ich czasową utratę i przygotować państwo do działania mimo zakłócenia.

Minimalny standard TechnoRepubliki obejmuje **redundancję**:

- łączności — alternatywne kable, trasy lądowe, łączność satelitarna, radiolinie, systemy wojskowe i kanaty awaryjne;
- energetyczną — zapasowe źródła zasilania, magazyny energii, lokalne bilansowanie, awaryjne zasilanie portów i punktów lądowania infrastruktury;
- portową — możliwość przekierowania przładunków między portami, alternatywne terminale, zapasowe trasy kolejowe i drogowe;
- dowodzenia — zapasowe centra koordynacji, łączność kryzysowa, wspólne procedury marynarki, straży granicznej, operatorów portów, energetyki i administracji lokalnej;
- naprawczą — dostęp do wyspecjalizowanych jednostek, ekip technicznych, części zamiennych, kabli, sprzętu podwodnego i umów serwisowych uruchamianych w trybie kryzysowym.

Scenariusze sabotażu

Dla teatru bałtyckiego należy prowadzić stałe scenariusze sabotażu i ćwiczenia międzyresortowe. Minimalny katalog scenariuszy obejmuje:

Scenariusz	Skutek strategiczny	Wymagana reakcja
Przecięcie kabla podmorskiego	zakłócenie łączności, danych, finansów lub systemów administracji	przełączenie na trasy zapasowe, lokalizacja uszkodzenia, komunikat publiczny, naprawa i dochodzenie
Sabotaż gazociągu	kryzys energetyczny, presja cenowa, efekt psychologiczny	izolacja odcinka, rezerwy, dywersyfikacja dostaw, ochrona pozostałej infrastruktury
Atak na port	paraliż handlu, opóźnienie mobilności wojskowej	przekierowanie przeladunków, ochrona portu, cyberodporność, wsparcie wojska i służb
Uszkodzenie farmy offshore	utrata mocy, wzrost niepewności inwestycyjnej	wyłączenie segmentu, naprawa, ochrona kabli eksportowych, komunikacja strategiczna
Zakłócanie GPS/AIS	ryzyko kolizji, chaos żeglugowy, utrata świadomości sytuacyjnej	przejsie na systemy alternatywne, ostrzeżenia dla żeglugi, śledzenie satelitarne
Operacja dezinformacyjna po awarii	panika, spadek zaufania, presja polityczna	szybka informacja państwa, ujawnienie faktów, neutralizacja narracji przeciwnika

Cel strategiczny

Celem TechnoRepubliki na Bałtyku jest zapewnienie, aby żaden incydent morski, podmorski, energetyczny, portowy ani telekomunikacyjny nie był w stanie sparaliżować państwa. Bałtyk ma być chroniony jako wspólna przestrzeń bezpieczeństwa Polski, NATO, państw nordyckich i bałtyckich. Oznacza to stałą współpracę wojskową, wywiadowczą, portową, energetyczną i technologiczną.

W formule operacyjnej:

Bezpieczeństwo Bałtyku = dozór dna morskiego × redundancja łączności i energii × odporność portów × szybka naprawa × sojusznicza odpowiedź.

TechnoRepublika nie może czekać na sabotaż, aby odkryć zależność. Musi znać swoje podmorskie arterie wcześniej, mierzyć ich podatność, ćwiczyć warianty awaryjne i budować zdolność działania mimo uszkodzenia. Bałtyk jest nie tylko granicą morską. Jest systemem życia gospodarczego, energetycznego, informacyjnego i wojskowego państwa.

5.3. Trójmorze jako korytarz odporności

Trójmorze nie może być dla Polski wyłącznie formatem spotkań politycznych, deklaracji dyplomatycznych i wspólnych komunikatów. W wersji bezpieczeństwa musi zostać zdefiniowane jako regionalny system korytarzy odporności, łączący infrastrukturę, logistykę, energię, dane, obronę, przemysł dual-use i mobilność wojskową. Jego celem nie jest sama współpraca regionalna, lecz budowa realnej zdolności Europy Środkowej do przetrwania kryzysu, wsparcia wschodniej flanki NATO, utrzymania przepływów gospodarczych i szybkiego reagowania na presję zewnętrzną.

Dla TechnoRepubliki Trójmorze oznacza przejście od myślenia o Polsce jako państwie granicznym do myślenia o Polsce jako organizatorce regionalnej sprawczości. Polska ma nie tylko korzystać z położenia między Bałtykiem, Adriatykiem i Morzem Czarnym, ale świadomie budować swoją centralność w sieciach: transportu, energii, danych, produkcji, bezpieczeństwa i dyplomacji. Im większa centralność Polski w tych sieciach, tym większa jej odporność, znaczenie sojusznicze i zdolność do kształtowania decyzji w NATO, UE i regionie.

Logika korytarzy odporności

Trójmorze powinno być projektowane jako centrum europejskie NATO oraz układ dwóch osi strategicznych:

- oś północ-południe — Bałtyk, Polska, Karpaty, Adriatyk, Morze Czarne;
- oś wschód-zachód — Białoruś, Ukraina, Polska, Niemcy, Europa Zachodnia

Dopiero skrzyżowanie tych osi tworzy realną głębię strategiczną. Oś północ-południe zmniejsza historyczną zależność regionu od infrastruktury zorientowanej wyłącznie na Zachód. Oś wschód-zachód utrzymuje połączenie z rdzeniem gospodarczym Europy i systemem sojuszniczym. TechnoRepublika musi łączyć obie logiki: być państwem frontowym wobec Wschodu, ale jednocześnie państwem centralnym dla regionalnej logistyki, energii, danych i produkcji.

Trójmorze jako system energii, logistyki, danych i obrony

W modelu TechnoRepubliki Trójmorze powinno zostać opisane wzorem:

$$\text{Trójmorze} = \text{energia} \times \text{logistyka} \times \text{dane} \times \text{obrona} \times \text{przemysł dual-use}$$

Energia zapewnia zasilanie państwa i gospodarki. Logistyka zapewnia przepływ wojsk, towarów, surowców, leków i pomocy. Dane zapewniają sterowanie, komunikację, AI, finanse i administrację. Obrona zapewnia zdolność odstraszenia i utrzymania korytarzy w warunkach presji. Przemysł dual-use zapewnia produkcję sprzętu, technologii i komponentów, bez których region pozostaje zależny od zewnętrznych dostawców.

Trójmorze musi więc stać się regionalnym systemem ciągłości działania. W kryzysie ma umożliwić przekierowanie transportu, energii, danych i dostaw przez alternatywne trasy. W czasie pokoju ma tworzyć wzrost gospodarczy, inwestycje infrastrukturalne, rynek dla technologii i wspólną bazę przemysłową. W czasie wojny lub presji hybrydowej ma zapewnić mobilność wojskową, odporność infrastruktury i ciągłość funkcji państwowych.

Główne elementy Trójmorza jako korytarza odporności

Element	Znaczenie dla TechnoRepubliki	Ryzyko	Odpowiedź strategiczna
Via Carpatia	drogowy kręgosłup północ-południe, mobilność wojskowa i gospodarcza	przerwanie korytarzy, wąskie gardła, brak przepustowości	przyspieszenie inwestycji, standard dual-use, zapasowe trasy
Rail Baltica i kolej regionalna	szybki transport ludzi, wojska, towarów i pomocy kryzysowej	paraliż transportu, różnice techniczne, opóźnienia inwestycyjne	interoperacyjność, terminale przeladunkowe, priorytet wojskowy
Porty Bałtyku, Adriatyku i Morza Czarnego	dostęp do handlu, energii, sprzętu wojskowego i surowców	blokada morska, sabotaż, cyberatak	sieć portów zapasowych, ochrona portów, logistyka NATO
Interkonektory i energia	odporność energetyczna regionu, dywersyfikacja dostaw	szantaż energetyczny, awarie, zależność od jednego kierunku	połączenia transgraniczne, magazyny energii, lokalne bilansowanie
Centra danych i sieci cyfrowe	suwerenność danych, AI, administracja, bezpieczeństwo komunikacji	cyberatak, zależność od globalnych platform, utrata łączności	regionalna chmura, redundancja, cyberodporność, data centers w Polsce
Przemysł dual-use	produkcja dronów, amunicji, sensorów, systemów energetycznych i cyber	zależność importowa, brak skali, rozproszenie produkcji	wspólne zamówienia, konsorcja przemysłowe, produkcja w regionie
Magazyny i rezerwy strategiczne	paliwa, leki, żywność, amunicja, części zamienne	przerwanie dostaw, panika rynkowa, kryzys logistyczny	regionalna mapa rezerw, zapasy 90–180 dni, wspólne procedury
Mobilność wojskowa	szybkie przerzuty sił NATO i wsparcia na flankę wschodnią	zatory, brak mostów, różne standardy, słaba koordynacja	audyt tras, infrastruktura dual-use, ćwiczenia i priorytetyzacja ruchu

Polska jako węzeł centralny

Celem TechnoRepubliki nie jest bierne uczestnictwo w Trójmorzu, lecz uzyskanie pozycji głównego węzła operacyjnego regionu. Polska powinna być miejscem, gdzie krzyżują się:

- korytarze transportowe północ-południe i wschód-zachód;
- interkonektory energetyczne i magazyny energii;
- centra danych, chmura państwowa i infrastruktura AI;
- łańcuchy produkcji dual-use;
- logistyka wojskowa NATO;
- zaplecze odbudowy Ukrainy;
- sieci naukowe, przemysłowe i technologiczne regionu.

Taka centralność nie powstanie sama. Wymaga konsekwentnej polityki inwestycyjnej, dyplomacji gospodarczej, wspólnych projektów infrastrukturalnych, standardów interoperacyjności, finansowania i stałego monitorowania KPI. Każdy projekt Trójmorza powinien być oceniany nie tylko według kosztu i terminu, ale również według wpływu na centralność Polski, odporność regionu i zdolność działania w kryzysie.

Ukraina i wschodnia flanka jako wymiar Trójmorza

Trójmorze w wersji bezpieczeństwa nie może pomijać Ukrainy. Ukraina jest strategiczną głębią bezpieczeństwa Polski i naturalnym rozszerzeniem korytarzy odporności na Wschód. Odbudowa Ukrainy, jej integracja infrastrukturalna, energetyczna, logistyczna i technologiczna z regionem powinny być traktowane jako projekt bezpieczeństwa, a nie wyłącznie program gospodarczy.

Polska powinna dążyć do tego, aby szlaki odbudowy Ukrainy, dostawy technologii, logistyka wojskowa, energetyka, magazyny, produkcja dronów, systemy cyberbezpieczeństwa i przemysł dual-use wzmacniały polską centralność, a nie omijały Polskę. W tym sensie Trójmorze jest również narzędziem walki o architekturę powojennej Europy Środkowo-Wschodniej.

Standard operacyjny Trójmorza

TechnoRepublika powinna promować w Trójmorzu wspólny standard operacyjny:

Standard	Sens operacyjny
Dual-use by design	każda duża inwestycja transportowa, energetyczna i cyfrowa musi mieć wariant cywilny i wojskowy
Redundancja	każdy krytyczny przepływ musi mieć trasę alternatywną
Interoperacyjność	systemy kolejowe, energetyczne, cyfrowe i wojskowe muszą współpracować ponad granicami
Rezerwy regionalne	paliwa, leki, amunicja, żywność i części krytyczne muszą być mapowane w skali regionu
Cyberodporność	infrastruktura Trójmorza musi być chroniona przed cyberatakiem i operacjami wpływu
Wspólne ćwiczenia	korytarze muszą być testowane w scenariuszach kryzysowych, wojskowych i logistycznych
KPI centralności	każdy projekt powinien zwiększać centralność Polski i odporność całego regionu

Scenariusze kryzysowe dla Trójmorza

Dla Trójmorza należy prowadzić stałe scenariusze i ćwiczenia. Minimalny katalog obejmuje:

Scenariusz	Skutek strategiczny	Odpowiedź TechnoRepubliki
Blokada lub sabotaż portu bałtyckiego	zakłócenie handlu i dostaw wojskowych	przekierowanie do portów alternatywnych, logistyka kolejowa i drogowa
Przerwanie korytarza kolejowego	paraliż mobilności wojskowej i gospodarczej	trasy zapasowe, transport drogowy, priorytet wojskowy
Kryzys energetyczny w regionie	wzrost cen, presja polityczna, ryzyko blackoutu	interkonektory, magazyny, lokalne bilansowanie, solidarność energetyczna
Cyberatak na sieć logistyczną	chaos w transporcie i odprawach	tryb manualny, systemy zapasowe, CERT regionalny
Nagły napływ uchodźców lub rannych	przeciążenie samorządów, zdrowia i transportu	centra recepcyjne, rezerwy medyczne, koordynacja z Ukrainą i NATO
Przerwanie dostaw leków, chipów lub amunicji	podatność strategiczna regionu	wspólne zakupy, rezerwy, produkcja regionalna, friend-shoring

Cel strategiczny

Celem TechnoRepubliki jest przekształcenie Trójmorza z formatu politycznego w system regionalnej odporności i sprawczości. Polska ma być nie tylko uczestnikiem spotkań, ale architektem korytarzy, właścicielem standardów, organizatorem projektów i węzłem wykonawczym regionu.

W formule operacyjnej:

**Trójmorze jako korytarz odporności = infrastruktura dual-use × energia × logistyka
× dane × przemysł × mobilność wojskowa × wspólne standardy.**

Dzięki temu Polska przestaje być wyłącznie państwem frontowym, które oczekuje wsparcia, a staje się państwem centralnym, które to wsparcie organizuje, wzmacnia i rozprowadza. Tak rozumiane Trójmorze jest jednym z głównych instrumentów przejścia od peryferyjności do podmiotowości strategicznej.

6. Instrumenty siły TechnoRepubliki: DIME+T+L

DIME+T+L - instrumenty siły TechnoRepubliki

Klasyczne DIME — dyplomacja, informacja, wojsko i gospodarka — wymaga w XXI wieku rozszerzenia do formuły DIME+T+L: dyplomacja, informacja, wojsko, gospodarka, technologia oraz prawo/regulacja.



Technologia nie jest pojedynczym sektorem. Jest mnożnikiem wszystkich instrumentów siły. Bez danych dyplomacja staje się reaktywna. Bez AI informacja przegrywa z dezinformacją. Bez software'u wojsko traci szybkość pętli decyzyjnej. Bez compute gospodarka przegrywa

produktywność. Bez energii każdy system cyfrowy staje się dekoracją. Dlatego TechnoRepublika traktuje technologię jako warstwę wzmacniającą wszystkie klasyczne narzędzia państwa.

Do tego układu należy dodać prawo i regulację jako szósty instrument sterowania. W epoce platform cyfrowych, AI, cyberbezpieczeństwa, surowców krytycznych, kontroli eksportu, ochrony danych, sankcji, zamówień publicznych i polityki przemysłowej prawo nie jest wyłącznie ramą formalną. Jest narzędziem kształtowania rynku, ograniczania zależności, wymuszania standardów bezpieczeństwa, ochrony infrastruktury krytycznej, budowy krajowych zdolności i neutralizacji działań przeciwnika.

W formule TechnoRepubliki:

DIME+T+L = dyplomacja + informacja + wojsko + gospodarka + technologia + prawo/regulacja

Prawo/regulacja jest szczególnie ważne, ponieważ wiele współczesnych konfliktów toczy się poniżej progu wojny: przez przejęcia spółek, zależność od platform, kontrolę danych, eksport technologii, dumping, monopole, sankcje, arbitraż regulacyjny, cybernormy i dostęp do infrastruktury. Państwo, które nie potrafi używać prawa jako instrumentu siły, oddaje pole aktorom zewnętrznym, korporacjom platformowym i przeciwnikom geoeconomicznym.

Dlatego TechnoRepublika nie zarządza bezpieczeństwem wyłącznie przez resorty. Zarządza je przez skoordynowany zestaw instrumentów DIME+T+L, w którym technologia skraca pętlę decyzji, a prawo nadaje decyzjom moc wykonawczą, standardy i trwałość instytucjonalną.

Instrument	Zakres	Miernik strategiczny
Dyplomacja	relacje dodatnie, koalicje zadaniowe, Trójmorze, B9, NATO, UE, partnerstwa globalne	intensywność i trwałość relacji dodatnich, liczba wspólnych projektów, skuteczność negocjacji, pozycja Polski w formatach regionalnych
Informacja	system informacyjny państwa, OSINT, narracja strategiczna, odporność kognitywna, komunikacja kryzysowa	czas detekcji dezinformacji, poziom zaufania społecznego, spójność przekazu państwa, odporność na operacje wpływu
Wojsko	odstraszanie przez odmowę, drony, rakiety, C4ISR, obrona powietrzna, cyber, rezerwy, mobilizacja	koszt agresji dla przeciwnika, gotowość bojowa, zapasy amunicji, czas mobilizacji, zdolność obrony infrastruktury krytycznej
Gospodarka	ekosystemy przemysłowe, kapitał ciepły, eksport, reindustrializacja, zamówienia strategiczne, produkcja dual-use	produktywność, eksport high-tech, udział przemysłu dual-use, MRL/TRL, własność IP, odporność łańcuchów dostaw
Technologia	AI, compute, cloud, quantum, software, data centers, cyber, półprzewodniki, sensory, automatyzacja	suwerenność compute, lokalizacja danych, liczba krajowych platform krytycznych, poziom cyberodporności, zdolność produkcji technologii strategicznych
Prawo / regulacja	ustawy strategiczne, regulacje rynku, kontrola inwestycji, zamówienia publiczne, sankcje, ochrona danych, standardy bezpieczeństwa	czas uchwalenia regulacji, skuteczność egzekucji, redukcja zależności, udział zamówień krajowych, liczba zablokowanych ryzykownych przejęć

Formuła DIME+T+L oznacza, że TechnoRepublika używa pełnego zestawu instrumentów siły: dyplomacji, informacji, wojska, gospodarki, technologii oraz prawa/regulacji. Technologia wzmacnia wszystkie pozostałe instrumenty, a prawo nadaje im moc wykonawczą. Państwo nie może ograniczać się do deklaracji strategicznych; musi sterować relacjami, rynkami, infrastrukturą, danymi i zdolnościami przez mierzalne decyzje, regulacje i wykonanie.

6.1. Sześć suwerennych torów państwa

Tor suwerenności	Minimalny standard
Dane	własne rejestry, przestrzenie danych, ochrona prywatności, standardy dostępu, interoperacyjność
Energia	sterowalne i odporne źródła, magazyny, mikrosieci, atom, OZE, wodór, lokalne bilansowanie
Oprogramowanie	systemy dowodzenia, administracji, zdrowia, energetyki, logistyki i cyberbezpieczeństwa
Produkcja	amunicja, drony, sensory, elektronika, leki krytyczne, magazyny, komponenty, robotyka
Obrona	wojsko, obrona cywilna, rezerwy, samorządy, obywatelskie kompetencje bezpieczeństwa
Decyzja	krótka pętla OODA, prezydenckie centrum strategiczne, agencje i KPI wykonania

Sześć suwerennych torów państwa pokazuje, że bezpieczeństwo TechnoRepubliki nie zależy wyłącznie od wojska. Państwo jest suwerenne dopiero wtedy, gdy samodzielnie kontroluje dane, energię, oprogramowanie, produkcję, obronę i proces decyzji. Utrata któregośkolwiek z tych torów tworzy zależność strategiczną: można mieć formalną niepodległość, ale realnie wykonywać cudze decyzje technologiczne, energetyczne, finansowe lub informacyjne.

Dlatego minimalny standard TechnoRepubliki polega na budowie własnych rejestrów, odpornych źródeł energii, krajowych systemów software, produkcji strategicznej, obywatelskiej obrony oraz krótkiej pętli OODA. Suwerenność nie jest deklaracją polityczną, lecz zdolnością państwa do działania mimo kryzysu, presji zewnętrznej, sabotażu, cyberataku lub wojny.

6.2. Reguła integracji instrumentów

Instrumenty siły nie działają osobno. Dyplomacja bez gospodarki jest prośbą. Wojsko bez produkcji jest zakupem katalogowym. Informacja bez danych jest komentarzem. Technologia bez energii jest prezentacją. Gospodarka bez ochrony informacyjnej staje się zasobem dla cudzych platform. Dlatego strategia wymaga projektowania instrumentów w pakietach, a nie w resortowych silosach.

Każda decyzja strategiczna powinna zawierać minimalny pakiet DIME+T: komunikat dyplomatyczny, zabezpieczenie informacyjne, wariant wojskowy lub ochronny, koszt gospodarczy oraz komponent technologiczny. Dopiero połączenie tych warstw tworzy sprawczość państwa.

Przykład	Pakiet DIME+T+L
Kryzys graniczny	dyplomacja sojusznicza + rozpoznanie informacyjne + mobilność wojskowa + zabezpieczenie logistyki + systemy AI/OSINT
Atak na infrastrukturę	komunikat do sojuszników + narracja dla obywateli + ochrona fizyczna + rezerwy gospodarcze + cyber i sensory
Szantaż energetyczny	koalicje zakupowe + informacja cenowa + ochrona infrastruktury + magazyny i kontrakty + system bilansowania
Presja Big Tech	dyplomacja regulacyjna + komunikacja suwerenności + ochrona danych + rynek dla alternatyw + suwerenna chmura

Tabela pokazuje, że w sytuacjach kryzysowych TechnoRepublika nie może reagować jednym narzędziem państwa. Każdy kryzys wymaga pakietu złożonego z kilku warstw: dyplomatycznej, informacyjnej, wojskowo-ochronnej, gospodarczej i technologicznej. Dopiero ich połączenie tworzy realną zdolność działania.

W przypadku kryzysu granicznego sama dyplomacja nie wystarczy bez rozpoznania, mobilności wojskowej i logistyki. Atak na infrastrukturę wymaga jednocześnie komunikatu do sojuszników, ochrony fizycznej, cyberobrony, rezerw i sensorów. Szantaż energetyczny musi być równoważony przez kontrakty, magazyny, bilansowanie i koalicje zakupowe. Presja Big Tech wymaga nie tylko regulacji, ale także suwerennej chmury, ochrony danych i rynku dla alternatyw.

Sens tabeli jest prosty: państwo sprawcze nie reaguje resortowo, lecz pakietowo. Każda decyzja strategiczna powinna od początku łączyć instrumenty DIME+T, a w docelowej wersji TechnoRepubliki także komponent prawno-regulacyjny jako DIME+T+L.

7. Scenariusze i warianty decyzji

Strategia nie może zakładać jednego przyszłego świata. Jej wartość polega na przygotowaniu wariantów działania, gdy rzeczywistość idzie inaczej niż plan. Dlatego Prezydenckie Centrum Strategiczne prowadzi rejestr założeń krytycznych, wargaming i red teaming. Każdy wariant powinien mieć przypisanego właściciela decyzji, dane wejściowe, próg uruchomienia, wariant komunikacyjny, koszt i miernik skutku.

Tabela porządkuje sześć kluczowych scenariuszy kryzysowych, które powinny być stale monitorowane przez Prezydenckie Centrum Strategiczne TechnoRepubliki. Jej logika jest cybernetyczna: dla każdego scenariusza wskazany jest sygnał ostrzegawczy, czyli moment, w którym system państwa powinien rozpoznać zmianę w otoczeniu, oraz odpowiedź strategiczna, czyli gotowy zestaw działań uruchamianych bez opóźnienia.

Najważniejsze są trzy grupy ryzyk. Pierwsza dotyczy bezpieczeństwa twardego: eskalacji na Wschodzie, kryzysu Bałtyku i osłabienia gwarancji USA. Druga obejmuje odporność infrastrukturalną: energię, surowce, porty, kable, gazociągi i systemy łączności. Trzecia dotyczy wojny informacyjnej i technologicznej: ataku kognitywnego oraz przechwycenia infrastruktury cyfrowej przez platformy, chmurę, modele AI lub prywatnych „bramkarzy danych”.

Scenariusz	Sygnal ostrzegawczy	Odpowiedź strategiczna
S1: Eskalacja wschodnia	presja militarna lub hybrydowa na granicy, Suwałki, Białoruś, Ukraina	wzmocnienie odstraszenia przez odmowę, mobilność wojskowa, narracja jedności, cyberodporność
S2: Kryzys Bałtyku	sabotaż kabli, portów, gazociągów, farm offshore lub systemów łączności	stały monitoring, redundancja, współpraca regionalna, awaryjne trasy komunikacji
S3: Burden-shift USA	zmniejszenie gotowości USA do ponoszenia ciężaru obrony Europy	wzrost produkcji krajowej, europejskie koalicje przemysłowe, większa rola Polski w B9/Trójmorzu
S4: Szok energetyczny lub surowcowy	przerwanie dostaw, wzrost cen, presja na przemysł i gospodarstwa domowe	magazyny, mikrosieci, kontrakty długoterminowe, substytucja, atom/OZE/H2
S5: Atak kognitywny	dezinformacja, podważanie zaufania, polaryzacja, manipulacja pokoleniowa	centrum narracji, szybkie sprostowania, edukacja odporności poznawczej, liderzy lokalni
S6: Przechwycenie infrastruktury cyfrowej	zależność od platform, cloud, modeli AI lub prywatnych bramkarzy danych	suwerenna chmura, regulacja dostępu, open source strategiczny, polskie data spaces
S7: szantaż nuklearny	groźby nuklearne, ćwiczenia strategiczne, rozmieszczenie broni taktycznej na Białorusi/Kaliningradzie, eskalacyjna propaganda	konsultacje NATO, komunikacja strategiczna bez paniki, obrona cywilna, ciągłość dowodzenia, odporność infrastruktury, brak ustępstw pod presją
S8: masowa FIMI/deepfake	falszywe nagrania liderów, spreparowane komunikaty państwa, skoordynowane boty, kampanie wpływu przed wyborami lub kryzysem	szybka weryfikacja źródeł, znakowanie autentycznych komunikatów, centrum kontrdezinformacji, współpraca z mediami i platformami, komunikaty kryzysowe
S9: Blackout / paraliż systemu państwa	awaria energetyczna, cyberatak na sieci, utrata łączności	mikrosieci, zasilanie awaryjne, centra zapasowe, tryb ręczny administracji i priorytet dla infrastruktury krytycznej.
S10: kryzys zdrowotny	epidemia, atak biologiczny, niedobór leków, przeciążenie szpitali, cyberatak na ochronę zdrowia	rezerwy leków i sprzętu, krajowa produkcja krytyczna, cyfrowy monitoring zdrowia, tryb szpitali kryzysowych, koordynacja sanitarna i wojskowa
S11: załamanie łańcucha dostaw	brak chipów, leków, amunicji, paliw, żywności lub komponentów przemysłowych; blokada portów lub transportu	rezerwy 90–180 dni, friend-shoring, produkcja krajowa, zamówienia strategiczne, alternatywne korytarze Trójmorza, substytucja technologiczna
S12: kryzys finansowania obrony	wzrost kosztów zbrojeń, presja budżetowa, ograniczony dostęp do kapitału, opóźnienia kontraktów, ryzyko długu	wieloletni fundusz obronny, obligacje obronne, priorytet produkcji krajowej, wspólne zakupy z sojusznikami, finansowanie UE/NATO, kontrola efektywności wydatków

Tabela pokazuje, że TechnoRepublika nie może działać reaktywnie. Musi mieć przygotowane wcześniej procedury odstraszania, redundancji, komunikacji, produkcji krajowej, suwerenności danych i odporności poznawczej społeczeństwa. W praktyce jest to matryca decyzyjna państwa-regulatora: sygnał → diagnoza → decyzja → działanie → sprzężenie zwrotne.

7.1. Rejestr założeń krytycznych

Założenie	Czujnik	Wariant awaryjny
USA utrzymają wiarygodne zaangażowanie w Europie	decyzje budżetowe, posture, rozmieszczenia, wypowiedzi NSS, priorytet Indo-Pacific	przyspieszyć europejsko-polskie zdolności i produkcję
Rosja pozostanie głównym wektorem zagrożenia	mobilizacja, produkcja zbrojeniowa, aktywność Białorusi, sabotaż w Europie	zwiększać odporność i odstraszanie przez odmowę
UE będzie zdolna do szybkiej polityki przemysłowej	tempo zamówień, regulacje, finansowanie obronności i energii	tworzyć koalicje projektowe poza najwolniejszym wspólnym mianownikiem
AI zwiększy zdolność decyzyjną państwa	jakość danych, cyberbezpieczeństwo, audyty, kompetencje kadr	utrzymać human-in-command i audyt modeli
Spółeczeństwo zaakceptuje koszt odporności	sondaże, inflacja, energia, poziom zaufania	komunikować kontrakt sprawczości i korzyści lokalne

Tabela przedstawia skróconą wersję rejestru założeń krytycznych, ograniczoną ze względu na objętość miejsca w dokumencie. W pełnej wersji operacyjnej każde założenie powinno posiadać osobną kartę kontroli strategicznej obejmującą: właściciela założenia, datę przeglądu, wskaźnik obalenia, test red-team, wariant awaryjny oraz decyzję aktualizacyjną.

Oznacza to, że założenia nie mogą być traktowane jako stałe przekonania strategiczne. Każde z nich musi być okresowo testowane, podważane i aktualizowane. Jeżeli pojawi się wskaźnik obalenia — na przykład zmiana postawy USA, eskalacja rosyjska, nieskuteczność UE, zawodność AI albo spadek akceptacji społecznej — państwo powinno uruchomić wariant awaryjny i podjąć formalną decyzję aktualizacyjną. Celem rejestru jest ochrona strategii przed błędem założeń, czyli sytuacją, w której państwo działa według modelu świata, który przestał być prawdziwy.

Rejestr założeń krytycznych jest jednym z podstawowych narzędzi sterowania strategicznego TechnoRepubliki. Jego celem jest stałe sprawdzanie, czy najważniejsze założenia strategii nadal odpowiadają rzeczywistości. Państwo nie może opierać bezpieczeństwa na deklaracjach, nadziejach ani raz przyjętych scenariuszach. Musi stale obserwować otoczenie, wykrywać sygnały ostrzegawcze i przygotowywać warianty awaryjne, zanim kryzys wymusi chaotyczną reakcję.

Założenia krytyczne:

- Pierwszym założeniem jest utrzymanie wiarygodnego zaangażowania USA w Europie. Należy monitorować decyzje budżetowe, rozmieszczenie wojsk, wypowiedzi strategiczne oraz przesuwanie priorytetów USA w stronę Indo-Pacific. W razie osłabienia gwarancji transatlantyckich Polska powinna przyspieszyć budowę własnych i europejskich zdolności obronnych oraz produkcyjnych.
- Drugie założenie dotyczy Rosji jako głównego wektora zagrożenia. Czujnikami są mobilizacja, produkcja zbrojeniowa, aktywność Białorusi i sabotaż w Europie. Odpowiedzią musi być zwiększanie odporności państwa, fortyfikacja, mobilność wojskowa i odstraszanie przez odmowę.
- Trzecie założenie odnosi się do zdolności UE do szybkiej polityki przemysłowej. Ponieważ Unia może działać wolno, TechnoRepublika powinna budować koalicje projektowe poza najwolniejszym wspólnym mianownikiem.
- Czwarte założenie dotyczy AI jako narzędzia wzmacniającego decyzje państwa. Warunkiem jest jakość danych, cyberbezpieczeństwo, audyt modeli i zasada human-in-command.
- Piąte założenie dotyczy akceptacji społecznej kosztów odporności. Państwo musi komunikować obywatelom kontrakt sprawczości: koszty bezpieczeństwa, energii i suwerenności cyfrowej muszą być powiązane z lokalnymi korzyściami, miejscami pracy, stabilnością i realną podmiotowością.

Rejestr założeń krytycznych jest więc mechanizmem antynaiwności strategicznej:

- pozwala państwu obserwować,
- porównywać,
- korygować
- działać z wyprzedzeniem.

Aneks A1. Słownik Tomu 1

Wspólny język strategii ogólnej i Mapy Oddziaływań Geopolitycznych

Słownik obejmuje terminy używane w Tomie 1. Pojęcia wdrożeniowe, sektorowe i legislacyjne rozwijane w rozdziałach 8–14 przypisano do słownika Tomu 2.

Zasada redakcyjna: wykaz obejmuje skróty, akronimy, oznaczenia złożone i symbole istotne dla zrozumienia strategii. Pominięto skróty oraz znaki oczywiste, redakcyjne i niewnoszące treści merytorycznej. Rozwinięcia angielskie podano wraz z polskim objaśnieniem.

A.1. Skróty, akronimy, symbole i oznaczenia Tomu 1

Nr	Skrót / symbol	Rozwinięcie	Znaczenie w dokumencie
1	A/B/C	warianty decyzyjne A, B i C	Zapis alternatywnych sposobów działania przygotowanych przed decyzją albo kryzysem.
2	A2AD	Anti-Access/Area Denial - blokowanie dostępu i swobody działania	Zestaw zdolności raketowych, przeciwlotniczych, elektronicznych, cybernetycznych, minowych i rozpoznawczych utrudniających przeciwnikowi wejście do obszaru i operowanie w nim.
3	AI	Artificial Intelligence - sztuczna inteligencja	Systemy wspierające analizę danych, wykrywanie ryzyk, symulacje i rekomendacje. W strategii nie przejmują odpowiedzialności konstytucyjnej człowieka.
4	AIS	Automatic Identification System - automatyczny system identyfikacji statków	Źródło danych o ruchu jednostek morskich; jego zakłócanie może ograniczać bezpieczeństwo żeglugi i świadomość sytuacyjną.
5	B9	Bucharest Nine - Bukaresztańska Dziewiątka	Format współpracy państw wschodniej flanki NATO, istotny dla planowania regionalnego, infrastruktury i wspólnego stanowiska bezpieczeństwa.
6	C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance	Zintegrowany system dowodzenia, łączności, informatyki, wywiadu, obserwacji i rozpoznania zapewniający wspólny obraz sytuacji i szybką decyzję.
7	CERT	Computer Emergency Response Team - zespół reagowania na incydenty komputerowe	Jednostka wykrywająca, analizująca i koordynująca reakcję na incydenty cyberbezpieczeństwa.
8	DIME	Diplomatic, Informational, Military, Economic	Klasyczne instrumenty siły państwa: dyplomacja, informacja, wojsko i gospodarka.
9	DIME+T	DIME rozszerzone o Technology	Model instrumentów siły uzupełniony o technologię jako mnożnik zdolności państwa.
10	DIME+T+L	DIME rozszerzone o Technology oraz Law/Regulation	Pełna formuła strategii: dyplomacja, informacja, wojsko, gospodarka, technologia oraz prawo i regulacja.

Nr	Skrót / symbol	Rozwinięcie	Znaczenie w dokumencie
11	E_l(t)	zbiór relacji w warstwie l i czasie t	Skierowane krawędzie grafu MOG opisujące oddziaływania między węzłami.
12	FIMI	Foreign Information Manipulation and Interference	Zagraniczna manipulacja informacyjna i ingerencja wymierzona w debatę publiczną, wybory, zaufanie i percepcję społeczną.
13	G_MOG(t)	graf MOG w czasie t	Formalny zapis całej mapy: zbioru węzłów V oraz krawędzi E _l (t) w poszczególnych warstwach.
14	GPS	Global Positioning System	Satelitarny system pozycjonowania wykorzystywany w transporcie, logistyce, synchronizacji czasu i działaniach wojskowych.
15	H₂	wodór - zapis chemiczny cząsteczki wodoru	Nośnik energii i surowiec przemysłowy rozpatrywany w kontekście OZE, magazynowania, bezpieczeństwa energetycznego i nowych łańcuchów wartości.
16	IP	Intellectual Property - własność intelektualna	Prawa do technologii, oprogramowania, wynalazków i know-how; ich krajowa kontrola jest miernikiem suwerenności gospodarczej.
17	KPI	Key Performance Indicator - kluczowy wskaźnik wykonania lub wyniku	Miernik postępu i rezultatu. W strategii musi mieć definicję, źródło danych, właściciela, częstotliwość aktualizacji i progi reakcji.
18	LNG	Liquefied Natural Gas - skroplony gaz ziemny	Paliwo transportowane drogą morską; terminale LNG są elementem dywersyfikacji i infrastruktury krytycznej.
19	MOG	Mapa Oddziaływań Geopolitycznych	Model geopolityki jako dynamicznego, skierowanego i wielowarstwowego grafu relacji.
20	MRL	Manufacturing Readiness Level - poziom gotowości produkcyjnej	Skala oceniająca, czy technologia może być wytwarzana stabilnie, jakościowo i w wymaganej skali.
21	NATO	North Atlantic Treaty Organization - Organizacja Traktatu Północnoatlantyckiego	Sojusz obronny stanowiący podstawowy format bezpieczeństwa militarnego Polski.
22	NSS	National Security Strategy - Strategia Bezpieczeństwa Narodowego	Nazwa klasy dokumentów porządkujących interes narodowy, środowisko strategiczne, instrumenty siły i warianty odpowiedzi.
23	OODA	Observe, Orient, Decide, Act - obserwuj, orientuj, decyduj, działaj	Pętla decyzyjna służąca skracaniu czasu od sygnału do wykonania i uczenia się państwa.
24	OPL	obrona przeciwlotnicza	Zdolności wykrywania i zwalczania zagrożeń powietrznych, będące częścią obrony warstwowej i przeciwdziałania A2AD.
25	OSINT	Open-Source Intelligence - rozpoznanie z jawnych źródeł	Analiza mediów, rejestrów, internetu, danych publicznych i zobrazowań dostępnych bez działań niejawnych.

Nr	Skrót / symbol	Rozwinięcie	Znaczenie w dokumencie
26	OZE	odnawialne źródła energii	Źródła takie jak wiatr, słońce, woda, biomasa i geotermia, rozpatrywane jako element miksu, lokalnego bilansowania i odporności.
27	PCS	Prezydenckie Centrum Strategiczne	Projektowane centrum integracji poznawczej i strategicznej: utrzymuje mapę ryzyk, scenariusze, KPI, red team i audyt wykonania.
28	PR	Public Relations - relacje publiczne	Komunikacja wizerunkowa; dokument odróżnia ją od strategicznej ochrony narracji i odporności informacyjnej.
29	R	ryzyko	Wartość wynikająca z prawdopodobieństwa, ekspozycji, podatności, konsekwencji i zabezpieczeń.
30	S	dotkliwość pojedynczego oddziaływania	Parametr skutku pojedynczego zdarzenia, odrębny od częstotliwości i gwałtowności.
31	S1-S12	oznaczenia dwunastu scenariuszy strategicznych	System identyfikatorów scenariuszy używany do powiązania sygnałów ostrzegawczych z przygotowanymi odpowiedziami.
32	SG	Straż Graniczna	Formacja odpowiedzialna za ochronę granicy i kontrolę ruchu granicznego; źródło danych i wykonawca w scenariuszach presji granicznej.
33	TRL	Technology Readiness Level - poziom gotowości technologicznej	Skala dojrzałości technologii od koncepcji i badań do demonstracji oraz wdrożenia operacyjnego.
34	UAS	Unmanned Aircraft System - bezzałogowy system powietrzny	Dron wraz z wyposażeniem, łącznością, stacją kontroli i elementami wsparcia.
35	UE	Unia Europejska	Wspólnota polityczna, prawna i gospodarcza będąca jednym z głównych środowisk regulacyjnych i strategicznych Polski.
36	USA	United States of America - Stany Zjednoczone Ameryki	Kluczowy sojusznik Polski w NATO, którego zmieniające się priorytety są traktowane jako założenie wymagające stałego testowania.
37	V	zbiór węzłów	Aktorzy i zasoby strategiczne w grafie MOG; podatność jest oznaczana odrębnie jako V _p .
38	Δt	okno czasu	Przedział, dla którego agreguje się zdarzenia i wyznacza zmianę parametrów.
39	λ	częstotliwość zdarzeń	Liczba oddziaływań w jednostce czasu w zdefiniowanym oknie obserwacji.
40	Π	priorytet decyzyjny	Ważony indeks służący kolejności decyzji; nie jest iloczynem nieporównywalnych wielkości.

A.2. Mapa Oddziaływań Geopolitycznych – pojęcia i zmienne

Nr	Pojęcie / zmienna	Definicja operacyjna
1	Aktor / węzeł V	Państwo, organizacja, korporacja, platforma, infrastruktura lub zasób strategiczny reprezentowany jako węzeł grafu MOG.
2	Częstotliwość λ	Liczba oddziaływań w jednostce czasu. Powinna być estymowana w określonym oknie Δt , z podaniem źródła danych i niepewności.
3	Dotkliwość oddziaływania S	Skala skutku pojedynczego zdarzenia. Model bazowy: $S = Z \times U \times E_f$, gdzie Z oznacza zdolność aktora, U – stopień jej użycia, a E_f – skuteczność wobec danego celu.
4	Ekspozycja X	Stopień, w jakim Polska, jej ludność, zasoby lub infrastruktura znajdują się w zasięgu danego oddziaływania.
5	Gwałtowność G	Szybkość narastania presji, a nie jej wielkość. Może być opisana jako $G = 1/(T_n + \varepsilon)$, gdzie T_n jest czasem narastania, a ε zapobiega dzieleniu przez zero.
6	Intencja / wrogość H	Ocena zamiaru aktora. Jest przesłanką estymacji prawdopodobieństwa zdarzenia, lecz nie stanowi samodzielnego mnożnika ryzyka.
7	Intensywność presji I	Skumulowana dotkliwość oddziaływań w czasie. Dla procesu zdarzeń można przyjąć $E[I] \approx \lambda \times E[S]$; termin zastępuje niejednoznaczne określenie „moc nacisku”.
8	Kierunek relacji	Wskazanie źródła i odbiorcy oddziaływania; relacja $A \rightarrow B$ nie jest automatycznie równoważna relacji $B \rightarrow A$.
9	Konsekwencje C	Wielkość możliwej szkody dla interesu narodowego, ludności, ciągłości decyzji, gospodarki, infrastruktury lub pozycji międzynarodowej.
10	Krawędź $E_l(t)$	Skierowana relacja między węzłami w warstwie l i czasie t, opisana zestawem zmiennych, źródłem danych oraz poziomem niepewności.
11	Krytyczność / brak substytutu K	Znaczenie zagrożonego zasobu lub funkcji oraz trudność ich zastąpienia w wymaganym czasie.
12	Luka gotowości L	Różnica między zdolnością potrzebną do odpowiedzi a zdolnością faktycznie dostępną w wymaganym czasie.
13	Mapa Oddziaływań Geopolitycznych (MOG)	Dynamiczny, skierowany, ważony i wielowarstwowy graf relacji geopolitycznych $G_{MOG}(t) = \{V, E_1(t), \dots, E_L(t)\}$.
14	Niepewność N	Miara braku pewności co do danych, parametrów lub modelu; powinna być prezentowana jako przedział, rozkład lub klasa jakości, a nie ukrywana w ocenie punktowej.
15	Normalizacja	Przekształcenie zmiennych o różnych jednostkach i skalach do porównywalnej postaci przed agregacją; parametry normalizacji muszą być jawne i testowane.
16	Okno czasu Δt	Jawnie określony przedział obserwacji, dla którego liczy się częstotliwość, intensywność, ryzyko i zmianę trendu.
17	Pilność U_p	Relacja czasu potrzebnego do przygotowania reakcji do czasu dostępnego przed materializacją skutku; rośnie wraz z kurczeniem się marginesu decyzji.

Nr	Pojęcie / zmienna	Definicja operacyjna
18	Podatność V_p	Wewnętrzna skłonność systemu do poniesienia szkody po wystąpieniu zdarzenia. Symbol V_p odróżnia podatność od zbioru węzłów V .
19	Prawdopodobieństwo q	Warunkowe prawdopodobieństwo zdarzenia w określonym horyzoncie, szacowane na podstawie danych, intencji, zdolności i kontekstu.
20	Priorytet decyzyjny Π	Ważony indeks ryzyka, pilności, krytyczności i luki gotowości: $\Pi = w_{RR} + w_{UU_p} + w_{KK} + w_{LL}$. Wagi muszą wynikać z jawnej polityki decyzyjnej.
21	Pętla decyzyjna	Sekwencja: sygnał → aktualizacja MOG → ocena ryzyka i priorytetu → warianty → decyzja → wykonanie → pomiar skutku → korekta modelu.
22	Relacja dodatnia	Relacja zwiększająca bezpieczeństwo, zdolności lub autonomię stron; jej pomiar obejmuje intensywność, trwałość, wzajemność i zastępowalność.
23	Ryzyko R	Oczekiwana dotkliwość szkody. Model bazowy: $R = q \times X \times V_p \times C \times (1 - M)$, gdzie M oznacza skuteczność zabezpieczeń w skali 0–1.
24	Ryzyko rezydualne	Ryzyko pozostające po uwzględnieniu istniejących zabezpieczeń i działań ograniczających.
25	Skuteczność zabezpieczeń M	Stopień redukcji ryzyka przez odporność, redundancję, ochronę i przygotowane reakcje; M należy kalibrować na danych testowych i zdarzeniach.
26	Walidacja modelu	Sprawdzenie modelu na danych historycznych, scenariuszach i nowych obserwacjach, obejmujące analizę wrażliwości, testy błędów oraz porównanie z modelami alternatywnymi.
27	Wariant reakcji a	Konkretny pakiet działań DIME+T+L oceniany pod względem czasu, kosztu, legalności, wykonalności, skutku i ryzyka ubocznego.
28	Warstwa l	Domena relacji, np. militarna, gospodarcza, informacyjna, energetyczna, technologiczna, logistyczna, zdrowotna lub dyplomatyczna.
29	Wektor relacji	Łączny opis kierunku, znaku, warstwy i parametrów oddziaływania; nie jest fizycznym wektorem, dopóki nie określono przestrzeni, skali i reguł agregacji.
30	Znak relacji	Klasyfikacja funkcji relacji jako wzmacniającej, neutralnej, konkurencyjnej lub szkodliwej; znak może zmieniać się w czasie i między warstwami.

A.3. Interes narodowy, geopolityka i pozycja Polski

Nr	Pojęcie	Definicja operacyjna
1	Aktor geopolityczny	Państwo, organizacja międzynarodowa, korporacja, platforma lub sieć posiadająca zasoby i zdolność wpływania na bezpieczeństwo, decyzje albo zależności innych podmiotów.
2	Aktor niepaństwowy	Podmiot spoza administracji państwa - np. korporacja technologiczna, fundusz, organizacja społeczna lub grupa zbrojna - który może wywierać realny wpływ strategiczny.

Nr	Pojęcie	Definicja operacyjna
3	Bezpieczeństwo narodowe	Zdolność ochrony państwa, ludności, terytorium, ciągłości decyzji i podstaw rozwoju przed zagrożeniami militarnymi oraz niemilitarnymi.
4	Centralność Polski	Pozycja Polski w sieci przepływów bezpieczeństwa, energii, logistyki, danych, handlu i sojuszy; rośnie, gdy inni muszą uwzględniać polski węzeł.
5	Chokepoint	Wąskie gardło infrastrukturalne, technologiczne, surowcowe lub regulacyjne, którego kontrola pozwala ograniczać przepływ i wywierać presję na inne podmioty.
6	De-risking	Ograniczanie ryzyka nadmiernej zależności przez dywersyfikację, zapasy, własne zdolności i wiarygodnych partnerów, bez pełnego zerwania współpracy.
7	Dobrobyt technologiczny	Dobrobyt oparty na produktywności, własności technologii, kompetencjach, eksporcie i zdolności wytwarzania, a nie wyłącznie na konsumpcji cudzych rozwiązań.
8	Fragmentacja geoeconomiczna	Podział handlu, kapitału, technologii i łańcuchów dostaw według bloków politycznych oraz kryteriów bezpieczeństwa.
9	Friend-shoring	Lokowanie krytycznych dostaw i produkcji w państwach politycznie wiarygodnych, aby ograniczyć ryzyko szantażu lub nagłego przerwania dostępu.
10	Geoekonomia	Używanie handlu, inwestycji, sankcji, technologii, surowców, energii i regulacji jako instrumentów rywalizacji oraz siły państwa.
11	Geopolityka	Analiza wpływu położenia, przestrzeni, zasobów, relacji i infrastruktury na cele, możliwości oraz ograniczenia państw.
12	Głębia strategiczna	Przestrzeń, infrastruktura, zasoby i relacje umożliwiające absorpcję uderzenia, manewr, odtworzenie zdolności i podtrzymanie operacji.
13	Interes narodowy	Hierarchia trwałych celów Polski: przetrwanie, suwerenność sterowania, odporność społeczna, dobrobyt technologiczny oraz pozycja i wpływ.
14	Kapitał narracyjny	Wiarygodność opowieści państwa o własnej roli i celu, która pomaga budować zaufanie obywateli, sojusze, inwestycje i przyciąganie talentów.
15	Konflikt ukryty	Relacja formalnie pokojowa, w której presja jest prowadzona poprzez informację, kapitał, regulację, technologie, pośredników lub zależności gospodarcze.
16	Kooperacja misyjna	Współpraca państw lub instytucji zorganizowana wokół wspólnego, mierzalnego celu strategicznego i podziału odpowiedzialności.
17	Nacisk jednostronny	Relacja, w której jeden aktor może szkodzić drugiemu lub wymuszać ustępstwa bez ponoszenia proporcjonalnego kosztu.
18	Niezbędność strategiczna	Stopień, w jakim sojusznicy i partnerzy nie mogą łatwo zastąpić wkładu Polski w bezpieczeństwo, logistykę, energię, dane lub produkcję.
19	Państwo centralne Europy	Model Polski jako organizatora przepływów i zdolności Europy Środkowej, a nie wyłącznie odbiorcy decyzji zewnętrznych lub bufora geopolitycznego.

Nr	Pojęcie	Definicja operacyjna
20	Państwo frontowe	Państwo bezpośrednio narażone na presję i konflikt na granicy systemu sojuszniczego; jego bezpieczeństwo zależy od własnej odporności i szybkości wsparcia.
21	Pozycja i wpływ	Zdolność Polski do kształtowania decyzji, standardów i koalicji dzięki wiarygodności, zdolnościom własnym oraz centralności w sieciach relacji.
22	Renta geostrategiczna	Korzyść polityczna, gospodarcza lub bezpieczeństwa uzyskiwana dzięki położeniu i niezbędności Polski dla regionu.
23	Substytucja strategiczna	Zastąpienie krytycznego dostawcy, technologii, trasy lub zasobu rozwiązaniem alternatywnym w celu ograniczenia nacisku.
24	Teatr oddziaływań	Geograficzna lub funkcjonalna przestrzeń rywalizacji, np. Wschód, Bałtyk, cyberprzestrzeń, energia, zdrowie albo łańcuchy dostaw.
25	Trójmorze	Format współpracy państw między Bałtykiem, Adriatykiem i Morzem Czarnym; w strategii ma tworzyć regionalny korytarz odporności i mobilności.
26	Wielobiegunowość	Ład, w którym wiele mocarstw i ośrodków gospodarczych prowadzi selektywną, transakcyjną politykę bez jednego dominującego centrum.
27	Współzależność uzbrojona	Wykorzystanie kontroli nad węzłami sieci gospodarczych, finansowych, cyfrowych lub logistycznych do monitorowania, ograniczania albo karania innych aktorów.
28	Zależność asymetryczna	Współzależność, w której jedna strona ponosi znacznie większy koszt zerwania relacji i dlatego jest bardziej podatna na nacisk.
29	Środowisko strategiczne	Dynamiczny układ państw, organizacji, rynków, technologii, zagrożeń i zależności, w którym Polska podejmuje decyzje bezpieczeństwa.

A.4. Cybernetyka państwa, decyzje i rozliczalność

Nr	Pojęcie	Definicja operacyjna
1	Architektura decyzji	Układ ról, informacji, progów, wariantów, kompetencji i ścieżek wykonania określający, jak państwo przechodzi od sygnału do wyniku.
2	Audyt wykonania	Niezależne sprawdzenie, czy decyzja została zrealizowana, jakie przyniosła skutki, koszty i odchylenia oraz kto za nie odpowiada.
3	Cybernetyka rządzenia	Projektowanie państwa jako regulatora: z celem, modelem rzeczywistości, informacją zwrotną, repertuarem działań i zdolnością uczenia się.
4	Czujnik strategiczny	Źródło danych lub wskaźnik wykrywający zmianę otoczenia, wzrost podatności albo zbliżanie się do progu alarmowego.
5	Informacja sterownicza	Aktualna i wiarygodna informacja o stanie systemu, odchyleniu, ryzyku i wyniku, która może uruchomić konkretną decyzję.
6	Integracja decyzyjna	Łączenie danych, ocen i wariantów różnych instytucji w jeden obraz sytuacji bez nieuprawnionego przejmowania ich kompetencji.
7	Karta decyzji strategicznej	Ustandaryzowany zapis problemu, interesu narodowego, podmiotów, mierników, wariantów, właściciela wyniku i zasad kontroli.

Nr	Pojęcie	Definicja operacyjna
8	Klauzula legalnej transformacji	Zasada prowadzenia zmian kolejno w ramach obecnych kompetencji, ustaw i - gdy jest to konieczne - legalnej zmiany konstytucji.
9	Kontrola demokratyczna	Mechanizmy jawności, parlamentu, sądów, audytu i udziału obywateli ograniczające arbitralność centrum decyzyjnego.
10	Metasystem państwa	Warstwa utrzymująca wspólny model sytuacji, mierniki i reguły koordynacji wielu resortów oraz agencji, bez zastępowania ich wykonania.
11	Model systemu	Uproszczona, jawna reprezentacja aktorów, zależności, zasobów, progów i mechanizmów, na której państwo opiera diagnozę oraz decyzje.
12	Państwo-regulator	Państwo posiadające model własnego systemu, mierzące odchylenia, uruchamiające wykonanie, kontrolujące wynik i uczące się z informacji zwrotnej.
13	Prezydenckie Centrum Strategiczne	Projektowane centrum analityczno-koordynacyjne i docelowy metasystem sterowania strategicznego, podporządkowany legalnym zasadom ustrojowym.
14	Protokół decyzji strategicznej	Jednolity proces obejmujący sygnał, klasyfikację, mapę relacji, warianty, red team, decyzję, wykonanie, audyt i aktualizację modelu.
15	Próg krytyczny	Poziom wskaźnika, po którego przekroczeniu uruchamiany jest tryb kryzysowy, wariant awaryjny albo eskalacja do wyższego decydenta.
16	Próg ostrzegawczy	Poziom wskaźnika sygnalizujący pogorszenie sytuacji i potrzebę pogłębionej analizy lub działania zapobiegawczego.
17	Pulpit KPI państwa	Zestaw mierników z przypisanymi źródłami, właścicielami i progami reakcji, służący bieżącemu monitorowaniu wykonania strategii.
18	Pętla OODA państwa	Zastosowanie cyklu obserwacji, orientacji, decyzji i działania do administracji, obrony, gospodarki i reagowania kryzysowego.
19	Red teaming	Kontrolowane podważanie założeń, planów i systemów przez zespół symulujący przeciwnika, awarię lub próbę obejścia reguł.
20	Rejestr założeń krytycznych	Okresowo testowana lista warunków, od których zależy poprawność strategii, wraz z czujnikami obalenia i wariantami awaryjnymi.
21	Rozliczalność	Możliwość wskazania, kto odpowiada za cel, dane, decyzję, wykonanie i wynik oraz jakie konsekwencje uruchamia odchylenie.
22	Scenariusz strategiczny	Spójny opis możliwego rozwoju sytuacji, sygnałów ostrzegawczych, skutków, decyzji i potrzebnych zasobów.
23	Sprzężenie zwrotne	Powrót informacji o skutkach działania do regulatora i obywateli, umożliwiający potwierdzenie wyniku lub korektę.
24	Sterowność	Zdolność państwa do utrzymania celów, podejmowania decyzji i uzyskiwania wyników mimo zakłóceń oraz presji zewnętrznej.
25	Wargaming	Symulowanie konfliktów i kryzysów w celu sprawdzenia zachowań aktorów, wariantów decyzji, ograniczeń i skutków ubocznych.
26	Wariant awaryjny	Przygotowana wcześniej odpowiedź uruchamiana po przekroczeniu progu, obaleniu założenia lub utracie podstawowego sposobu działania.
27	Właściciel wyniku	Jednoznacznie wskazana osoba lub instytucja odpowiadająca za rezultat, zasoby, termin, jakość danych i reakcję na odchylenie.

Nr	Pojęcie	Definicja operacyjna
28	Założenie krytyczne	Twierdzenie o otoczeniu lub własnych zdolnościach, którego fałszywość może unieważnić plan i wymaga stałego monitorowania.

A.5. Obrona, odstraszanie i współdziałanie sojusznicze

Nr	Pojęcie	Definicja operacyjna
1	Bezpieczeństwo Bałtyku	Ochrona portów, kabli, gazociągów, energetyki offshore, żeglugi, dna morskiego i zdolności sojuszniczych na Morzu Bałtyckim.
2	Burden-sharing	Podział kosztów i zadań obronnych między sojuszników, obejmujący wydatki, siły, infrastrukturę, produkcję i gotowość.
3	Burden-shifting	Przesuwanie większej części odpowiedzialności i kosztów obrony na innych sojuszników; w strategii jest sygnałem do budowy zdolności własnych.
4	Ciągłość działania władz	Zdolność konstytucyjnych organów państwa do podejmowania i wykonywania decyzji podczas wojny, blackoutu, cyberataku lub paraliżu administracji.
5	Dowodzenie przez misję	Model, w którym przełożony określa cel i zamiar, a wykonawca dobiera środki stosownie do zmiennej sytuacji i dostępnych zasobów.
6	Drone wall	Warstwowy system sensorów, zakłócania, bezzatłogowców, efektorów i procedur służący ochronie granicy oraz infrastruktury przed dronami.
7	Infrastruktura dual-use	Obiekt lub system projektowany do zastosowań cywilnych i wojskowych, np. droga, kolej, port, sieć łączności lub energetyka.
8	Infrastruktura krytyczna	Systemy i obiekty niezbędne do funkcjonowania państwa, gospodarki i ludności, których zakłócenie może wywołać poważne skutki.
9	Interoperacyjność sojusznicza	Zdolność sił, procedur, danych, łączności i infrastruktury różnych państw do wspólnego działania.
10	Kill chain	Sekwencja wykrycia, identyfikacji, decyzji, wskazania i rażenia celu; jej szybkość i odporność wpływają na przewagę operacyjną.
11	Kill web	Sieciowa organizacja sensorów, dowództwa, efektorów, AI i operatorów, w której wiele elementów może elastycznie tworzyć ścieżkę działania.
12	Mobilizacja	Przejęcie państwa, sił zbrojnych, gospodarki i społeczeństwa z trybu pokojowego do zwiększonej gotowości i wykonania zadań obronnych.
13	Mobilność wojskowa	Zdolność szybkiego przemieszczania sił, sprzętu i zaopatrzenia dzięki drogom, kolei, portom, mostom, procedurom i priorytetom ruchu.
14	Obrona cywilna	System ochrony ludności, ratownictwa, schronienia, ewakuacji, ostrzegania, ciągłości usług i przygotowania obywateli na kryzys oraz wojnę.
15	Obrona totalna	Model łączący siły zbrojne, administrację, przemysł, infrastrukturę, gospodarkę i przygotowane społeczeństwo w jeden system odporności.
16	Obrona warstwowa	Układ wielu uzupełniających się warstw wykrywania, ochrony i zwalczania, utrudniający przeciwnikowi przełamanie systemu jednym środkiem.

Nr	Pojęcie	Definicja operacyjna
17	Odporność jako odstraszanie	Zdolność przetrwania ataku i szybkiego odtworzenia funkcji, która obniża oczekiwane korzyści przeciwnika.
18	Odstraszanie	Wpływanie na kalkulację przeciwnika tak, aby uznał agresję za nieskuteczną, zbyt kosztowną lub politycznie nieopłacalną.
19	Odstraszanie przez karę	Zapowiedź i zdolność nałożenia po agresji kosztu większego niż możliwa korzyść przeciwnika.
20	Odstraszanie przez odmowę	Przekonanie przeciwnika, że nie osiągnie celu, ponieważ państwo ma obronę, redundancję i zdolność dalszego działania.
21	Operacja hybrydowa	Skoordynowane użycie środków militarnych i niemilitarnych poniżej albo wokół progu wojny: cyberataków, dezinformacji, sabotażu, migracji i presji ekonomicznej.
22	Operacja podprogowa	Wrogie działanie celowo utrzymywane poniżej poziomu, który automatycznie wywołałby pełną odpowiedź wojskową lub sojuszniczą.
23	Presja nuklearna	Wykorzystywanie arsenału, gróźb, ćwiczeń i narracji nuklearnej do zastraszania, ograniczania decyzji lub rozbijania spójności sojuszu.
24	Produkcja jako odstraszanie	Zdolność szybkiego uzupełniania amunicji, dronów, sensorów, części i uzbrojenia, która pokazuje przeciwnikowi trwałość potencjału obronnego.
25	Przesmyk suwalski	Obszar łączący Polskę z Litwą i pozostałymi państwami bałtyckimi, kluczowy dla spójności terytorialnej NATO na wschodniej flance.
26	Redundancja	Celowe utrzymywanie zapasowych tras, systemów, źródeł, personelu lub procedur, aby pojedyncza awaria nie przerwała funkcji krytycznej.
27	Rezerwy strategiczne	Zapasy paliw, leków, żywności, amunicji, komponentów i innych zasobów podtrzymujących działanie podczas przerwania dostaw.
28	Sabotaż	Celowe uszkodzenie infrastruktury, produkcji, danych lub procesów w celu obniżenia zdolności państwa bez otwartego starcia militarnego.
29	Teatr wschodni	Obszar zagrożeń i działań obejmujący Rosję, Białoruś, Ukrainę, Litwę, przesmyk suwalski i infrastrukturę przygraniczną.
30	Wiarygodność sojusznicza	Przekonanie partnerów, że Polska spełni zobowiązania, posiada realne zdolności i może zapewnić wkład potrzebny do wspólnego działania.
31	Wschodnia flank NATO	Państwa i obszary sojuszu bezpośrednio narażone na presję ze wschodu, wymagające wysuniętej obrony, mobilności i wzmocnienia.
32	Świadomość sytuacyjna	Aktualny i wspólny obraz zdarzeń, aktorów, zasobów i ryzyk umożliwiający właściwą orientację oraz koordynację decyzji.

A.6. Technologie, geoeconomia i odporność systemowa

Nr	Pojęcie	Definicja operacyjna
1	AI governance	Zasady, role, rejestry, audyty i zabezpieczenia określające, w jaki sposób państwo projektuje, kupuje, używa i kontroluje systemy AI.
2	Bezpieczeństwo ekonomiczne	Zdolność gospodarki i państwa do utrzymania kluczowych funkcji, finansowania i produkcji mimo presji, szoków oraz przerwania dostaw.

Nr	Pojęcie	Definicja operacyjna
3	Bezpieczeństwo energetyczne	Zapewnienie energii o wymaganej jakości, cenie i ciągłości dla obywateli, przemysłu, obrony i usług krytycznych.
4	Bezpieczeństwo przemysłowe	Kontrola zdolności projektowania, wytwarzania, serwisowania i skalowania produktów krytycznych dla państwa.
5	Black start	Zdolność uruchomienia elektrowni lub części systemu elektroenergetycznego bez zasilania zewnętrznego po rozległej awarii.
6	Blackout	Rozległa utrata zasilania mogąca wywołać efekt łańcuchowy w łączności, zdrowiu, transporcie, wodzie, administracji i bezpieczeństwie.
7	Bramkarz danych	Podmiot kontrolujący dostęp do kluczowych zbiorów, modeli, platform lub interfejsów i mogący narzucać warunki państwu albo użytkownikom.
8	Chmura suwerenna	Środowisko obliczeniowe, nad którym państwo zachowuje kontrolę prawną, operacyjną, kryptograficzną, serwisową i możliwość migracji.
9	Compute	Moc obliczeniowa, układy, centra danych i energia potrzebne do trenowania, uruchamiania oraz kontrolowania modeli AI.
10	Cyberatak	Celowe działanie przeciw poufności, integralności lub dostępności systemów i danych, służące kradzieży, zakłóceniu, manipulacji albo paraliżowi.
11	Cyberbezpieczeństwo	Zespół środków prawnych, organizacyjnych i technicznych chroniących systemy, sieci, dane oraz ciągłość usług cyfrowych.
12	Cyberodporność	Zdolność systemu do zapobiegania incydentom, wykrywania ich, utrzymywania funkcji, ograniczania szkody i bezpiecznego odtworzenia.
13	Dane jako infrastruktura suwerenności	Zasada uznająca krytyczne dane za zasób równie ważny jak energia, transport i łączność, wymagający kontroli, jakości i ochrony.
14	Dezinformacja	Celowe tworzenie lub rozpowszechnianie fałszywych i zmanipulowanych treści w celu zmiany percepcji, zaufania lub decyzji.
15	Ekosystem przemysłowy	Sieć przedsiębiorstw, nauki, kapitału, infrastruktury, dostawców i państwa zdolna wspólnie rozwijać oraz skalować strategiczne technologie.
16	Energia jako tor suwerenności	Zasada, że brak odpornego zasilania paraliżuje wojsko, przemysł, AI, zdrowie, transport i administrację.
17	Gospodarka zdolności narodowych	Model, w którym celem polityki gospodarczej jest także budowa technologii, produkcji, kompetencji, eksportu i odporności potrzebnych państwu.
18	Interoperacyjność danych	Zdolność systemów i instytucji do bezpiecznej wymiany danych oraz wspólnego rozumienia ich znaczenia zgodnie z uprawnieniami.
19	Kontrolowana niezależność strategiczna	Zdolność utrzymania krytycznych funkcji dzięki własnej lub sojuszniczej produkcji, zapasom, alternatywom i prawu do migracji.
20	Krytyczna technologia	Technologia, której utrata, zakaz dostępu lub przejęcie może poważnie ograniczyć bezpieczeństwo, gospodarkę albo proces decyzyjny państwa.

Nr	Pojęcie	Definicja operacyjna
21	Odporność energetyczna	Zdolność systemu energii do utrzymania dostaw, ograniczenia skutków awarii i szybkiego odtworzenia po ataku albo szoku.
22	Odporność informacyjna	Zdolność instytucji i obywateli do rozpoznawania manipulacji, zachowania wspólnego pola faktów i działania mimo presji informacyjnej.
23	Odporność poznawcza	Zdolność zachowania osądu, orientacji i woli działania pod wpływem dezinformacji, przeciążenia, lęku, polaryzacji i manipulacji.
24	Odporność łańcucha dostaw	Zdolność wykrywania zakłóceń, przełączania dostaw, korzystania z zapasów i odtwarzania przepływu bez utraty funkcji krytycznych.
25	Państwo przedsiębiorcze	Państwo zdolne wyznaczać misję, współtworzyć rynki, ponosić ryzyko technologiczne i wiązać wsparcie z mierzalnym wynikiem publicznym.
26	Produkcja strategiczna	Krajowa lub sojusznicza zdolność wytwarzania dóbr niezbędnych dla obrony, energii, zdrowia, infrastruktury i cyfryzacji.
27	Prywatny bramkarz	Korporacja lub platforma kontrolująca kluczową infrastrukturę, rynek, dane albo kanał dostępu i przez to zdolna ograniczać decyzje publiczne.
28	Reindustrializacja	Odbudowa i modernizacja zdolności produkcyjnych w sektorach o znaczeniu dla produktywności, eksportu i bezpieczeństwa.
29	Strategiczny open source	Świadome wykorzystywanie i rozwijanie otwartego oprogramowania tam, gdzie zwiększa ono audytowalność, niezależność serwisową i konkurencję.
30	Surowce krytyczne	Materiały niezbędne dla kluczowych technologii i sektorów, których dostawy są skoncentrowane, trudne do zastąpienia lub narażone na presję.
31	Suwerenna AI	Zdolność państwa do używania modeli, danych i infrastruktury AI bez krytycznej zależności od obcej platformy lub pojedynczego dostawcy.
32	Suwerenność danych	Zdolność kontrolowania krytycznych zbiorów, zasad dostępu, przetwarzania, lokalizacji, bezpieczeństwa i możliwości przeniesienia danych.
33	Suwerenność energetyczna	Zdolność kształtowania miksu, infrastruktury, rynku i rezerw bez krytycznej zależności od jednego dostawcy albo technologii.
34	System informacyjny państwa	Połączony układ rejestrów, źródeł, analiz, modeli, alarmów i raportów zapewniający organom wspólny obraz sytuacji.
35	Vendor lock-in	Uzależnienie od jednego dostawcy technologii, chmury, licencji lub platformy, które utrudnia migrację, audyt albo utrzymanie systemu.
36	Wojna informacyjna	Zorganizowane oddziaływanie na informację, percepcję i decyzje przeciwnika poprzez propagandę, cyberoperacje i manipulację kanałami komunikacji.
37	Wojna kognitywna	Długotrwała walka o sposób postrzegania rzeczywistości, tożsamość, emocje, zaufanie i wolę działania społeczeństwa.
38	Własność technologiczna	Kontrola nad IP, dokumentacją, kodem, kompetencjami, serwisem i możliwością rozwoju technologii.
39	Zakaz autonomicznej decyzji krytycznej	Zasada, że AI nie może samodzielnie ostatecznie rozstrzygać o prawach obywatela, życiu, zdrowiu, użyciu siły ani eskalacji militarnej.

Nr	Pojęcie	Definicja operacyjna
40	Zero trust	Model bezpieczeństwa bez domyślnego zaufania: każdy użytkownik, urządzenie, dostęp i żądanie są weryfikowane oraz ograniczane do minimum.
41	Łańcuch dostaw	Sekwencja dostawców, produkcji, transportu, magazynowania i dystrybucji potrzebna do dostarczenia produktu lub usługi.
42	Łańcuch strategiczny	Łańcuch dostaw kluczowy dla obrony, energii, zdrowia, cyfryzacji lub żywności, wymagający audytu, rezerw i planu przełączenia.

A.7. Zakres słownika Tomu 2

Nr	Zakres	Lokalizacja definicji
1	Legislacja i zgodność	Definicje ustawowe, ścieżki prawne, ograniczenia kompetencyjne i standardy kontroli – Tom 2, rozdział 12.
2	Metryki wykonawcze	Definicje KPI, KRI, progów, źródeł danych, właścicieli i częstotliwości aktualizacji – Tom 2, rozdziały 8–10.
3	Modele sektorowe	Operacyjne słowniki obrony, energii, technologii, zdrowia, gospodarki i informacji – Tom 2, rozdział 11.
4	Protokoły decyzji	Karty decyzji, karty ryzyka, zasady eskalacji, audytu i odpowiedzialności – Tom 2, rozdziały 8–10.
5	Ryzyka realizacyjne	Ryzyka polityczne, techniczne, prawne, finansowe i społeczne wdrożenia wraz z działaniami ograniczającymi – Tom 2, rozdział 14.
6	Wdrożenie instytucjonalne	Role organów, zespołów, właścicieli danych, harmonogramów i trybów przejściowych – Tom 2, rozdział 13.

***Bez wspólnego języka nie ma wspólnego obrazu sytuacji,
odpowiedzialnej decyzji ani sprawnego wykonania.***

Baza źródłowa i inspiracje

Narodowa Strategia Bezpieczeństwa TechnoRepubliki ma charakter programowo-strategiczny i interdyscyplinarny. Łączy polskie dokumenty państwowe, doktrynę NATO i Unii Europejskiej, doświadczenia państw obrony kompleksowej, analizy wojny w Ukrainie, badania nad geoekonomią, cyberbezpieczeństwem i odpornością infrastruktury oraz dorobek teorii systemów, cybernetyki, analizy sieciowej i zarządzania ryzykiem.

Źródła uporządkowano według ich statusu. Dokumenty prawne, urzędowe i sojusznicze stanowią podstawę normatywną; raporty naukowe i analityczne wspierają diagnozę; literatura metodologiczna uzasadnia model MOG i pętlę decyzyjną. Materiały TechnoSanacji, publikacje programowe oraz przykłady rozwiązań przedsięwzięć technologicznych są jawnie oznaczone jako inspiracje projektowe, a nie jako niezależny dowód empiryczny.

Zasada redakcyjna. Dostęp do źródeł internetowych zweryfikowano 26 sierpnia 2026 r.

1. Dokumenty prawne, państwowe i sojusznicze

Podrozdział obejmuje dokumenty o najwyższym statusie normatywnym i doktrynalnym. Wyznaczają one prawne granice działania organów państwa, zobowiązania sojusznicze, standardy odporności oraz aktualne kierunki rozwoju bezpieczeństwa, obronności i cyberbezpieczeństwa.

Polska: prawo i dokumenty strategiczne

- [1.01] Rzeczpospolita Polska. [Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.](#), 1997. **Znaczenie:** Punkt odniesienia dla legalności transformacji, kompetencji władz, stanów nadzwyczajnych oraz ochrony praw i wolności.
- [1.02] Prezydent Rzeczypospolitej Polskiej. [Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej](#), 2020. **Znaczenie:** Oficjalny punkt odniesienia dla interesów narodowych, środowiska bezpieczeństwa, odporności i przygotowań państwa.
- [1.03] Biuro Bezpieczeństwa Narodowego. [Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej](#), 2024 [S1]. **Znaczenie:** Aktualizują diagnozę zagrożeń i potrzeby reformy systemu kierowania bezpieczeństwem narodowym.
- [1.04] Rzeczpospolita Polska. [Ustawa z 11 marca 2022 r. o obronie Ojczyzny, z późniejszymi zmianami](#), 2022–2026. **Znaczenie:** Podstawa kompetencji, planowania obronnego, mobilizacji, finansowania obronności i odpowiedzialności organów państwa.
- [1.05] Rzeczpospolita Polska. [Ustawa z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, z późniejszymi zmianami](#), 2024–2026. **Znaczenie:** Podstawa prawna ochrony ludności, alarmowania, budowli ochronnych, zasobów, ciągłości działania i obrony cywilnej.
- [1.06] Rada Ministrów. [Program Ochrony Ludności i Obrony Cywilnej na lata 2025–2026](#), 2025. **Znaczenie:** Operacjonalizuje finansowanie infrastruktury ochronnej, łączności, zapasów, szkoleń i przygotowania administracji terenowej.
- [1.07] Rada Ministrów. [Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej](#), 2026. **Znaczenie:** Aktualna podstawa rozwoju Krajowego Systemu Cyberbezpieczeństwa i odporności cyfrowej państwa, gospodarki i obywateli.

NATO: odstraszanie, odporność i współpraca z przemysłem

- [1.08] North Atlantic Treaty Organization. [The North Atlantic Treaty](#), 1949. **Znaczenie:** Podstawowa rama obrony zbiorowej, konsultacji oraz obowiązku rozwijania indywidualnej i zbiorowej zdolności do odparcia napaści.
- [1.09] NATO. [NATO 2022 Strategic Concept](#), 2022. **Znaczenie:** Doktrynalny punkt odniesienia dla odstraszania, obrony, zarządzania kryzysowego, odporności i technologii przełomowych.
- [1.10] NATO. [Strengthened Resilience Commitment](#), 2021. **Znaczenie:** Potwierdza narodową odpowiedzialność i wspólne zobowiązanie do rozwijania odporności wspierającej zadania Sojuszu.

- [1.11] NATO. [Resilience, Civil Preparedness and Article 3](#), wersja aktualna 2026 [S4]. **Znaczenie:** Definiuje odporność oraz siedem bazowych wymagań dotyczących ciągłości władzy, energii, ludności, żywności i wody, zdrowia, łączności i transportu.
- [1.12] NATO. [The Hague Summit Declaration](#), 2025. **Znaczenie:** Aktualizuje cele zdolnościowe i ścieżkę dochodzenia do 5% PKB na obronę i wydatki związane z bezpieczeństwem do 2035 r.
- [1.13] NATO. [Guidance for Enhancing Public-Private Cooperation for Resilience](#), 2026. **Znaczenie:** Wyznacza zasady współpracy władz z prywatnymi operatorami usług podstawowych i infrastruktury krytycznej.
- [1.14] NATO. [Strategy for Industry–NATO Cooperation](#), 2026. **Znaczenie:** Podstawa współpracy z przemysłem, skalowania produkcji, utrzymania zdolności i zabezpieczenia łańcuchów dostaw.

Unia Europejska: gotowość, infrastruktura i bezpieczeństwo cyfrowe

- [1.15] Rada Unii Europejskiej. [A Strategic Compass for Security and Defence](#), 2022. **Znaczenie:** Rama działania UE w zakresie bezpieczeństwa, obronności, odporności, partnerstw i rozwoju zdolności.
- [1.16] Komisja Europejska i Wysoki Przedstawiciel Unii. [European Preparedness Union Strategy](#), 2025. **Znaczenie:** Wprowadza podejście whole-of-government i whole-of-society do przygotowania na kryzysy oraz kulturę preparedness by design.
- [1.17] Komisja Europejska i Wysoki Przedstawiciel Unii. [White Paper for European Defence – Readiness 2030](#), 2025. **Znaczenie:** Określa potrzeby zdolnościowe, wspólne zakupy, inwestycje przemysłowe i rolę technologii przelomowych.
- [1.18] Parlament Europejski i Rada. [Dyrektywa \(UE\) 2022/2557 w sprawie odporności podmiotów krytycznych – CER](#), 2022. **Znaczenie:** Ustanawia podejście all-hazards do podmiotów zapewniających usługi kluczowe dla gospodarki i społeczeństwa.
- [1.19] Parlament Europejski i Rada. [Dyrektywa \(UE\) 2022/2555 w sprawie wysokiego wspólnego poziomu cyberbezpieczeństwa – NIS2](#), 2022. **Znaczenie:** Wyznacza obowiązki zarządzania cyberryzykiem, raportowania incydentów i odpowiedzialności kierownictwa podmiotów kluczowych.
- [1.20] Parlament Europejski i Rada. [Rozporządzenie \(UE\) 2024/1689 ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji – AI Act](#), 2024. **Znaczenie:** Rama prawna wykorzystywania AI, w tym systemów wysokiego ryzyka, nadzoru, dokumentacji i odpowiedzialności.

Państwa obrony kompleksowej

- [1.21] Security Committee of Finland. [Security Strategy for Society](#), 2025. **Znaczenie:** Aktualny fiński model bezpieczeństwa kompleksowego, współpracy władz, biznesu, organizacji społecznych i obywateli.
- [1.22] Government Offices of Sweden. [Defence Resolution 2025–2030](#), 2024–2025. **Znaczenie:** Aktualna podstawa szwedzkiej obrony totalnej, finansowania obrony cywilnej i zdecentralizowanego kierowania podczas kryzysu i wojny.

2. Raporty naukowe, analityczne i branżowe

Źródła tej grupy służą diagnozie i porównaniu wariantów. Nie mają mocy prawnej, lecz dostarczają danych, analiz przypadków, doświadczeń operacyjnych i wniosków dotyczących Polski, wschodniej flanki NATO, infrastruktury krytycznej, wojny w Ukrainie, cyberbezpieczeństwa oraz bezpieczeństwa gospodarczego.

Polska, wschodnia flanki i przemysł obronny

- [2.01] RAND. [Polish Armed Forces Modernization: A New Cornerstone of European Security?](#), 2025 [2025_RAND_Poland-Cornerstone-European-Security.pdf]. **Znaczenie:** Ocena modernizacji Sił Zbrojnych RP, jej trwałości, skali i znaczenia dla europejskiego systemu bezpieczeństwa.
- [2.02] Fundacja im. Kazimierza Pułaskiego. [Analiza polskiego przemysłu obronnego i współpracy z Koreą Południową](#), 2025 [2025_Pulaski_Poland-Defense-Industry-South-Korea.pdf]. **Znaczenie:** Wspiera ocenę transferu technologii, polonizacji, zdolności produkcyjnych i ryzyka zależności od dostawców zagranicznych.
- [2.03] Instytut Europy Środkowej. [Tarcza Wschód – analiza programu i jego znaczenia strategicznego](#), 2025 [2025_IES_East-Shield-Tarcza-Wschod.pdf]. **Znaczenie:** Podstawa dla odstraszania przez odmowę, fortyfikacji, sensorów, mobilności i ochrony wschodniej granicy.

- [2.04] Wojska Obrony Terytorialnej. *Odporność państwa i działania hybrydowe*, 2023 [S38; 2023_WOT-Odpornosc-Hybrydowa.pdf]. **Znaczenie:** Wspiera model odporności powszechnej, współpracy lokalnej i reagowania na presję poniżej progu wojny.
- [2.05] Sieć Badawcza Łukasiewicz. *Nowa strategia bezpieczeństwa – uwarunkowania i kierunki*, 2025 [S42; 2025_Lukasiewicz_Nowa-Strategia-Bezpieczenstwa.pdf]. **Znaczenie:** Wnosi perspektywę technologiczną, przemysłową i instytucjonalną do projektowania zdolności państwa.
- [2.06] Ośrodek Studiów Wschodnich. *Szczyt NATO w Hadze i zobowiązanie 5% PKB*, 2025 [2025_OSW-Hague-Summit-5proc.pdf]. **Znaczenie:** Pomaga interpretować polityczne, finansowe i zdolnościowe konsekwencje nowego celu inwestycji obronnych.

Odstraszanie, gotowość i obrona totalna

- [2.07] RAND Corporation. *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*, 2016 [2016_RAND-Reinforcing-Deterrence-Baltics-Wargame.pdf]. **Znaczenie:** Klasyczne studium czasu reakcji, rozmieszczenia sił i wartości gier wojennych w planowaniu obrony regionu.
- [2.08] European Parliamentary Research Service. *Comprehensive Military Mobility*, 2025 [2025_EPRS_Comprehensive-Military-Mobility.pdf]. **Znaczenie:** Analiza infrastruktury dual-use, procedur transgranicznych i mobilności wojskowej w Europie.
- [2.09] NATO Science and Technology Organization. *Preparedness, Readiness and Capability Assessment*, 2024 [S34; 2024_NATO-STO_SAS192-Preparedness-Readiness.pdf]. **Znaczenie:** Wspiera budowę mierników gotowości, testów, progów i oceny rzeczywistej zdolności do działania.
- [2.10] Frontiers. *Total Defence and Multilevel Governance*, 2026 [S35; 2026_Frontiers_Total-Defence-Multilevel-Governance.pdf]. **Znaczenie:** Analizuje koordynację między władzami centralnymi, regionalnymi, lokalnymi oraz podmiotami prywatnymi.
- [2.11] Politeja. *Putting Comprehensive Defence to Work*, bez daty w korpusie [RES_Politeja_Putting_Comprehensive_Defense_to_Work.pdf]. **Znaczenie:** Przedstawia warunki praktycznego uruchomienia obrony kompleksowej poza poziomem deklaracji.
- [2.12] NATO Parliamentary Assembly. *Resilience and Civil Preparedness*, 2021 [S37; 2021_NATO-PA-Resilience-Civil-Preparedness.pdf]. **Znaczenie:** Wspiera cywilny wymiar odporności, ciągłość usług i zdolność społeczeństwa do wsparcia obrony.
- [2.13] Swedish Civil Contingencies Agency. *Civil Defence: Lessons Identified from Ukraine*, 2024 [2024_SWE-MSB_Civil-Defence-Lessons-Ukraine.pdf]. **Znaczenie:** Źródło wniosków dotyczących zapasów, logistyki, komunikacji, decentralizacji i ciągłości usług.

Wojna w Ukrainie, cyberprzestrzeń i AI

- [2.14] Jack Watling, Oleksandr Danylyuk i Nick Reynolds. *Preliminary Lessons from Ukraine's Offensive Operations, 2022–23*, RUSI, 2024 [RUSI_Ukraine-Offensive-Lessons-2022-23.pdf]. **Znaczenie:** Doświadczenia dotyczące rozpoznania, dowodzenia, amunicji, logistyki, adaptacji i regeneracji zdolności.
- [2.15] NATO Innovation Hub i środowisko NATO ACT. *Cognitive Warfare Concept*, 2024 [2024_NATO-Cognitive-Warfare-Concept.pdf]. **Znaczenie:** Inspiruje analizę presji na percepcję, zaufanie i wolę społeczną; materiał należy traktować jako koncepcyjny, a nie obowiązującą doktrynę NATO.
- [2.16] Microsoft. *Defending Ukraine: Early Lessons from the Cyber War*, 2022 [2022_Microsoft-Russia-Cyberattack-Ukraine.pdf]. **Znaczenie:** Studium współdziałania państwa i sektora technologicznego podczas rozproszonej kampanii cybernetycznej.
- [2.17] Parlament Europejski. *Cyber Operations in Russia's War against Ukraine*, 2023 [2023_EP-Cyber-Russian-War-Ukraine.pdf]. **Znaczenie:** Analiza roli cyberoperacji, ich ograniczeń i powiązania z działaniami militarnymi oraz informacyjnymi.
- [2.18] European Parliamentary Research Service. *Defence and Artificial Intelligence*, 2025 [2025_EPRS-Defence-and-AI.pdf]. **Znaczenie:** Źródło dla zastosowań AI w obronności, zasad odpowiedzialności oraz potrzeby zachowania human-in-command.
- [2.19] Zespół badawczy ICS. *AI Cyber Resilience Index for Industrial Control Systems*, bez daty w korpusie [RES_AI_Cyber_Resilience_Index_ICS.pdf]. **Znaczenie:** Wspiera pomiar odporności cyberfizycznej energetyki, przemysłu i innych systemów sterowania.

[2.20] Center for Security and Emerging Technology. *The Semiconductor Supply Chain*, 2021 [2021_CSET_Semiconductor-Supply-Chain.pdf]. **Znaczenie:** Podstawa analizy chokepoints technologicznych, zależności produkcyjnych i bezpieczeństwa dostaw chipów.

Bałtyk, gospodarka, energia i łańcuchy dostaw

[2.21] Zespół autorów MDPI. *Baltic Ports and Poland's Energy Security*, 2025 [2025_MDPI-Baltic-Polish-Ports-Energy-Security.pdf]. **Znaczenie:** Analiza znaczenia portów, terminali i infrastruktury morskiej dla bezpieczeństwa energetycznego Polski.

[2.22] European Parliamentary Research Service. *Security and Resilience of Submarine Cables in the European Union*, 2025 [2025_EPRS-Submarine-Cable-EU.pdf]. **Znaczenie:** Źródło dla ochrony kabli, redundancji tras, zdolności naprawczych i współpracy publiczno-prywatnej.

[2.23] Unia Europejska i NATO. *Critical Infrastructure Resilience*, 2023 [2023_EU-NATO-Critical-Infrastructure-Resilience.pdf]. **Znaczenie:** Wspiera integrację wymagań wojskowych i cywilnych oraz współpracę operatorów infrastruktury z władzami.

[2.24] European Parliamentary Research Service. *EU Economic Security Doctrine*, 2025 [2025_EPRS_EU-Economic-Security-Doctrine.pdf]. **Znaczenie:** Podstawa analizy de-riskingu, inwestycji, kontroli eksportu i technologii krytycznych.

[2.25] Hellberg i Lundmark. *Transformation of European Defence Supply Chains*, 2025 [2025_SJMS-Defence-Supply-Chains.pdf]. **Znaczenie:** Wspiera ocenę skalowania produkcji, zależności dostawczych i odporności europejskiej bazy przemysłowo-obronnej.

[2.26] Parlament Europejski. *Energy Security and the European Economy*, 2025 [2025_EP_Energy-Security-and-European-Economy.pdf]. **Znaczenie:** Łączy bezpieczeństwo energii, zapasy, konkurencyjność przemysłu i finansowanie obronności.

[2.27] RAND Corporation. *Measuring National Power in the Postindustrial Age*, 2005 [2005_RAND-Measuring-National-Power-MR1110.pdf]. **Znaczenie:** Rozróżnia zasoby państwa od zdolności ich konwersji w realny efekt strategiczny.

[2.28] Mario Draghi. *The Future of European Competitiveness*, 2024. **Znaczenie:** Łączy bezpieczeństwo, technologię, energię, inwestycje i przemysłową zdolność Europy.

3. Podstawa metodologiczna MOG i cybernetyki państwa

Mapa Oddziaływań Geopolitycznych jest autorską syntezą analizy sieciowej, zarządzania ryzykiem, teorii decyzji i cybernetyki. Poniższe źródła nie potwierdzają jednego gotowego modelu MOG, lecz dostarczają rygoru pojęciowego i narzędzi potrzebnych do jego operacjonalizacji, kalibracji, walidacji oraz audytu.

Ryzyko, prawdopodobieństwo i decyzje wielokryterialne

[3.01] International Organization for Standardization. *ISO 31000:2018 – Risk Management: Guidelines*, 2018. **Znaczenie:** Porządkuje identyfikację, analizę, ocenę, postępowanie, monitorowanie i komunikowanie ryzyka.

[3.02] International Organization for Standardization. *ISO Guide 73:2009 – Risk Management: Vocabulary*, 2009. **Znaczenie:** Ujednolica pojęcia ryzyka, zdarzenia, konsekwencji, prawdopodobieństwa, podatności i zabezpieczeń.

[3.03] National Institute of Standards and Technology. *NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments*, 2012. **Znaczenie:** Dostarcza metodyki budowy scenariuszy zagrożeń, oceny podatności, prawdopodobieństwa i skutków.

[3.04] Stanley Kaplan i B. John Garrick. *On the Quantitative Definition of Risk*, Risk Analysis 1(1), 1981. **Znaczenie:** Klasyczny schemat ryzyka oparty na scenariuszu, prawdopodobieństwie oraz konsekwencjach.

[3.05] Judea Pearl. *Probabilistic Reasoning in Intelligent Systems*, 1988. **Znaczenie:** Podstawa aktualizacji bayesowskiej, modelowania zależności i jawnego opisywania niepewności.

[3.06] Andrea Saltelli i in. *Global Sensitivity Analysis: The Primer*, 2008. **Znaczenie:** Metodyka badania wpływu wag, parametrów i niepewności na wyniki modelu MOG.

[3.07] David Vose. *Risk Analysis: A Quantitative Guide*, 3. wyd., 2008. **Znaczenie:** Praktyczne zastosowanie rozkładów prawdopodobieństwa, symulacji Monte Carlo i analizy scenariuszy.

[3.08] Valerie Belton i Theodor J. Stewart. *Multiple Criteria Decision Analysis: An Integrated Approach*, 2002. **Znaczenie:** Podstawa wielokryterialnego indeksu priorytetu i jawnego ustalania wag decyzyjnych.

Grafy, sieci wielowarstwowe i świadomość sytuacyjna

- [3.09] Mikko Kivelä, Alexandre Arenas, Marc Barthelemy, James P. Gleeson, Yamir Moreno i Mason A. Porter. [Multilayer Networks](#), Journal of Complex Networks 2(3), 2014. **Znaczenie:** Formalna podstawa przedstawiania aktorów i relacji MOG jako dynamicznego, skierowanego i wielowarstwowego grafu.
- [3.10] Mark Newman. *Networks*, 2. wyd., 2018. **Znaczenie:** Podstawa pomiaru centralności, przepływów, wspólnot, odporności i dynamiki sieci.
- [3.11] Mica R. Endsley. [Toward a Theory of Situation Awareness in Dynamic Systems](#), Human Factors 37(1), 1995. **Znaczenie:** Uzasadnia wymagania wspólnego obrazu sytuacji, jakości danych i rozumienia dynamiki otoczenia.
- [3.12] John R. Boyd. *A Discourse on Winning and Losing*, 1987; wydania późniejsze. **Znaczenie:** Źródło pętli OODA i znaczenia tempa obserwacji, orientacji, decyzji i działania.

Cybernetyka regulatora i systemu zdolnego do przetrwania

- [3.13] Norbert Wiener. *Cybernetics: Or Control and Communication in the Animal and the Machine*, 1948. **Znaczenie:** Fundamentalna teoria sterowania, komunikacji i sprzężenia zwrotnego.
- [3.14] W. Ross Ashby. [An Introduction to Cybernetics](#), 1956. **Znaczenie:** Źródło prawa wymaganej różnorodności oraz analizy regulatora wobec złożonych zakłóceń.
- [3.15] Roger C. Conant i W. Ross Ashby. [Every Good Regulator of a System Must Be a Model of That System](#), International Journal of Systems Science 1(2), 1970. **Znaczenie:** Uzasadnia potrzebę utrzymywania przez państwo jawnego i aktualnego modelu własnego otoczenia oraz zdolności.
- [3.16] Stafford Beer. *Brain of the Firm*, 1972. **Znaczenie:** Rozwija Viable System Model i funkcjonalne warstwy organizacji zdolnej do utrzymania autonomii.
- [3.17] Stafford Beer. *The Heart of Enterprise*, 1979. **Znaczenie:** Rozwija relacje między operacjami, koordynacją, kontrolą, inteligencją strategiczną i tożsamością systemu.
- [3.18] Francis Heylighen. *Cybernetics and Second-Order Cybernetics*, 2001 [S46; 2001_Cybernetics-Second-Order-Heylighen.pdf]. **Znaczenie:** Porządkuje sprzężenie zwrotne, celowość, adaptację i rolę obserwatora w modelu sterowania.
- [3.19] Marian Mazur. *Cybernetyka i charakter*, 1976. **Znaczenie:** Polska podstawa teorii systemu autonomicznego, sterowania sobą oraz trwałych właściwości dynamicznych człowieka i organizacji.
- [3.20] Józef Kossecki. *Cybernetyka społeczna*, wydania różne. **Znaczenie:** Źródło analizy sterowania społecznego, torów informacyjnych i energetycznych oraz autonomii systemu państwowego.

Zarządzanie ryzykiem AI i cyberbezpieczeństwem

- [3.21] National Institute of Standards and Technology. [Artificial Intelligence Risk Management Framework – AI RMF 1.0](#), 2023. **Znaczenie:** Wprowadza funkcje Govern–Map–Measure–Manage oraz wymagania dotyczące wiarygodności, dokumentowania i oceny ryzyka AI.
- [3.22] National Institute of Standards and Technology. [The NIST Cybersecurity Framework – CSF 2.0](#), 2024. **Znaczenie:** Porządkuje zarządzanie, identyfikację, ochronę, detekcję, reakcję i odbudowę systemów cyfrowych.

Zastrzeżenie metodologiczne. MOG jest modelem autorskim, który będzie wymagał słownika budowanego na rzeczywistych zmiennych oraz normalizacji skal, wskazania źródeł danych, przedziałów niepewności, testów historycznych, analizy wrażliwości, symulacji Monte Carlo, red teamingu i okresowej walidacji progów ostrzegawczych.

4. Inspiracje programowe i materiały własne TechnoSanacji

Podrozdział obejmuje koncepcje, książki, studia przypadków i opracowania własne, które wpłynęły na język oraz architekturę TechnoRepubliki. Inspiracje te nie są traktowane jako źródła normatywne. Ich rolą jest dostarczanie pytań, modeli projektowych i kontrastowych perspektyw, które następnie podlegają ocenie prawnej, naukowej i strategicznej.

Klasyka geopolityki i geoeconomii

- [4.01] Alfred Thayer Mahan. *The Influence of Sea Power upon History, 1660–1783*, 1890. **Znaczenie:** Inspiracja dla znaczenia Bałtyku, portów, infrastruktury morskiej i linii komunikacyjnych.
- [4.02] Halford J. Mackinder. *The Geographical Pivot of History*, 1904. **Znaczenie:** Punkt odniesienia dla położenia Polski na styku Europy Zachodniej i wschodniej przestrzeni kontynentalnej.

- [4.03] Nicholas J. Spykman. *The Geography of the Peace*, 1944. **Znaczenie:** Inspiracja dla Polski jako węzła Rimlandu i spinacza między Bałtykiem, Karpatami i Morzem Czarnym.
- [4.04] Zbigniew Brzeziński. *The Grand Chessboard: American Primacy and Its Geostrategic Imperatives*, 1997. **Znaczenie:** Perspektywa geostrategiczna Eurazji oraz znaczenia Europy Środkowo-Wschodniej.
- [4.05] John J. Mearsheimer. *The Tragedy of Great Power Politics*, 2001. **Znaczenie:** Źródło realistycznej analizy rywalizacji mocarstw, niepewności intencji i warunkowości gwarancji.
- [4.06] Edward N. Luttwak. *From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce*, 1990. **Znaczenie:** Podstawa języka geoeconomii, sankcji, przemysłu, energii i handlu jako instrumentów siły.
- [4.07] Henry Farrell i Abraham L. Newman. *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, *International Security* 44(1), 2019. **Znaczenie:** Inspiracja dla analizy chokepoints, asymetrycznych zależności i prywatnych węzłów globalnej infrastruktury.

Państwo technologiczne, misyjne i odporne na prywatne bramki dostępu

- [4.08] Mariana Mazzucato. *The Entrepreneurial State*, 2011/2013 [załącznik: *Entrepreneurial_State_-_web.pdf*]. **Znaczenie:** Inspiracja dla państwa podejmującego ryzyko, tworzącego rynki, organizującego misje i rozwijającego kapitał cierpliwy.
- [4.09] Mariana Mazzucato. *Mission-Oriented Innovation Policy*, 2017 i publikacje późniejsze. **Znaczenie:** Podstawa przekładu celów strategicznych na portfele misji, zdolności wykonawcze, zamówienia i mierniki wyniku.
- [4.10] Alexander C. Karp i Nicholas W. Zamiska. *The Technological Republic: Hard Power, Soft Belief and the Future of the West*, 2025 [załącznik: *TECHNOLOGICAL REPUBLIC Karp Zamiska.pdf*]. **Znaczenie:** Manifest technologiczno-polityczny inspirujący współpracę państwa, nauki, przemysłu i sektora oprogramowania; wymaga krytycznej adaptacji do polskiej podmiotowości.
- [4.11] Palantir Technologies i materiały dotyczące platform danych. *Integracja danych, ontologia operacyjna i software-defined decision support*. **Znaczenie:** Studium rozwiązań wspierających wspólny obraz operacyjny; nie jest wzorcem jedynej dostawcy ani substytutem suwerenności danych.
- [4.12] Denise Hearn, Nidhi Hegde i Matt Stoller. *The Other Red Tape: Market Concentration and the Rise of Private Gatekeepers*, American Economic Liberties Project, 2021 [AELP_TheOtherRedTape_Final_Clean.pdf]. **Znaczenie:** Krytyczna inspiracja dotycząca prywatnej regulacji rynku, koncentracji platform i infrastrukturalnych bramek.
- [4.13] Alby Anand Kurian. *The Marketing of Nations for a Permacrisis Era: The Greater Global Purpose Framework*, working paper, 2026. **Znaczenie:** Inspiracja dla pojęcia nadrzędnego celu państwa i kapitału narracyjnego; wymaga oznaczenia jako praca koncepcyjna, nie utrwalaony standard naukowy.

Materiały własne TechnoSanacji i TechnoRepubliki

- [4.14] Andrzej Węgrzyn / TechnoSanacja. *TECHNO-REPUBLIKA POLSKA*, materiał programowy. **Znaczenie:** Wczesny zapis celów ustrojowych, obywatelskiej obrony, agencji zadaniowych i technologicznego państwa.
- [4.15] Andrzej Węgrzyn. *Ruch sanacyjny jako regulator cybernetyczny*, materiał autorski. **Znaczenie:** Łączy teorię regulatora, polską cybernetykę, cyrkulację elit i międzypokoleniowy ruch na rzecz TechnoRepubliki.
- [4.16] Andrzej Węgrzyn. *Struktura agentowa TechnoRepubliki oraz metodyka agentów w państwie*. **Znaczenie:** Podstawa grafu ról, kart odpowiedzialności, pętli wykonania oraz współpracy agentów instytucjonalnych, ludzkich i AI.

Zasada wykorzystania inspiracji. Książki programowe, materiały przedsiębiorstw oraz opracowania własne służą projektowaniu i stawianiu hipotez. Każdy postulat prawny, finansowy, militarny lub technologiczny powinien być następnie konfrontowany z dokumentami z grupy 1, dowodami z grupy 2 oraz rygorem metodologicznym grupy 3.

Sudety, 27.08.2026. - Materiał udostępniony na licencji Creative Commons - Uznanie autorstwa