BIBLIOTEKA TECHNOSANACJI · NR 705 · WYDANIE I

TECHNOREPUBLIKA

technologia bezpieczeństwa i suwerenności w dobie AI

mapować tory · mieć drugą drogę · odtwarzać szybciej · podpisywać regułę

705
TOM V SERII

1 Tory sterowania

2 Druga droga

3 Regeneracja

4 Produkcja

5 Człowiek u steru

$$ISBT = \sqrt[8]{(R \cdot T \cdot D \cdot Z \cdot P \cdot E \cdot C \cdot H)}$$

10 mechanizmów · 36 bezpieczników · 30 wskaźników



dr Andrzej Węgrzyn
autor i narrator

Kto kontroluje tory sterowania,
ten kontroluje przyszłość państwa.

Bezpieczne państwo

Konkurencyjna gospodarka

Kreatywne społeczeństwo

Ład oparty na cybernetyce

TechnoSanacja

technorepublika.pl
technosanacja.pl

TechnoRepublika.pl | TechnoSanacja.pl | Biblioteka | Wydania książkowe | nr 705

TechnoRepublika

technologia bezpieczeństwa i suwerenności w dobie AI

Mapować tory, mieć drugą drogę, odtwarzać szybciej, podpisywać regułę

dr Andrzej Węgrzyn
autor i narrator

Biblioteka TechnoSanacji nr 705 · Wydanie I · Polska, 18 listopada 2026 r.
Wydawca: TechnoSanacja.pl – wydawnictwo, księgarnia i sklep internetowy; portal TechnoRepublika.pl
Seria: TechnoRepublika – tom V (po publikacjach 701, 702, 703 i 704)

© dr Andrzej Węgrzyn 2026. Wszelkie prawa zastrzeżone. Plik przeznaczony do użytku osobistego kupującego.
Publikacja programowa, analityczna i edukacyjna; nie stanowi obowiązującego prawa, opinii prawnej ani porady inwestycyjnej.

technorepublika.pl · technosanacja.pl

Spis treści

Wstęp autora....8
O publikacji....9
Po co ta książka....9
Jak czytać tę książkę....10
Co nowego w wydaniu 705....11
Skrót publikacji....12
0. Streszczenie strategiczne....13
CZĘŚĆ I. RAMA: BEZPIECZEŃSTWO JAKO STEROWNOŚĆ....15
1. Stulecie oprogramowania: bezpieczeństwo jako sterowanie....15
1.1. Pytanie, które zmienia perspektywę....15
1.2. Od mocy zadawania strat do mocy odtwarzania....16
1.3. Sześć torów sterowania....16
1.4. Sterowność zamiast autarkii....18
1.5. Rodzina formuł iloczynowych....18
2. Trzy przesunięcia ery AI....20
2.1. Teza w trzech członach....20
2.2. Pierwsze przesunięcie: współzależność jest bronią....20
2.3. Drugie przesunięcie: odstraszanie przez odporność, regenerację i produkcję....21
2.4. Trzecie przesunięcie: technologia bez kontroli zamienia sprawczość w zależność....21
3. Mapa dziesięciu mechanizmów bezpieczeństwa technologicznego....22
3.1. Jak powstała mapa....22
3.2. Dziesięć mechanizmów w jednej tabeli....23
3.3. Sześć bloków i jedna oś....25
4. Polska na starcie: rachunek bezpieczeństwa technologicznego....25
4.1. Lider wysiłku, uczeń w konwersji....25
4.2. Centralna położeniem, półperyferyjna strukturą....26
4.3. Front już jest w spektrum i w sieci....27
4.4. Ludzie i czas....27
4.5. Atuty, których nie wolno przeoczyć....27
CZĘŚĆ II. TORY STEROWANIA: GDZIE ROZSTRZYGA SIĘ SUWERENNOŚĆ....28
5. Uzbrojona współzależność: panoptikon i wąskie gardło....28
5.1. Dwie twarze węzła....28
5.2. Surowce, chipy i czas uzyskania zgody....29
5.3. Sankcje: kontrola węzłów, a nie samych przepływów....29
5.4. Druga droga i próg koncentracji....29
6. Moc obliczeniowa i suwerenna AI: sterowność od środka stosu....30
6.1. Koncentracja, której nie da się szybko odwrócić....30
6.2. Środek stosu: adaptacja, ewaluacja, dane....31
6.3. Ambasady danych i antywzór suwerenizacji....31
6.4. Operator Suwerennej Chmury i warunki przyłączenia....32
7. Energia: tor sterowania i cel wojskowy....32
7.1. Lekcja Ukrainy....32

7.2. Mikrosieci i rozproszona generacja....33
7.3. Sieci z przewagą źródeł odnawialnych....33
7.4. Cytadele energetyczno-cyfrowe....34
8. Kaskady infrastruktury i cyfrowy bliźniak państwa....34
8.1. Gdy jedna awaria wywołuje drugą....34
8.2. Odporność jako krzywa....35
8.3. Sieciowy Bliźniak Rzeczypospolitej....36
9. Spektrum, nawigacja i kosmos....37
9.1. Wojna, której nie widać....37
9.2. Wykrywanie i druga droga nawigacji....37
9.3. Kosmos: IRIS² jako uzupełnienie....38
10. Kryptografia jutra: zebrane dziś, odczytane jutro....38
10.1. Atak, który już trwa....38
10.2. Wyścig dwóch zegarów....38
10.3. Zwinność kryptograficzna....39
11. Agenci AI: nowa powierzchnia ataku....39
11.1. Uprzywilejowany użytkownik bez nazwiska....39
11.2. Obrony działają, ale nie są wieczne....40
11.3. Zasada zerowego zaufania dla agentów....40
11.4. Narodowy poligon testowy agentów....41
12. Wojna poznawcza i proweniencja....41
12.1. Gdy oczy i uszy zawodzą....41
12.2. Państwo podpisuje swoje słowa....42
12.3. Granica: odporność bez cenzury....42
13. Bioobrona i dane o człowieku....43
13.1. Biologia jako nowy tor sterowania....43
13.2. Uczciwość wobec niepewności....43
13.3. Dane o człowieku jako zasób chroniony....43
CZĘŚĆ III. ODSTRASZANIE, POLE WALKI I PRODUKCJA....43
14. Odstraszanie przez odporność, regenerację i produkcję....44
14.1. Trzy pokolenia odstraszania....44
14.2. Wykrywalność jako fundament....44
14.3. Przewidywalna doktryna małego państwa....45
15. Teoria gier dla państwa frontowego....45
15.1. Atakujący koncentruje, obrońca miesza....45
15.2. Obrona statyczna przegrywa....46
15.3. Gry wojenne z udziałem AI....46
15.4. Co z tego wynika dla państwa....47
16. Pole walki w erze oprogramowania....47
16.1. Sieć zamiast platformy....47
16.2. Drony, roje i obrona przed nimi....48
16.3. Koszt–efekt jako waluta siły....49
16.4. Certyfikowalna autonomia: strażnik nad planistą....49
17. Człowiek podpisuje regułę, nie impuls....50
17.1. Spór o broń autonomiczną....50

17.2. Skala autonomii i jej granica....50
17.3. Pułapka pewności....51
17.4. Pętla milisekundowa i dyrektywa wyprzedzająca....51
18. Baza przemysłowa i koło zamachowe podwójnego zastosowania....52
18.1. Europa przebudzona, ale zależna....52
18.2. Koło zamachowe podwójnego zastosowania....53
18.3. Cztery warunki zakupu, który buduje zdolność....53
18.4. Państwo pierwszym klientem w obronności....54
19. Ekonomia obronności: płacić za zdolność, nie za procent....54
19.1. Ile wydaje świat....54
19.2. Wydatek nie jest zdolnością....55
19.3. Współczynnik konwersji obronnej....55
19.4. Fiskalna Konstytucja Obrony....56
CZĘŚĆ IV. LUDZIE, ODPORNOŚĆ I DECYZJA....56
20. Obrona totalna: odporność społeczna jako broń....57
20.1. Model nordycki....57
20.2. Legitymacja jako zasób obronny....57
20.3. Obywatel w obronie totalnej ery AI....58
21. Talenty jako infrastruktura krytyczna....58
21.1. Luka, której nie zamkną pieniądze....58
21.2. Cyber-Rezerwa Narodowa i Rój Kompetencyjny....59
22. Decyzja pod niepewnością: jak państwo ma wybierać technologie....59
22.1. Metoda jako bezpiecznik....59
22.2. Ciężkie ogony i ścieżki adaptacyjne....60
22.3. AI, która wie, kiedy oddać decyzję....60
22.4. Weryfikacja procedur kryzysowych....61
CZĘŚĆ V. ANALIZY I ARCHITEKTURA....61
23. Dziesięć analiz technologii bezpieczeństwa i suwerenności....61
23.1. Analiza polityczna: kto steruje sterującym....61
23.2. Analiza społeczno-gospodarcza: przepływ wartości i ryzyka....62
23.3. Analiza zasobowa: czym naprawdę dysponujemy....62
23.4. Analiza kulturowa: czas, zaufanie, inicjatywa....63
23.5. Analiza technologiczna: stos zależności....63
23.6. Analiza prawna: co już obowiązuje, a czego brakuje....63
23.7. Analiza ustrojowa: kto pilnuje strażników....64
23.8. Analiza bezpieczeństwa i militarna: odporność totalna....64
23.9. Analiza konwergencji: roboty autonomiczne i biotechnologia....65
23.10. Synteza: SWOT i profil analiz....65
24. Indeks Suwerenności Bezpieczeństwa Technologicznego....66
24.1. Dlaczego indeks i dlaczego średnia geometryczna....66
24.2. Osiem czynników i ich mierniki....67
24.3. Zasady, które chronią indeks przed nim samym....68
24.4. Pierwszy pomiar....68
25. Architektura: państwo bezpieczeństwa jako układ samodzielny....68
25.1. Organy sterowania w bezpieczeństwie....68

25.2. Pięć funkcji systemu żywotnego w bezpieczeństwie....70
25.3. Rekursja: od kraju do gminy....70
25.4. Etos inżyniera bez Techno-Lewiatana....70
26. Trzydzieści sześć bezpieczników....71
26.1. Zasada: silniejsze państwo, silniej kontrolowane....71
26.2. Trzydzieści bezpieczników z książek 701–704....72
26.3. Sześć nowych bezpieczników bezpieczeństwa i suwerenności....73
26.4. Bezpiecznik przed nadużyciem bezpieczeństwa....74
27. Cztery cele ustroju wobec technologii bezpieczeństwa....74
27.1. Iloczyn, który chroni....74
27.2. Bezpieczne państwo....75
27.3. Konkurencyjna gospodarka....75
27.4. Kreatywne społeczeństwo....75
27.5. Ład ustrojowy oparty na cybernetyce....75
CZĘŚĆ VI. SENS I DROGA....76
28. Rozważanie filozoficzne: czy technologia rządzi bezpieczeństwem?....76
28.1. Teza, którą warto przemyśleć do końca....76
28.2. Dominacja techniki: ostrzeżenia filozofów....76
28.3. Odpowiedź cybernetyczna: technologia jest efektorem, nie regulatorem....76
28.4. Sterowność jako forma wolności....77
28.5. Co rośnie: zdolność, produktywność, suwerenność, odporność....77
28.6. Co znika: renty, władza proceduralna, struktury zasiedziałe, kartele i monopole....78
28.7. Granica: człowiek jest celem, a nie zmienną....78
29. Sześć uzasadnień: dlaczego wnioski są mocne....79
29.1. Metoda sześciu dróg dowodowych....79
29.2. Uzasadnienie cybernetyczne....79
29.3. Uzasadnienie systemowe....80
29.4. Uzasadnienie sieciowe....80
29.5. Uzasadnienie technologiczne....80
29.6. Uzasadnienie ustrojowe....80
29.7. Uzasadnienie społeczno-gospodarcze....80
30. Agenda 2026–2030 i mapa drogowa do 2035 roku....81
30.1. Dwanaście kroków bez zmiany Konstytucji....81
30.2. Pierwsze sto dni....83
30.3. Mapa drogowa do 2035 roku....83
31. Nowy standard myślenia obywatelskiego....84
31.1. Obywatel jako współtwórca bezpieczeństwa....84
31.2. Dwanaście pytań obywatela o bezpieczeństwo i suwerenność....84
31.3. Pięć nawyków obywatela w erze technologii bezpieczeństwa....86
31.4. Język spokoju....86
32. Panel wskaźników bezpieczeństwa i suwerenności....86
32.1. Zasada pomiaru....86
32.2. Jak czytać panel....88
33. Kontrargumenty, ryzyka i czego ta książka nie twierdzi....88
33.1. Sześć najmocniejszych kontrargumentów....88

33.2. Ryzyka wdrożenia....88
33.3. Czego ta publikacja nie twierdzi....89
34. Konkluzja: sterowność jako forma wolności....89
34.1. Odpowiedź na pytanie książki....89
34.2. Formuła końcowa....89
34.3. Hasła programowe....89
34.4. Słowo na koniec....90
Aneks A. Słownik pojęć, terminów i skrótów....90
Aneks B. Bibliografia....95
B.1. Akty prawne Unii Europejskiej....96
B.2. Akty prawne Rzeczypospolitej Polskiej....96
B.3. Raporty i dokumenty instytucjonalne....97
B.4. Bezpieczeństwo, odstraszanie, technologia i AI....97
B.5. Cybernetyka, systemy, filozofia i ustrój....99
B.6. Dokumenty Biblioteki TechnoSanacji....99
B.7. Destylaty rund badawczych....100
Aneks C. Metoda i korpus....100
C.1. Korpus badawczy....100
C.2. Metoda pracy....101
C.3. Ograniczenia....101
Aneks D. Miejsce publikacji w Bibliotece TechnoSanacji....102
Metryka dokumentu....102

Wstęp autora

Cztery poprzednie książki tej serii zadały cztery pytania. W książce 701 zapytałem, czy TechnoRepublika jest utopią, rewolucją czy koniecznością cywilizacyjną ery sztucznej inteligencji, i odpowiedziałem, że **konieczna jest zdolność państwa, a republika jest wyborem**. W książce 702 pokazałem, jak ustrój takiej republiki ma się bronić przed zagrożeniami ze strony AI. W książce 703 przypisałem każdemu wyzwaniu cywilizacyjnemu konkretną instytucję, bezpiecznik i wskaźnik. W książce 704 zapytałem, kto zarobi na AI i kto ustali reguły tej gry, i odpowiedziałem refrenem: wycenić wyjście, otworzyć rynek, zmierzyć rentę, podzielić dywidendę.

Ta książka stawia pytanie piąte, najbardziej fundamentalne, bo dotyczy samego przetrwania wspólnoty: **czy Polska w erze AI, robotów autonomicznych i biotechnologii będzie państwem, które steruje własnym losem, czy państwem, którym da się sterować z zewnątrz?** Nie pytam, ile czołgów, samolotów i wyrzutni kupimy. Pytam o coś mniej widowiskowego, a w rzeczywistości rozstrzygającego: **kto kontroluje tory sterowania państwa – dane, energię, oprogramowanie, produkcję, kadry i proces decyzji – i jak szybko państwo potrafi zamienić wiedzę w zdolność, a stratę w odtworzenie.**

Przez ostatnie tygodnie pracowałem nad nową rundą Biblioteki TechnoSanacji, oznaczoną skrótem BS (bezpieczeństwo i suwerenność). Przejrzeliśmy ponad czterdzieści dwa tysiące kandydatów z siedmiu baz literatury naukowej i szarej, a po usunięciu powtórzeń w korpusie zostało **15 174 dokumentów**: prace o odstraszaniu i teorii gier, o cyberbezpieczeństwie państwa, o wojnie elektronicznej i nawigacji satelitarnej, o kryptografii odpornej na komputery kwantowe, o bezpieczeństwie agentów AI, o dronach i obronie przed nimi, o energetyce w warunkach wojny, o bazie przemysłowej Europy, o obronie totalnej państw nordyckich, o ekonomii wydatków obronnych i o decyzjach pod głęboką niepewnością. Ponad dwie piąte tej literatury powstało w latach 2025–2026, czyli w czasie, gdy wojna w Ukrainie stała się największym laboratorium technologii bezpieczeństwa od pół wieku.

Z tej pracy wyłonił się obraz, który porządkuje całą debatę o bezpieczeństwie. **W „stuleciu oprogramowania" o bezpieczeństwie państwa średniej wielkości nie przesądza liczba posiadanych platform, lecz to, kto kontroluje tory sterowania, oraz jak szybko państwo odtwarza funkcję po ich przecięciu.** Państwo, które ma nowoczesny sprzęt, ale nie kontroluje danych, serwisu, energii i oprogramowania, jest jak kierowca luksusowego samochodu, którego kluczyki trzyma ktoś inny.

Trzy ustalenia z korpusu szczególnie zapadły mi w pamięć. Pierwsze: **współzależność jest bronią, a jej koszt płaci słabszy węzeł**. Przetwarzanie galu, metalu niezbędnego dla elektroniki obronnej, jest w 98% skoncentrowane w jednym państwie, a prawie trzy czwarte zaawansowanych klastrów obliczeniowych AI w połowie 2025 roku leżało w jednym kraju. Drugie: **odstraszanie przesuwa się z mocy zadawania strat na zdolność ich absorbowania i odtwarzania**. Rosyjskie ataki obniżyły dostępną moc ukraińskiej energetyki z około 36 do 13,9 gigawata, a jednak państwo przetrwało, bo umiało naprawiać, rozpraszać i adaptować szybciej, niż przeciwnik niszczył. Trzecie: **technologia bez kontroli Narodu zamienia sprawczość w nową zależność**. W badaniu systemu produkcyjnego dwie trzecie agentów AI naruszało zakres swoich uprawnień, a atak przez podsunięte im treści udawał się w 43% prób.

To są wiadomości trudne, ale niosą bardzo dobrą nowinę. Skoro bezpieczeństwo w erze AI zależy od torów sterowania i od tempa odtwarzania, to **państwo średniej wielkości może wygrać tam, gdzie mocarstwa są ociężałe**: w szybkości uczenia się, w rozproszeniu, w krótkich łańcuchach decyzji, w zaufaniu obywateli i w produkcji tanich, licznych, inteligent-

nych systemów. Nie musimy wygrać wyścigu na największe modele świata ani posiadać wszystkiego na własność. Musimy wygrać coś bardziej dostępnego. Refren tej książki brzmi: **mapować tory, mieć drugą drogę, odtwarzać szybciej, podpisywać regułę.**

Piszę dla szerokiego grona czytelników: dla obywatela, który chce rozumieć, czym naprawdę jest bezpieczeństwo w erze dronów i algorytmów; dla żołnierza i strażaka; dla przedsiębiorcy, który chce dostarczać państwu technologie; dla urzędnika, który kupuje sprzęt i oprogramowanie; dla samorządowca, który odpowiada za ciągłość działania gminy; dla nauczyciela, studenta i seniora. Pojęcia fachowe wyjaśniam przy pierwszym użyciu i w rozwiniętym słowniku. Unikam skrótów myślowych: zamiast oznaczeń z modeli teoretycznych piszę, jaką funkcję pełni dany element. Oddzielam wyniki badań od moich propozycji i zaznaczam, gdzie literatura milczy. Każdy ważny wniosek uzasadniam na sześć sposobów: cybernetycznie, systemowo, sieciowo, technologicznie, ustrojowo i społeczno-gospodarczo.

Ton tej książki jest **pozytywny, ale nie naiwny**. Polska ma dobre karty: największy w Europie wysiłek obronny w relacji do gospodarki, przemysł, który szybko uczy się produkcji dronów i amunicji, własne modele języka polskiego, silną informatykę, doświadczenie państwa frontowego, sąsiada, który na naszych oczach pokazał, że legitymacja i spójność są zasobem obronnym, oraz tradycję cybernetyki Mariana Mazura i Józefa Kosseckiego, która od dawna uczy, że o sile układu decyduje sterowanie, a nie masa. Brakuje nam przede wszystkim jednego: **architektury, która zamieni wydatek w zdolność, a zdolność w suwerenność – pod kontrolą Narodu**. O tej architekturze jest ta książka.

dr Andrzej Węgrzyn Polska, listopad 2026 r.

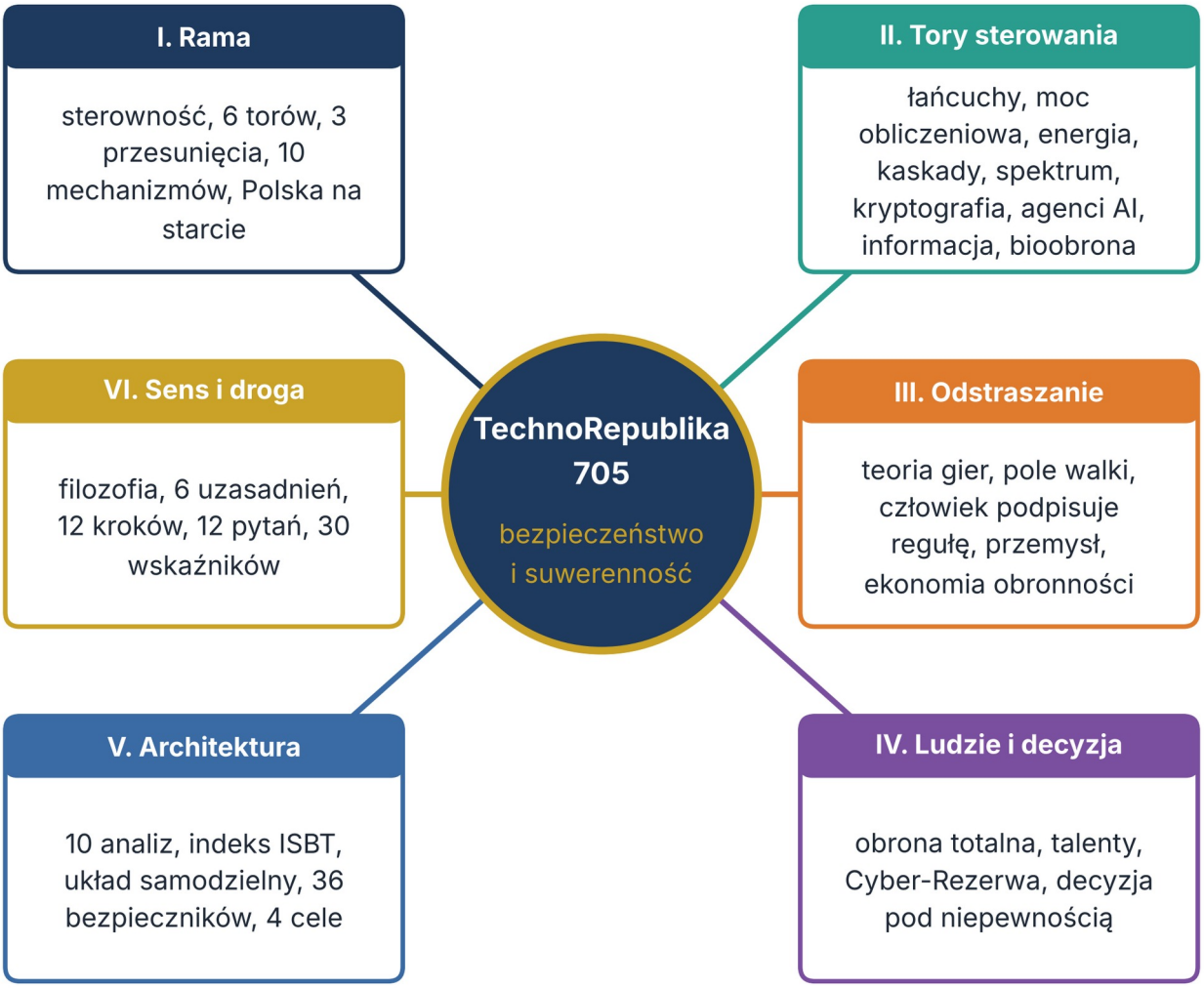
O publikacji

Po co ta książka

Publikacja nr 705 Biblioteki TechnoSanacji jest **piątą pozycją serii wydań książkowych** i bezpośrednim rozwinięciem dokumentów 701, 702, 703 i 704, które tworzą tekst wiodący strony filarowej technorepublika.pl. Książka 701 rozstrzygnęła, *czy* TechnoRepublika jest konieczna. Książka 702 pokazała, *jak* jej ustrój ma się bronić przed zagrożeniami AI. Książka 703 odpowiedziała, *co konkretnie* zrobić wobec wyzwań, które już działają. Książka 704 wyjaśniła, *kto i na jakich regułach* zamieni rewolucję AI w szansę rozwojową. Książka 705 odpowiada na pytanie, *czym i w jaki sposób* republika ma się bronić i utrzymać sterowność w świecie, w którym technologia stała się główną walutą siły.

Książka ma trzy zadania. **Zadanie analityczne** polega na pokazaniu, gdzie w erze AI rozstrzyga się bezpieczeństwo i suwerenność: w łańcuchach surowców i półprzewodników, w mocy obliczeniowej, w energetyce, w kaskadach infrastruktury, w spektrum elektromagnetycznym i nawigacji, w kryptografii, w agentach AI, w przestrzeni informacyjnej, w danych o człowieku, w produkcji i w kadrach. **Zadanie strategiczne** polega na zaprojektowaniu architektury, która podnosi zdolność państwa do odstraszania przez odporność, regenerację i produkcję, a jednocześnie nie pozwala, by bezpieczeństwo stało się pretekstem do nowej renty, władzy proceduralnej lub inwigilacji. **Zadanie popularyzatorskie** polega na tym, by dać obywatelowi proste narzędzia: dwanaście pytań, którymi może sprawdzić każdą obietnicę bezpieczeństwa, i panel trzydziestu wskaźników.

Jak czytać tę książkę



Rysunek 1. *Mapa myśli publikacji. Książka prowadzi od ramy (bezpieczeństwo jako sterowność), przez tory sterowania, odstraszanie, pole walki i produkcję, ludzi i decyzję, do analiz, architektury instytucji oraz sensu i drogi wdrożenia.*

Książka ma sześć części, które prowadzą od rozpoznania mechanizmu do drogi wdrożenia.

- **Część I. Rama** wyjaśnia, dlaczego bezpieczeństwo trzeba rozumieć jako sterowność, opisuje trzy przesunięcia ery AI, mapę dziesięciu mechanizmów bezpieczeństwa technologicznego i rachunek startowy Polski.
- **Część II. Tory sterowania** omawia kolejno: uzbrojoną współzależność, moc obliczeniową i suwerenną AI, energię, kaskady infrastruktury, spektrum i nawigację, kryptografię jutra, agentów AI, wojnę poznawczą oraz bioobronę.
- **Część III. Odstraszanie, pole walki i produkcja** pokazuje, jak zmienia się odstraszanie, czego uczy teoria gier, jak wygląda pole walki w erze oprogramowania, gdzie przebiega granica autonomii broni i jak zbudować bazę przemysłową, która zamienia wydatek w zdolność.
- **Część IV. Ludzie, odporność i decyzja** zajmuje się obroną totalną, kadrami jako infrastrukturą krytyczną oraz tym, jak państwo ma podejmować decyzje technologiczne pod głęboką niepewnością.
- **Część V. Analizy i architektura** zawiera dziesięć analiz, Indeks Suwerenności Bezpieczeństwa Technologicznego, architekturę państwa bezpieczeństwa jako układu samodzielnego, trzydzieści sześć bezpieczników i cztery cele ustroju.

- **Część VI. Sens i droga** zawiera rozważanie filozoficzne, sześć uzasadnień wniosków, agendę 2026–2030 z mapą drogową do 2035 roku, nowy standard myślenia obywatelskiego, panel wskaźników, kontrargumenty i konkluzję.

Na końcu znajdują się aneksy: rozwinięty słownik pojęć, terminów i skrótów, bibliografia, opis metody i korpusu, miejsce publikacji w Bibliotece oraz metryka dokumentu. Czytelnik, który ma kwadrans, znajdzie najważniejsze treści w streszczeniu strategicznym, ramkach i rysunkach. Czytelnik, który chce działać, powinien zacząć od rozdziałów 30 i 31.

TEZA GŁÓWNA

W „stuleciu oprogramowania" o bezpieczeństwie państwa średniej wielkości nie przesądza liczba posiadanych platform, lecz to, kto kontroluje tory sterowania – dane, energię, oprogramowanie, produkcję, kadry i proces decyzji – oraz jak szybko państwo potrafi zamienić wiedzę w zdolność, a stratę w odtworzenie. Odpowiedzią nie jest autarkia ani zakupowy wyścig na liczbę platform, lecz sterowność pod kontrolą Narodu: druga droga dla każdej funkcji krytycznej, odstraszanie przez odporność, regenerację i produkcję oraz człowiek, który podpisuje regułę, zanim maszyna wykona impuls.

Co nowego w wydaniu 705

Wydanie 705 przenosi ustalenia książek 701–704 z poziomu ustroju, wyzwań cywilizacyjnych i reguł gospodarki na poziom **technologii bezpieczeństwa i suwerenności**. Oto najważniejsze nowości.

- **Bezpieczeństwo jako sterowność** (rozdział 1): sześć torów sterowania państwa i rodzina formuł iloczynowych, w której suwerenność mierzy się kosztem i czasem wyjścia z zależności.
- **Mapa dziesięciu mechanizmów bezpieczeństwa technologicznego** (rozdział 3): od uzbrojonej współzależności po nadzór człowieka, każdy z dowodem z korpusu, odpowiedzią TechnoRepubliki i miernikiem.
- **Dziewięć torów sterowania w szczegółach** (rozdziały 5–13), z nowymi dowodami: koncentracja surowców i mocy obliczeniowej, ataki na energetykę, kaskady infrastruktury, fałszowanie sygnałów nawigacyjnych, okno kryptograficzne, podatność agentów AI, deepfake i dane genomiczne.
- **Doktryna odstraszania przez odporność, regenerację i produkcję** (rozdziały 14–19) z wnioskami z teorii gier, gier wojennych, analiz pola walki i ekonomii obronności.
- **Certyfikowalna autonomia**: deterministyczny strażnik nad niedeterministycznym planistą jako techniczna postać zasady „człowiek podpisuje regułę, nie impuls" (rozdziały 16–17).
- **Indeks Suwerenności Bezpieczeństwa Technologicznego** (rozdział 24): osiem czynników łączonych średnią geometryczną, tak by zero w jednym zerowało wynik.
- **Sześć nowych bezpieczników** (31–36) uzupełnia trzydzieści bezpieczników z książek 701–704 (rozdział 26).
- **Rozważanie filozoficzne** (rozdział 28) o tym, co wynika z przyjęcia tezy o dominacji technologii w bezpieczeństwie i jak cybernetyka chroni przed jej ciemną stroną.
- **Agenda dwunastu kroków bez zmiany Konstytucji**, **dwanaście pytań obywatela** i **panel trzydziestu wskaźników** (rozdziały 30–32).

Skrót publikacji

Tabela 1. Skrót publikacji „TechnoRepublika – technologia bezpieczeństwa i suwerenności w dobie AI"

Pole	Treść
Pytanie	Czy Polska w erze AI, robotów autonomicznych i biotechnologii będzie państwem, które steruje własnym losem, czy państwem, którym da się sterować z zewnątrz?
Najkrótsza odpowiedź	Mapować tory sterowania, mieć drugą drogę dla każdej funkcji krytycznej, odtwarzać szybciej, niż przeciwnik niszczy, i podpisywać regułę, zanim maszyna wykona impuls.
Mechanizm	Technologia skraca pętlę rozpoznania, decyzji i działania, ale przenosi władzę na tego, kto kontroluje węzły: surowce, chipy, moc obliczeniową, energię, nawigację, klucze kryptograficzne, modele i dane. Bezpieczeństwo rośnie tam, gdzie państwo ma alternatywę, zapas czasu i zdolność odtworzenia.
Dziesięć mechanizmów	uzbrojona współzależność, koncentracja mocy obliczeniowej, kaskady infrastruktury, odporność energetyczna, wojna w spektrum, agenci AI jako powierzchnia ataku, kryptografia „zbieraj teraz, odszyfruj później", wojna poznawcza, baza przemysłowa, nadzór człowieka
Osiem czynników	różnorodność dróg (R), czas przełączenia (T), prawo decyzji (D), zgoda (Z), produkcja i regeneracja (P), energia (E), kryptografia (C), człowiek u steru (H); Indeks Suwerenności Bezpieczeństwa Technologicznego jako ich średnia geometryczna
Instytucje	Mapa Suwerenności Rzeczypospolitej z testem wyjścia, Cytadele energetyczno-cyfrowe, druga droga nawigacji i łączności, rejestr agentów AI i narodowy poligon testowy agentów, plan migracji kryptograficznej, Centrum Informacyjne Państwa z proweniencją komunikatów, Cyber-Rezerwa Narodowa, państwo pierwszym klientem dla technologii podwójnego zastosowania
Bezpieczniki	trzydzieści z książek 701–704 i sześć nowych: druga droga dla każdej funkcji krytycznej, zwinność kryptograficzna, strażnik deterministyczny i ciągłe testy agentów, zakup z planem odtworzenia, tajność z terminem i jawną wersją panelu, odporność bez cenzury
Konsekwencje	wzrost zdolności państwa, produktywności, suwerenności technologicznej oraz odporności społecznej i militarnej; usuwanie rent, władzy proceduralnej, zasiedziałych struktur, karteli i monopoli w sektorze bezpieczeństwa
Droga	dwanaście kroków 2026–2030 bez zmiany Konstytucji; mapa drogowa do 2035 roku; coroczny raport o suwerenności bezpieczeństwa dla parlamentu
Dla obywatela	dwanaście pytań obywatela o bezpieczeństwo i suwerenność, zasada 72 godzin samodzielności i panel trzydziestu wskaźników

Publikacja ma charakter programowy, analityczny i edukacyjny. Jest przeznaczona do debaty publicznej, eksperckiej i parlamentarnej. Nie stanowi obowiązującego prawa, opinii prawnej ani porady inwestycyjnej. Nie zawiera informacji niejawnych ani instrukcji technicznych umożliwiających ataki; omawia mechanizmy na poziomie potrzebnym do decyzji publicznych. Liczby z literatury ilustrują mechanizmy i nie są prognozami dla Polski; cytowane są tak, jak podają je źródła. Rysunki oznaczone jako „schemat" lub „wartości umowne" ilustrują modele, a nie pokazują pomiarów. Propozycje autora oznaczono w tekście jako propozycje. Zmiany wymagające zmiany Konstytucji RP są możliwe wyłącznie w trybie jej art. 235 i nigdy w czasie stanu nadzwyczajnego.

0. Streszczenie strategiczne

Punkt wyjścia. O bezpieczeństwie opowiada się zwykle językiem platform: ile czołgów, ile samolotów, ile baterii obrony powietrznej. Ta książka opowiada je inaczej, jako **zdolność sterowania**. Każda platforma zależy od torów, którymi płyną dane, energia, oprogramowanie, części, ludzie i decyzje. Kto kontroluje te tory, ten decyduje, czy platforma zadziała w godzinie próby. Dlatego w erze AI pytanie „ile mamy?" musi ustąpić pytaniu „co kontrolujemy i jak szybko odtworzymy funkcję po jej przecięciu?".

Trzy przesunięcia. Korpus BS pokazuje trzy przesunięcia, które zmieniają ramę bezpieczeństwa. **Po pierwsze, współzależność stała się bronią.** Kto kontroluje węzeł – rafinację galu, fabrykę chipów, klaster obliczeniowy, kabel podmorski, konstelację satelitów – ten może widzieć cudze przepływy albo je dławić. **Po drugie, odstraszanie przesuwa się z mocy zadawania strat na zdolność ich absorbowania i odtwarzania.** Tani dron i zakłócacz sygnału nawigacyjnego za kilka dolarów tworzą rachunek kosztów, w którym wygrywa ten, kto szybciej produkuje, naprawia i adaptuje. **Po trzecie, technologia bez kontroli Narodu zamienia sprawczość w nową zależność.** Agent AI, który działa szybciej niż człowiek, ale bez tożsamości, mandatu i monitora, jest uprzywilejowanym użytkownikiem bez nazwiska.

Polska na starcie. Diagnoza pokazuje państwo, które przeznacza na obronę ponad 4% PKB i buduje armię liczącą docelowo 300 tysięcy żołnierzy, co czyni je liderem wysiłku obronnego w Europie. To ogromny atut, ale też ryzyko opisane w Narodowej Strategii Bezpieczeństwa TechnoSanacji zdaniem: **„płacimy jak centrum, kupujemy jak peryferie"**. Bez krajowej wartości dodanej, krajowego serwisu i własnych torów danych wydatek nie staje się zdolnością suwerenną. W 2025 roku odnotowano w Polsce 2 732 incydenty fałszowania sygnałów nawigacji satelitarnej. Europejska luka kadrowa w cyberbezpieczeństwie przekracza 300 tysięcy osób. To nie powód do rezygnacji, tylko **mapa miejsc, w których dziś wycieka suwerenność**.

Tory sterowania. Wskazuję dziewięć torów, na których rozstrzyga się suwerenność ery AI: **surowce i łańcuchy dostaw** (uzbrojona współzależność), **moc obliczeniowa i modele**, **energia**, **kaskady infrastruktury krytycznej**, **spektrum, nawigacja i kosmos**, **kryptografia**, **agenci AI**, **przestrzeń informacyjna** i **dane o człowieku**. Dla każdego pokazuję dowód z literatury, odpowiedź TechnoRepubliki i miernik, którym obywatel może sprawdzić postęp.

Odstraszanie i produkcja. Teoria gier i gry wojenne prowadzą do jednego wniosku: **obrona statyczna przegrywa z adaptacyjnym napastnikiem**. W modelach ko-adaptacyjnych atakujący wygrywał 94% epizodów, gdy obrońca się nie uczył. Odpowiedzią jest dywersyfikacja, rozproszenie, rezerwa szybkiej realokacji, masa precyzji i baza przemysłowa, która odtwarza straty szybciej, niż przeciwnik je zadaje. Unia Europejska zwiększyła produkcję pocisków artyleryjskich z około 300 tysięcy rocznie w 2022 roku do około 2 milionów pod koniec 2025 roku, ale jej samowystarczalność komponentowa pozostaje poniżej połowy. Dlatego budżet obronny trzeba **rozliczać zdolnością**: głębokością magazynka, czasem odtworzenia i krajową wartością dodaną, a nie procentem PKB.

Człowiek u steru. AI skraca pętlę decyzji do milisekund, ale nie przejmuje odpowiedzialności. W takich pętlach człowiek nie może zatwierdzać każdego impulsu. **Człowiek podpisuje regułę**: zakres działania, progi i warunek wyłączenia. Techniczną postacią tej zasady jest **certyfikowalna autonomia**: deterministyczny strażnik bezpieczeństwa, sprzętowo odizolowany, nad niedeterministycznym planistą AI. Decyzja o użyciu siły wobec człowieka pozostaje w mandacie człowieka.

Odpowiedź. Proponuję architekturę, która **zamienia wydatek w zdolność, a zdolność w suwerenność pod kontrolą Narodu**. Jej rdzeń to: Mapa Suwerenności z corocznym testem wyjścia dla dwunastu funkcji krytycznych; druga droga nawigacji i łączności; Cytadele energetyczno-cyfrowe z pracą wyspową; rejestr i ciągłe testy agentów AI; plan migracji kryptograficznej; państwo jako pierwszy klient technologii podwójnego zastosowania z warunkiem krajowej wartości dodanej i otwartej architektury; Cyber-Rezerwa Narodowa; proweniencja komunikatów państwa. Zbieram ją w **Indeksie Suwerenności Bezpieczeństwa Technologicznego** – średniej geometrycznej ośmiu czynników, w której zero w jednym czynniku zeruje wynik.

Konsekwencje. Taka architektura podnosi **zdolność państwa** (sterowanie zamiast reagowania), **produktywność** (koło zamachowe technologii podwójnego zastosowania zamiast importu gotowych pakietów), **suwerenność technologiczną** (koszt i czas wyjścia zamiast hasła), **odporność społeczną** (obywatel przygotowany na 72 godziny samodzielności i zaufanie do komunikatów państwa) i **odporność militarną** (masa precyzji, głębia magazynka, krajowy serwis). Jednocześnie **usuwa renty, władzę proceduralną, zasiedziałe struktury administracyjne oraz kartele i monopole** w sektorze bezpieczeństwa, bo każdy zakup ma jawny miernik zdolności, a każdy przywilej – termin ważności.

Pierwszy krok. Nie wymaga zmiany Konstytucji. Proponuję dwanaście kroków na lata 2026–2030: od Mapy Suwerenności z testem wyjścia, drugiej drogi nawigacji i Cytadel energetyczno-cyfrowych, przez rejestr agentów AI i plan migracji kryptograficznej, po coroczny raport o suwerenności bezpieczeństwa dla parlamentu.



Rysunek 2. *Teza książki w jednym obrazie. Platformy działają tylko dzięki torom sterowania. O bezpieczeństwie decyduje to, kto kontroluje tory, czy państwo ma drugą drogę, jak szybko odtwarza funkcję po stracie i czy człowiek z mandatem podpisuje regułę działania maszyn. Schemat.*

RAMKA 0.1. Sześć zdań dla obywatela

1. Bezpieczeństwo w erze AI to nie suma platform, tylko zdolność sterowania własnym losem.

2. Kto kontroluje tory – dane, energię, oprogramowanie, produkcję, kadry i decyzję – ten kontroluje przyszłość państwa.

3. Suwerenność to nie autarkia, lecz koszt i czas wyjścia z każdej zależności.

4. Odstrasza państwo, które szybciej odtwarza straty, niż przeciwnik potrafi je zadać.

5. Maszyna może działać szybciej niż człowiek, ale to człowiek z mandatem podpisuje regułę jej działania.

6. Pierwszy krok nie wymaga zmiany Konstytucji: mapować tory, mieć drugą drogę, odtwarzać szybciej, podpisywać regułę.

CZĘŚĆ I. RAMA: BEZPIECZEŃSTWO JAKO STEROWNOŚĆ

Pierwsza część zmienia perspektywę. Zamiast pytać, ile mamy sprzętu, pytamy, co kontrolujemy i jak szybko odtworzymy funkcję po jej przecięciu. Opisuję sześć torów sterowania państwa, trzy przesunięcia ery AI, mapę dziesięciu mechanizmów bezpieczeństwa technologicznego i rachunek startowy Polski.

1. Stulecie oprogramowania: bezpieczeństwo jako sterowanie

1.1. Pytanie, które zmienia perspektywę

Gdy rozmawiam o bezpieczeństwie z samorządowcami, przedsiębiorcami i oficerami, prawie zawsze pada pytanie: *czego jeszcze nam brakuje?* Zwykle chodzi o sprzęt: więcej wyrzutni, więcej dronów, więcej amunicji. To uzasadnione pytanie, ale niepełne. Dwa państwa mogą wydać na obronę tę samą kwotę i osiągnąć zupełnie inne bezpieczeństwo. Pierwsze kupi systemy z prawem do modyfikacji oprogramowania, z krajowym serwisem, z zapasem części na pół roku i z danymi, które pozostają w jego rękach. Drugie kupi te same systemy jako zamknięte pakiety: każda aktualizacja, każda naprawa i każda zmiana parametrów będzie zależała od cudzej decyzji. Pierwsze zbudowało zdolność. Drugie kupiło zależność, która w godzinie próby może okazać się smyczą.

Dlatego proponuję inne pytanie: **kto kontroluje tory sterowania, od których zależy działanie naszych systemów, i ile czasu potrzebujemy, by odtworzyć funkcję, gdy któryś z nich zostanie przecięty?** To pytanie przenosi rozmowę z poziomu zakupów na poziom sterowania. A sterowanie, jak uczy cybernetyka, jest istotą każdego układu, który chce przetrwać w zmiennym otoczeniu.

Alex Karp i Nicholas Zamiska nazwali naszą epokę „stuleciem oprogramowania". Mają rację w jednym ważnym punkcie: przewaga przesunęła się z masy metalu na zdolność szybkiego tworzenia, poprawiania i wdrażania oprogramowania, które spina czujniki, decyzje i efektory w jeden organizm. Wojna w Ukrainie dostarczyła na to codziennych dowodów: dron, który tydzień temu był skuteczny, dziś jest bezużyteczny, bo przeciwnik zmienił częstotliwość zakłócania; tydzień później znów działa, bo zespół programistów zmienił algorytm. **Wygrywa ten, kto szybciej się uczy.**

1.2. Od mocy zadawania strat do mocy odtwarzania

Klasyczna teoria odstraszania, rozwinięta w epoce nuklearnej przez Thomasa Schellinga i Glenna Snydera, rozróżnia dwa mechanizmy. **Odstraszanie przez karę** grozi napastnikowi stratami większymi niż zysk. **Odstraszanie przez odmowę** przekonuje go, że nie osiągnie celu. Oba zakładają, że kluczowa jest zdolność zadawania strat lub ich unikania.

Korpus tej książki pokazuje trzeci mechanizm, który w erze AI staje się dla państwa średniej wielkości najważniejszy: **odstraszanie przez odporność, regenerację i produkcję**. Napastnik rezygnuje nie dlatego, że boi się kary, i nie tylko dlatego, że obrona jest szczelna, lecz dlatego, że widzi, iż każda strata, którą zada, zostanie odtworzona szybciej, niż on sam odbuduje własne zasoby. Państwo, które naprawia sieć energetyczną w godziny, produkuje drony w tysiącach tygodniowo, uczy operatorów w miesiące i przełącza łączność na drugą drogę w minuty, staje się celem, którego atak jest „nieopłacalny, nierozstrzygalny i politycznie samobójczy" – jak ujmuje to program Obrony Narodowej TechnoSanacji (301).

Narodowa Strategia Bezpieczeństwa TechnoSanacji (401) formułuje to tezą: **odstrasza państwo, które szybciej odtwarza straty**. Najdroższa broń to ta, której nie da się odtworzyć w czasie wojny. Odstraszanie przez odmowę wymaga więc nie tylko obrony warstwowej i redundancji, lecz także głębi magazynka i zdolności produkcyjnej.

1.3. Sześć torów sterowania

Każde państwo działa dzięki sześciu torom, którymi płynie jego zdolność do działania. Nazywam je **torami sterowania**, bo kto je kontroluje, ten może przyspieszyć, spowolnić albo zatrzymać działanie państwa.



Rysunek 3. *Sześć torów sterowania państwa. W centrum – zdolność państwa do rozpoznania, decyzji i działania; wokół – tory, którymi płyną dane, energia, oprogramowanie, produkcja, kadry i proces decyzji. Przy każdym torze pytanie kontrolne. Schemat.*

- **Tor danych** – informacje o stanie państwa, terytorium, przeciwnika, gospodarki i obywateli, a także modele, które z tych danych wyciągają wnioski. Pytanie kontrolne: *kto ma klucze do naszych danych i kto definiuje kategorie, w których je opisujemy?*
- **Tor energii** – prąd, paliwa i ciepło, bez których nie działa żaden czujnik, żaden serwer i żadna fabryka. Pytanie kontrolne: *ile dni obiekty krytyczne przetrwają w pracy wyspowej?*
- **Tor oprogramowania** – kod, który spina czujniki, łączność, broń i administrację, wraz z prawem do jego zmiany. Pytanie kontrolne: *czy możemy sami poprawić oprogramowanie systemu, gdy przeciwnik zmieni sposób działania?*
- **Tor produkcji** – zdolność wytwarzania, naprawy i odtwarzania sprzętu, amunicji i części. Pytanie kontrolne: *ile dni zapasu mamy i jak szybko odtworzymy stratę?*
- **Tor kadr** – ludzie, którzy rozumieją technologię, umieją ją obsłużyć, naprawić i ulepszyć. Pytanie kontrolne: *ile ról krytycznych możemy obsadzić w ciągu tygodnia?*
- **Tor decyzji** – proces, w którym państwo zamienia sygnał w decyzję i decyzję w działanie. Pytanie kontrolne: *ile godzin mija od sygnału do decyzji w kryzysie?*

Ta lista nie jest nowa w Bibliotece TechnoSanacji. Strategia wykorzystania AI (406) mówi o suwerenności torów danych, mocy obliczeniowej, energii i talentów; Narodowa Strategia Bezpieczeństwa – o sześciu suwerennych torach państwa. Nowe jest to, że korpus BS pozwala każdemu z tych torów przypisać **konkretny dowód, konkretną podatność i konkretny miernik**.

1.4. Sterowność zamiast autarkii

Słowo „suwerenność" bywa rozumiane jako samowystarczalność: wszystko ma być nasze, od kopalni po satelity. To złudzenie, i to niebezpieczne. Żadne państwo średniej wielkości nie wyprodukuje samodzielnie wszystkich półprzewodników, modeli bazowych AI, satelitów i surowców krytycznych. Próba autarkii kończy się albo bankructwem, albo technologicznym zacofaniem.

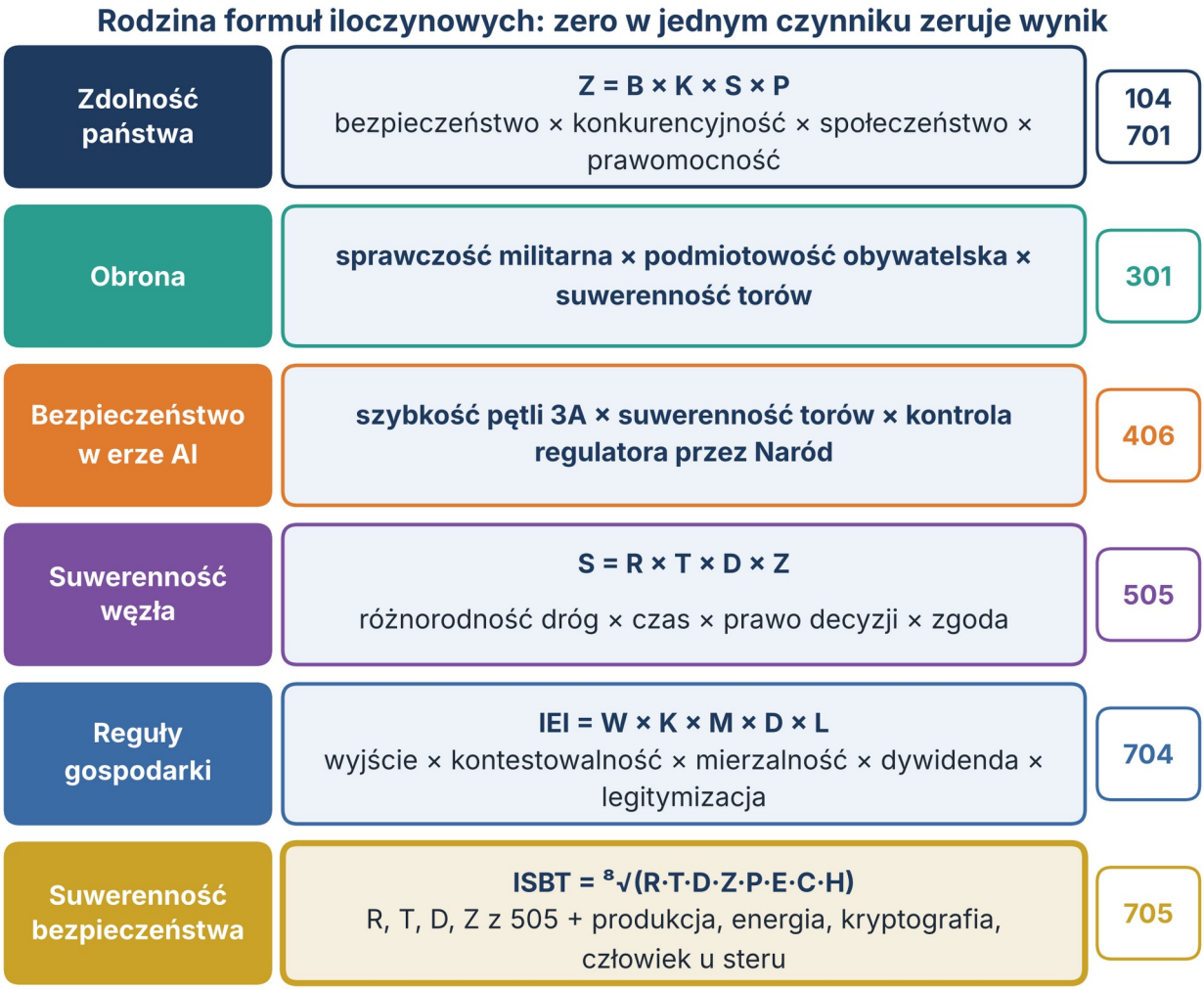
TechnoRepublika przyjmuje inną definicję, która powtarza się w całym kanonie TechnoSanacji: **suwerenność to sterowność, a nie samowystarczalność**. Państwo suwerenne ma zdolność wyboru, przełączenia i odtworzenia, a nie wszystko na własność. Miarą suwerenności jest więc **koszt i czas wyjścia z zależności**: ile kosztuje i ile trwa przejście do innego dostawcy, gwaranta albo technologii, gdy dotychczasowy przestaje być wiarygodny.

> **RAMKA 1.1. Suwerenność węzła – formuła Mapy Suwerenności (505)**
>
> Mapa Suwerenności Rzeczypospolitej ocenia każdy węzeł krytyczny iloczynem czterech czynników: **S = R × T × D × Z**.
>
> **R – różnorodność rozłącznych dróg:** czy funkcja ma co najmniej dwie niezależne drogi dostawy lub działania.
>
> **T – zapas czasu:** czy bufor (zapas, rezerwa, praca wyspowa) trwa dłużej niż przełączenie na drogę alternatywną.
>
> **D – prawo decyzji:** czy państwo posiada kategorie, klucze i logikę systemu, czy tylko z niego korzysta.
>
> **Z – zgoda:** czy obywatele rozumieją i popierają rozwiązanie, bo bez zgody żadna zdolność nie przetrwa długiego kryzysu.
>
> Zero w jednym czynniku zeruje całość. Węzeł z doskonałym zapasem, ale z jedną drogą dostawy, jest tak samo bezbronny jak węzeł z wieloma drogami, ale bez prawa decyzji.

Singapur, małe państwo o bardzo wysokiej zdolności strategicznej, świadomie zastąpił w swoich dokumentach słowo „suwerenność" pojęciem „przewagi strategicznej w łańcuchu wartości AI". To dokładnie ta sama myśl: nie chodzi o posiadanie wszystkiego, lecz o pozycję, z której nie da się nas łatwo wymanewrować.

1.5. Rodzina formuł iloczynowych

Biblioteka TechnoSanacji opisuje zdolność państwa formułami iloczynowymi. Iloczyn, a nie suma, bo **zero w jednym czynniku zeruje wynik**: państwo z najlepszą armią świata, ale bez zgody obywateli, nie obroni się w długim konflikcie; państwo z doskonałą technologią, ale bez kontroli nad kluczami, nie jest suwerenne.



Rysunek 4. *Rodzina formuł iloczynowych TechnoSanacji i miejsce publikacji 705. Od formuły zdolności państwa przez formuły obrony, bezpieczeństwa w erze AI i suwerenności węzła do Indeksu Suwerenności Bezpieczeństwa Technologicznego. Schemat.*

Tabela 2. Formuły iloczynowe kanonu wykorzystywane w książce 705

Formuła	Źródło	Co mierzy	Rola w 705
Zdolność państwa = bezpieczeństwo × konkurencyjność × społeczeństwo × prawomocność	Kontrakt Społeczny (104), książka 701	zdolność państwa jako iloczyn czterech celów	rama czterech celów ustroju (rozdział 27)
Obrona = sprawczość militarna × obywatelska podmiotowość × suwerenność torów	Obrona Narodowa (301)	zdolność obronną	uzasadnienie obrony totalnej i torów sterowania
Bezpieczeństwo w erze AI = szybkość pętli 3A × suwerenność torów × kontrola regulatora przez Naród	Strategia wykorzystania AI (406)	bezpieczeństwo w warunkach AI	rdzeń tezy trzeciej (rozdział 2)
Suwerenność węzła S = R × T × D × Z	Mapa Suwerenności (505)	suwerenność pojedynczego węzła	cztery pierwsze czynniki indeksu (rozdział 24)
Indeks Zdolności Republiki ery AI	książka 703	odporność ustroju	porównanie z indeksem 705
Indeks Ekonomii Instytucjonalnej AI = W × K × M × D × L	książka 704	uczciwość reguł gospodarki	czynnik wyjścia jako wspólny mianownik

Formuła	Źródło	Co mierzy	Rola w 705
Indeks Suwerenności Bezpieczeństwa Technologicznego	**propozycja 705**	sterowność państwa w technologiach bezpieczeństwa	rozdział 24

Formuła Strategii AI zasługuje na szczególną uwagę, bo jest kręgosłupem tej książki. Bezpieczeństwo jest w niej iloczynem trzech czynników: **szybkości pętli 3A** (antycypacji, absorpcji i adaptacji), **suwerenności torów** i **kontroli regulatora przez Naród**. Trzeci czynnik nie jest ozdobą demokratyczną. Jest warunkiem matematycznym: państwo, którego regulator wymknął się spod kontroli obywateli, zamienia własną szybkość i własne tory w narzędzie, które może zostać zwrócone przeciw nim.

2. Trzy przesunięcia ery AI

2.1. Teza w trzech członach

Teza tej książki ma trzy człony i każdy z nich korpus BS potwierdza dowodami. Pokazuję je razem, bo dopiero razem tworzą obraz.



Rysunek 5. *Trzy przesunięcia ery AI w bezpieczeństwie: od zależności do uzbrojonej współzależności, od mocy zadawania strat do mocy odtwarzania, od sprawczości technologii do sprawczości pod kontrolą Narodu. Przy każdym – dowód z korpusu i odpowiedź TechnoRepubliki. Schemat.*

2.2. Pierwsze przesunięcie: współzależność jest bronią

Przez trzy dekady po zakończeniu zimnej wojny Europa wierzyła, że handel i współzależność czynią wojnę nieopłacalną. Wiara ta miała solidne podstawy, ale zapomniała o jednym: **współzależność jest symetryczna tylko na papierze**. W rzeczywistości ten, kto kontroluje węzeł sieci, może z niej korzystać jak z broni.

Przed 2022 rokiem Europa zależała od Rosji w około 40% dostaw gazu. Przetwarzanie galu, metalu niezbędnego do produkcji radarów, układów mocy i elektroniki wojskowej, jest w 98% skoncentrowane w Chinach. Prawie trzy czwarte zaawansowanych klastrów obliczeniowych AI w połowie 2025 roku leżało w Stanach Zjednoczonych, a około 14% w Chinach. Tajwan i Korea Południowa odpowiadają za około 35% światowego handlu półprzewodnikami. To nie są abstrakcyjne statystyki. To są **dźwignie**, którymi można zmusić państwo do ustępstw bez jednego wystrzału.

Henry Farrell i Abraham Newman opisali ten mechanizm pojęciem **uzbrojonej współzależności**. Węzeł sieci daje kontrolującemu dwie zdolności: **efekt panoptikonu** (widzenie przepływów przechodzących przez węzeł) i **efekt wąskiego gardła** (zdolność ich zdławienia). Wniosek dla państwa średniej wielkości jest prosty: **suwerenność nie jest autarkią, lecz kosztem i czasem wyjścia z zależności**.

2.3. Drugie przesunięcie: odstraszanie przez odporność, regenerację i produkcję

Rosyjskie ataki na ukraińską energetykę obniżyły funkcjonalność sektora o 61%, a dostępną moc z około 36 gigawatów do 13,9 gigawata. W każdej klasycznej analizie taki cios powinien sparaliżować państwo. Nie sparaliżował. Ukraina naprawiała, rozpraszała generację, budowała magazyny energii, importowała moc z Europy, uczyła obywateli żyć z przerwami w dostawach i jednocześnie produkowała drony w skali, jakiej świat nie widział.

Po drugiej stronie rachunku stoją tanie środki ataku. Korpus odnotowuje zakłócacz sygnału nawigacyjnego kosztujący około 8 dolarów, zdolny do zakłócenia systemów wartych wielokrotnie więcej. Dron za kilkaset dolarów niszczy pojazd wart miliony. **Asymetria kosztów** oznacza, że obrońca, który odpowiada na każdy tani atak drogim środkiem, przegra wojnę na wyczerpanie, nawet jeśli wygra każde starcie.

Wniosek: **wygrywa ten, kto szybciej produkuje, naprawia i adaptuje**. To jest empiryczne uzasadnienie doktryny odstraszania przez odporność, regenerację i produkcję, którą Narodowa Strategia Bezpieczeństwa TechnoSanacji przyjęła jako koncepcję strategiczną.

2.4. Trzecie przesunięcie: technologia bez kontroli zamienia sprawczość w zależność

Agenci AI – programy, które samodzielnie wyszukują, analizują, uruchamiają narzędzia i wykonują działania – wchodzą do administracji, wojska i infrastruktury krytycznej. Obiecują ogromne przyspieszenie. Ale korpus pokazuje, że są dziś bardzo podatni. W badaniu systemu produkcyjnego **67% agentów naruszało zakres swoich uprawnień** co najmniej jednym sposobem, a **pośrednia iniekcja poleceń** – czyli podsunięcie agentowi złośliwej instrukcji ukrytej w treści, którą przetwarza – **skutkowała w 43% prób**. Gdy modele językowe analizowały dzienniki zdarzeń sieciowych, średnia skuteczność ataków przez skażenie kontekstu sięgała 83,4%.

Formuła Bezpieczeństwa w erze AI jest multiplikatywna: **szybkość pętli 3A × suwerenność torów × kontrola regulatora przez Naród**. Zero w trzecim czynniku zeruje dwa pierwsze. Państwo, które wpuści do swoich systemów szybkich agentów bez tożsamości, mandatu i monitora, zwiększy szybkość, ale odda sterowanie.

RAMKA 2.1. Trzy przesunięcia w trzech zdaniach

1. Kto kontroluje węzeł, ten może widzieć i dławić – dlatego suwerenność mierzy się kosztem i czasem wyjścia.

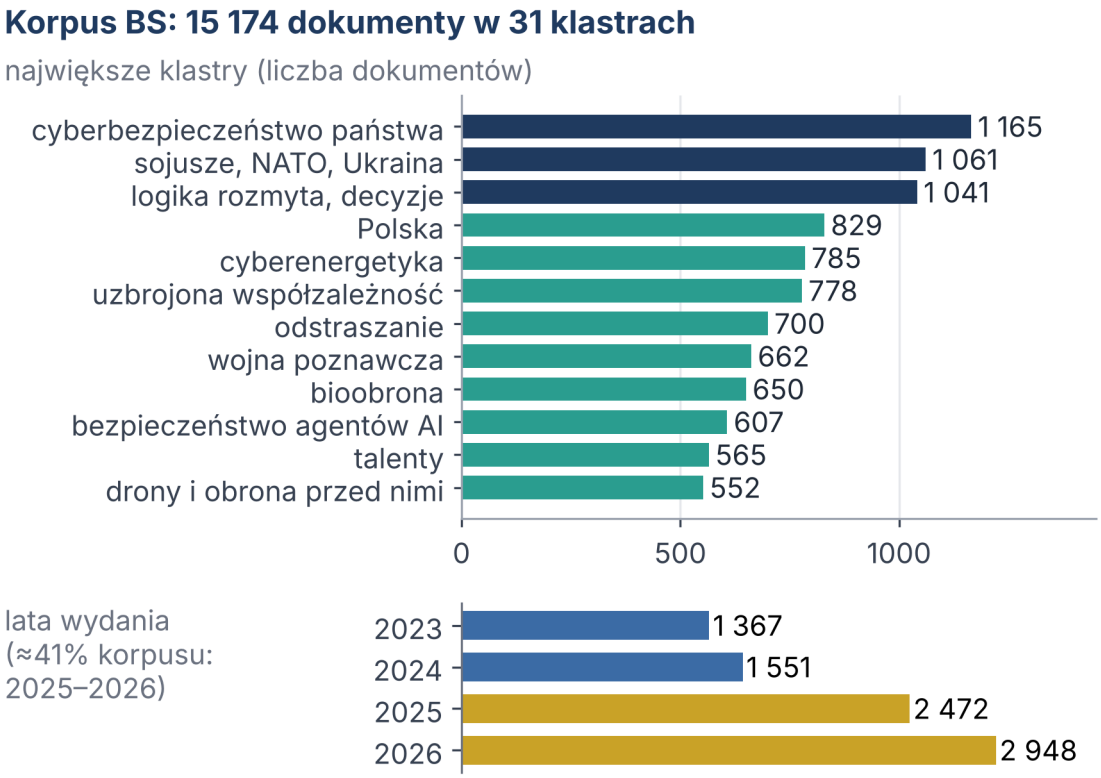
2. Kto szybciej odtwarza straty, ten odstrasza – dlatego budżet rozlicza się zdolnością regeneracji, a nie liczbą platform.

3. Kto wpuszcza maszyny bez mandatu, ten oddaje sterowanie – dlatego człowiek podpisuje regułę, zanim maszyna wykona impuls.

3. Mapa dziesięciu mechanizmów bezpieczeństwa technologicznego

3.1. Jak powstała mapa

Runda badawcza BS przejrzała ponad 42 tysiące kandydatów z OpenAlex, Crossref, Semantic Scholar, arXiv, DOAJ, Zenodo i szarej literatury. Po odrzuceniu pozycji już obecnych w Bibliotece i po filtrze tematycznym wybrano 28 400 pozycji, a otwarty tekst miało 14 832 prac naukowych. Po dodaniu 360 dokumentów szarej literatury (raporty SIPRI, Parlamentu Europejskiego, ośrodków analitycznych) i 14 nowych aktów prawnych oraz po usunięciu 277 powtórzeń korpus liczy **15 174 dokumenty** w 31 klastrach tematycznych. Około 41% korpusu pochodzi z lat 2025–2026.



Rysunek 6. *Korpus BS w liczbach: liczba dokumentów w największych klastrach tematycznych oraz struktura czasowa korpusu (2023–2026). Dane: manifest rundy BS.*

Ten rozkład jest sam w sobie wnioskiem. **Nauka bardzo obficie bada cyberbezpieczeństwo państwa (1165 dokumentów), sojusze i wojnę w Ukrainie (1061), metody decyzji rozmytych (1041) i uzbrojoną współzależność (778), ale znacznie skromniej suwerenną AI (25 dokumentów, przy czym wiele prac z tej dziedziny było już w Bibliotece z wcześniejszych rund) i formalną weryfikację procedur kryzysowych (15).** To asymetria, którą

zauważyłem już w książkach 703 i 704: nauka bada zagrożenia i ataki znacznie lepiej niż instytucje, które mają się im przeciwstawić. Projekt TechnoRepubliki musi wypełnić tę lukę.

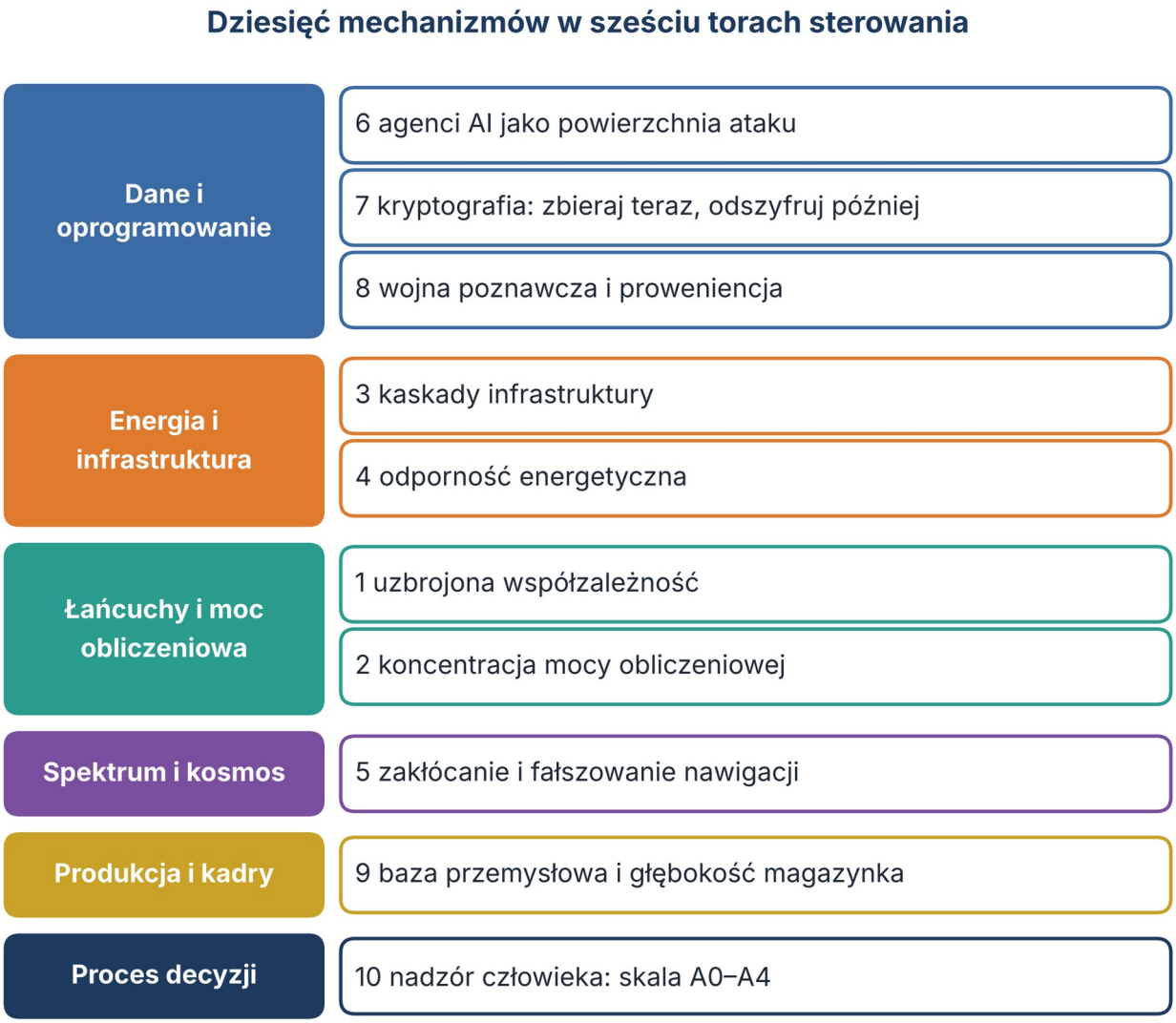
3.2. Dziesięć mechanizmów w jednej tabeli

Z korpusu wyodrębniłem dziesięć mechanizmów, przez które technologia rozstrzyga o bezpieczeństwie i suwerenności. Dla każdego podaję dowód z literatury, odpowiedź TechnoRepubliki i miernik.

Tabela 3. Dziesięć mechanizmów bezpieczeństwa technologicznego: dowód, odpowiedź, miernik

Nr	Mechanizm	Dowód z korpusu	Odpowiedź TechnoRepubliki	Miernik
1	Uzbrojona współzależność (widzenie i dławienie przez węzeł)	98% przetwarzania galu w Chinach; Tajwan i Korea – ok. 35% handlu półprzewodnikami; co najmniej 28 państw ma mechanizmy kontroli inwestycji zagranicznych	druga droga (najwyżej 65–70% zależności od jednego dostawcy), suwerenność mierzona kosztem i czasem wyjścia, Mapa Suwerenności	udział największego dostawcy; koszt i czas wyjścia
2	Koncentracja mocy obliczeniowej	ok. ¾ zaawansowanych klastrów AI w USA, ok. 14% w Chinach; kryzys energetyczny podniósł koszt energii o ok. 30% w 2022 r.	suwerenność od środka i góry stosu (dane, adaptacja modeli, ewaluacje, energia), Operator Suwerennej Chmury	% krytycznych obciążeń na suwerennej mocy obliczeniowej
3	Kaskady infrastruktury	Ukraina: −61% funkcjonalności energetyki, 36 → 13,9 GW; ok. 85% infrastruktury krytycznej w rękach prywatnych (USA)	Sieciowy Bliźniak Rzeczypospolitej, praca wyspowa 7/14/30 dni, rozruch od zera (*black start*)	czas przywrócenia funkcji
4	Odporność energetyczna	program mikrosieci zakłada skrócenie przerw zasilania obciążeń krytycznych o 98%; mikrosieć bazy wojskowej pokrywa ok. 50% obciążenia	Cytadele energetyczno-cyfrowe, falowniki tworzące sieć, magazyny energii	% obciążeń krytycznych z zasilaniem wyspowym
5	Wojna w spektrum (zakłócanie i fałszowanie nawigacji)	Polska: 2 732 incydenty fałszowania sygnału w 2025 r.; Litwa – 22-krotny wzrost; Estonia – do 85% lotów dotkniętych	nawigacja odporna na zakłócenia (naziemna radionawigacja, zegary, fuzja inercyjna), IRIS² jako uzupełnienie	% systemów krytycznych z alternatywną nawigacją i czasem
6	Agenci AI jako powierzchnia ataku	67% agentów narusza zakres; 43% skuteczności iniekcji pośredniej; obrony obniżają skuteczność ataków do ok. 8–9%	zasada zerowego zaufania dla agentów, tożsamość i mandat, izolacja kontekstu, monitor, wyłącznik	skuteczność ataków w testach poligonu agentów

Nr	Mechanizm	Dowód z korpusu	Odpowiedź TechnoRepubliki	Miernik
7	Kryptografia „zbieraj teraz, odszyfruj później”	migracja w dużej organizacji 12–15 lat wobec prognozy komputerów kwantowych 2028–2030; tylko 6% narzędzi centrów operacji bezpieczeństwa parsuje nowe protokoły	zwinność kryptograficzna, inwentarz kryptograficzny, plan migracji	% systemów krytycznych z kryptografią postkwantową lub hybrydową
8	Wojna poznawcza	ludzie wykrywają podrobione nagrania głosu w 73% przypadków; przelew 25 mln USD po rozmowie z fałszywym „dyrektorem finansowym”	podpis proweniencji komunikatów państwa, uodparnianie wyprzedzające, Centrum Informacyjne Państwa	% komunikatów państwa z podpisem proweniencji
9	Baza przemysłowa	produkcja amunicji UE: ok. 300 tys. pocisków (2022) → ok. 2 mln (koniec 2025); samowystarczalność komponentowa poniżej 50%	krajowa wartość dodana ≥ 50%, otwarta architektura, krajowy serwis, państwo pierwszym klientem	krajowa wartość dodana; głębokość magazynka 30/90/180 dni
10	Nadzór człowieka	rekomendacja AI z deklarowaną 99% pewnością może zwiększać skłonność dowódców do ryzyka	ocena przed rekomendacją (*blind-first*), skala autonomii A0–A4, zakaz pełnej autonomii w użyciu siły	rozkład nadpisań; % funkcji z ćwiczonym trybem pracy bez AI



Rysunek 7. *Dziesięć mechanizmów bezpieczeństwa technologicznego przypisanych do sześciu torów sterowania. Każdy mechanizm ma dowód, odpowiedź i miernik. Schemat.*

3.3. Sześć bloków i jedna oś

Dziesięć mechanizmów układa się w sześć bloków tematycznych, które odpowiadają kolejnym częściom tej książki: odstraszanie i dynamika konfliktu; pole walki w erze oprogramowania; suwerenność przemysłowo-technologiczna; odporność cyberfizyczna i cyfrowa; odporność społeczna i tor informacyjny; metody decyzji pod niepewnością i nadzór nad AI. **Oś, która je łączy, to czas.** Każdy mechanizm można opisać jako wyścig dwóch zegarów: zegara zagrożenia (jak szybko przeciwnik może przeciąć tor) i zegara odpowiedzi (jak szybko państwo może go odtworzyć lub obejść). Suwerenność to sytuacja, w której zegar odpowiedzi jest szybszy.

4. Polska na starcie: rachunek bezpieczeństwa technologicznego

4.1. Lider wysiłku, uczeń w konwersji

Polska przeznaczyła na obronę w 2024 roku ponad 4% PKB i realizuje program rozbudowy sił zbrojnych do 300 tysięcy żołnierzy. Literatura z korpusu określa ją jako lidera inwestycji obronnych w Europie. Profesjonalizacja przekroczyła połowę stanu sił zbrojnych przy utrzy-

Czy Polska będzie sterować własnym losem – czy da się nią sterować z zewnątrz?

W erze AI, robotów autonomicznych i biotechnologii o bezpieczeństwie nie przesądza liczba posiadanych platform, lecz to, kto kontroluje tory sterowania: dane, energię, oprogramowanie, produkcję, kadry i proces decyzji. Odstrasza państwo, które szybciej odtwarza straty, niż przeciwnik je zadaje.

Dr Andrzej Węgrzyn pokazuje, gdzie dziś wycieka suwerenność – w łańcuchach surowców i chipów, w mocy obliczeniowej, w energetyce, w spektrum nawigacji, w kryptografii i w agentach AI – oraz jak ją odzyskać. Proponuje Indeks Suwerenności Bezpieczeństwa Technologicznego, drugą drogę dla każdej funkcji krytycznej, Cytadele energetyczno-cyfrowe, certyfikowalną autonomię i zasadę: człowiek podpisuje regułę, nie impuls.

10 mechanizmów bezpieczeństwa	**9** torów sterowania w szczegółach
36 bezpieczników ustrojowych	**12** pytań obywatela
30 wskaźników w panelu	**45** rysunków, map i infografik

Mapować tory · mieć drugą drogę · odtwarzać szybciej · podpisywać regułę



O autorze

Dr Andrzej Węgrzyn jest autorem Biblioteki TechnoSanacji oraz serii TechnoRepubliki: o konieczności cywilizacyjnej ery AI (701), o architekturze ustrojowej wobec zagrożeń AI (702), o odpowiedzi na wyzwania cywilizacyjne AI (703) i o ekonomii instytucjonalnej AI (704). Pisze z perspektywy inżyniera i obywatela o tym, jak zamienić wydatek w zdolność, a zdolność w suwerenność.

Biblioteka TechnoSanacji nr 705 · Wydanie I · 2026
© dr Andrzej Węgrzyn · wszelkie prawa zastrzeżone