

Obrona Narodowa Rzeczypospolitej



Projekt obrony narodowej TechnoRepubliki opartego o technologię i obywateli

Obrona Narodowa Rzeczypospolitej

National Defense = sprawczość militarna × obywatelska podmiotowość × suwerenność zasobów



**NARÓD
I SPOŁECZNOŚĆ**



Gemini Notebook

Formuła naczelną

Obroną Polski jest zdolność Narodu do samodzielnego przetrwania, odstraszenia i zwyciężania — osiągnięta przez sprawcze państwo z regulatorem, obywatelski system obrony, wojsko nowego wzoru, suwerenną technologię, odporność energetyczną oraz zaawansowaną produkcję militarną i dual use.

Spis treści:

Formuła naczelna

I. Przestanki założycielskie

II. Cel strategiczny i doktryna obronna

III. Uzasadnienie formuły naczelnej

IV. Model cybernetyczny: państwo z regulatorem

V. Pięć linii wysiłku strategicznego

VI. Zakotwiczenie ustrojowe

VII. Architektura siedmiu warstw obrony

VIII. System Górskich Cytadel

IX. Zasady wdrożenia

X. Dziesięć haseł Narodowej Obrony TechnoRepubliki

XI. Konkluzja

Aneks A. Słownik pojęć, terminów i skrótów

Załącznik B. Bibliografia

Obrona nie jest wyłącznie zadaniem wojska. Jest funkcją całego państwa, całego społeczeństwa i całej gospodarki. TechnoRepublika rozumie obronę jako system połączonych torów: danych, energii, software'u, produkcji, infrastruktury, ludzi, rezerw, terytorium i decyzji. Jeżeli którykolwiek z tych torów zostanie przejęty, przerwany albo sparaliżowany, suwerenność państwa staje się pozorna.

Dlatego Obrona Narodowa opiera się na formule:

**Obrona Narodowa = sprawczość militarna × obywatelska podmiotowość
× suwerenność torów danych, energii, software'u i produkcji.**

Jest to obrona sprawcza, ekonomicznie racjonalna i demokratycznie kontrolowana. Nie jest to militarizm bez rozliczalności. Nie jest to państwo koszarowe. Jest to system odpowiedzi strategicznej na główne zagrożenia XXI wieku: wojnę konwencjonalną, presję nuklearną, sabotaż infrastruktury, cyberatak, operacje informacyjne, terroryzm, kryzysy energetyczne, pandemie, paraliż logistyczny oraz turbulencje geostrategiczne.

Obowiązek obrony ojczyzny, zapisany jako obowiązek obywatela w projekcie nowej Konstytucji Rzeczypospolitej, staje się w tej doktrynie nie tylko powinnością wojskową, lecz także prawem do uczestnictwa w bezpieczeństwie państwa: przez szkolenie, rezerwy, kompetencje technologiczne, obronę cywilną, odporność lokalną, gotowość energetyczną i ochronę wspólnoty.

I. Przestanki założycielskie

1. Polska jako państwo centralne Europy

Polska nie jest peryferią Zachodu ani buforem między cudzymi imperiami. Jest państwem centralnym Europy Środkowej, położonym na styku głównych osi strategicznych kontynentu: Bałtyku, wschodniej flanki NATO, korytarzy północ-południe, osi Odra-Wisła-Bug, przesmyku suwalskiego, Karpat, Sudetów oraz korytarzy transportowych łączących porty, energetykę, przemysł i zaplecze sojusznicze.

To położenie jest zarazem szansą i ryzykiem. Polska może być rdzeniem europejskiej odporności albo polem manewru cudzych strategii. Rzeczpospolita wybiera pierwszą drogę: budowę centralnego państwa frontowego wysokiej sprawczości.

2. Zmiana charakteru wojny

Wojna XXI wieku nie jest już wyłącznie starciem dywizji pancernych. Jest wojną systemów. O wyniku decydują: rozpoznanie, dane, drony, rakiety, satelity, cyberprzestrzeń, odporność społeczeństwa, produkcja amunicji, energia, zdolność do naprawy infrastruktury i szybkość adaptacji.

Pole walki stało się przejrzyste. Tania precyzja niszczy drogie platformy. Drony i amunicja krążąca zmieniają ekonomię wojny. Cyberatak może sparaliżować administrację, bankowość, energetykę i logistykę. Dezinformacja może rozbić wolę społeczną szybciej niż atak kinetyczny. Przeciwnik uderza nie tylko w żołnierza, ale w sensor, kabel, satelitę, aplikację, magazyn, stację transformatorową, narrację i zaufanie społeczne.

3. Teza Karp–Zamiska: software i AI jako hard power

Nowoczesna siła państwa nie wynika już tylko z liczby czołgów, samolotów i okrętów. Wynika z połączenia technologii, oprogramowania, sztucznej inteligencji, danych, przemysłu i kultury strategicznej.

Rzeczpospolita przyjmuje zasadę: **software, AI i dane są twardą siłą państwa**. Państwo, które nie kontroluje własnych danych, nie rozumie własnego pola walki. Państwo, które nie posiada własnych systemów dowodzenia, nie ma krótkiej pętli decyzyjnej. Państwo, które nie produkuje krytycznych komponentów, nie odstrasza — tylko deklaruje odstraszenie.

4. Wojsko nowego wzoru

Klasyczny model armii zawodowej nie wystarcza. Nie oznacza to prostego odrzucenia profesjonalnego wojska, lecz jego radykalne przeprojektowanie. TechnoRepublika potrzebuje wojska nowego wzoru: mniejszej liczby struktur pozornych, większej liczby zdolności realnych; mniej hierarchicznego rytuału, więcej odpowiedzialności zadaniowej; mniej platform prestiżowych, więcej taniej masy precyzji, rezerw, dronów, rakiet, systemów C4ISR, cyberobrony, obrony powietrznej i przygotowanych obywateli.

II. Cel strategiczny i doktryna obronna

Celem Obrony Narodowej jest uczynienie agresji na Polskę:

nieoptymalną, nierozstrzygalną i politycznie samobójczą dla każdego przeciwnika.

Doktryna opiera się na czterech mechanizmach odstraszenia.

1. Odstraszenie przez odmowę

Przeciwnik nie może uznać, że szybki atak doprowadzi do przełamania państwa. Polska ma być państwem, którego nie da się sparaliżować jednym uderzeniem, zdobyć jednym manewrem ani zaszantażować jednym kryzysem. Służy temu warstwowa obrona powietrzna, obrona przeciwrakietowa, counter-UAS, rozproszenie infrastruktury, schrony, rezerwy, redundancja energetyczna, odporne centra danych i obywatelski system obrony.

2. Odstraszanie przez karanie

Rzeczpospolita musi posiadać wiarygodną zdolność do odpowiedzi na agresję: przez długodystansowe ognie, rakiety, drony uderzeniowe, zdolności cybernetyczne, środki precyzyjnego rażenia i zdolności zakłócania systemu przeciwnika. Zdolność karania nie oznacza awanturnictwa. Oznacza, że agresor wie, iż koszt napaści przekroczy każdy możliwy zysk.

3. Odporność jako odstraszanie

Jeżeli społeczeństwo, administracja, energetyka, łączność, służba zdrowia, transport i samorządy działają mimo presji, przeciwnik traci nadzieję na szybkie złamanie państwa. Odporność jest formą odstraszania, bo odbiera sens uderzeniu. Państwo odporne nie musi być państwem agresywnym. Wystarczy, że jest państwem trudnym do złamania.

4. Produkcja jako odstraszanie

Zaawansowana technologicznie produkcja militarna i dual use jest częścią doktryny obronnej. Amunicja, rakiety, drony, sensory, systemy łączności, energetyka, komponenty elektroniczne, software i zaplecze naprawcze nie są dodatkiem do strategii. Są jej rdzeniem.

Produkcja jest odstraszaniem

Państwo, które może szybko odtworzyć straty, adaptować konstrukcje, skalować produkcję i uczyć się szybciej od przeciwnika, staje się trudne do pokonania.

5. Zwyciężanie jako miara trzecia

Odstraszanie odpowiada na pytanie, jak nie dopuścić do wojny. Odporność odpowiada na pytanie, jak przetrwać jej pierwszy okres. Pozostaje pytanie trzecie: co znaczy wygrać. Doktryna, która go nie stawia, planuje trwanie, a nie rozstrzygnięcie.

Zwycięstwo państwa broniącego się nie polega na zdobyczu terytorialnej. Polega na doprowadzeniu agresora do stanu, w którym kontynuowanie wojny jest dla niego droższe niż jej zakończenie na warunkach akceptowalnych dla Polski, przy jednoczesnym zachowaniu zdolności państwa do funkcjonowania po konflikcie. Wymaga to zdolności do wojny długiej: zapasów i produkcji liczonych w miesiącach, rezerw kadrowych, finansów wojennych, ochrony zdrowia i logistyki cywilnej. Wymaga też zdolności oddziaływania na kalkulację przeciwnika w trakcie konfliktu — sterowania eskalacją, wiarygodnego rażenia w głąb oraz oddziaływania informacyjnego i gospodarczego.

Trzecim warunkiem zwycięstwa jest zdolność odbudowy. Państwo, które przetrwało uderzenie i zniechęciło agresora, lecz nie potrafi odtworzyć energetyki, łączności, transportu i administracji, przegrywa pokój po wygranej wojnie. Dlatego odbudowa jest w TechnoRepublice planowana przed wojną, a nie po niej: jako zapasowe węzły, rezerwy materiałowe, zdolności naprawcze, kadry inżynierskie i gotowe procedury uruchamiania funkcji państwa od nowa.

III. Uzasadnienie formuły naczelnej

Formuła naczelna nie jest hasłem politycznym. Jest twierdzeniem o warunkach koniecznych obrony państwa średniej wielkości położonego na głównej osi zagrożenia w centralnej Europie. Twierdzenie to daje się uzasadnić czterema niezależnymi drogami dowodowymi: cybernetyczną, systemową, sieciową i militarną. Każda z tych dróg wychodzi z innych przesłanek i posługuje się innym aparatem pojęciowym, a mimo to prowadzi do tego samego wniosku o strukturze obrony. Zbieżność czterech niezależnych uzasadnień jest najmocniejszym argumentem, jakim może dysponować doktryna: to, co wynika z jednej teorii, bywa artefaktem tej teorii; to, co wynika z czterech teorii naraz, jest własnością rzeczywistości.

Rozdział niniejszy przeprowadza te cztery dowody, wskazuje warunki, w których formuła byłaby fałszywa, oraz podaje mierniki pozwalające sprawdzić, czy państwo faktycznie ją realizuje. Doktryna, której nie da się obalić, nie jest doktryną — jest wyznaniem wiary. Rzeczpospolita przyjmuje odwrotną zasadę: każdy człon formuły ma swoją miarę i swój próg falsyfikacji.

1. Rozbiór formuły: trzy miary i sześć członów

Formuła naczelna składa się z dwóch części. Pierwsza określa, czym obrona jest — wskazuje przedmiot i trzy miary jego sprawdzenia. Druga określa, przez co obrona jest osiągnięta — wskazuje sześć członów wykonawczych.

Część pierwsza:

zdolność Narodu do samodzielnego przetrwania, odstraszenia i zwyciężania.

Obrona zostaje zdefiniowana jako zdolność, a nie jako zasób, instytucja ani wydatek. Zdolność jest kategorią sprawdzalną: mierzy się ją zachowaniem układu pod obciążeniem, a nie deklaracją ani stanem ewidencyjnym. Podmiotem tej zdolności jest Naród, a nie resort — obrona jest funkcją wspólnoty politycznej, w której wojsko jest narzędziem wyspecjalizowanym, lecz nie jedynym. Przymiotnik „samodzielnego” wyznacza próg suwerenności: zdolność, która działa wyłącznie pod warunkiem cudzej zgody, cudzego zasilania lub cudzego oprogramowania, jest zdolnością pozorną. Sojusz wzmacnia zdolność własną; nie zastępuje jej.

Trzy miary tworzą rosnącą skalę wymagań. Przetrwanie oznacza, że państwo pod uderzeniem nadal widzi, decyduje, komunikuje się, zasila i rządzi. Odstraszenie oznacza, że przeciwnik przed uderzeniem szacuje koszt jako przekraczający możliwy zysk. Zwyciężanie oznacza, że państwo potrafi doprowadzić konflikt do zakończenia na własnych warunkach politycznych. Trzecia miara jest najtrudniejsza i najczęściej pomijana w dokumentach obronnych: łatwiej zaplanować przetrwanie niż zdefiniować, co znaczy wygrać.

Część druga: **sześć członów wykonawczych.**

- 1) sprawcze państwo z regulatorem — wyodrębniony, kompetentny i rozliczalny podsystem sterowania obroną,
- 2) obywatelski system obrony — powszechna, przeszkolona i zorganizowana partycypacja obywateli,
- 3) wojsko nowego wzoru — siły zbrojne zaprojektowane wokół efektu, a nie wokół struktury etatowej,
- 4) suwerenna technologia — kontrola danych, oprogramowania, modeli, łączności, kosmosu i kluczy,
- 5) odporność energetyczna — zdolność zasilania obrony, danych i gospodarki mimo zakłóceń,
- 6) zaawansowana produkcja militarna i dual use — zdolność wytwarzania i odtwarzania środków walki.

Formuła twierdzi, że sześć członów jest zbiorem warunków koniecznych, a nie listą życzeń o dowolnych wagach. Usunięcie któregośkolwiek członu nie osłabia obrony proporcjonalnie — likwiduje ją w jednej z trzech miar. Państwo bez regulatora może mieć wojsko, lecz nie ma decyzji. Państwo bez energii może mieć dane, lecz nie ma ich przetwarzania. Państwo bez produkcji może mieć zapasy, lecz nie ma odtworzenia. To jest właśnie treść dowodu przeprowadzonego niżej.

2. Uzasadnienie cybernetyczne

Cybernetyka jest nauką o sterowaniu i komunikacji w układach złożonych. Jej twierdzenia nie zależą od tego, czy układem jest organizm, przedsiębiorstwo, czy państwo prowadzące wojnę. Dlatego dostarcza najmocniejszego, bo najbardziej ogólnego uzasadnienia formuły.

2.1. Twierdzenie o dobrym regulatorze

Ronald Conant i W. Ross Ashby dowiedli w 1970 roku, że każdy dobry regulator układu musi być modelem tego układu. Twierdzenie to ma dla obrony konsekwencję bezwzględną: państwo może sterować tylko tym fragmentem rzeczywistości, który odwzorowuje. Jeżeli państwo nie ma aktualnego modelu własnej infrastruktury krytycznej, własnych zapasów, własnego pola walki i własnego społeczeństwa, to nie steruje obroną — reaguje na doniesienia.

Model rzeczywistości nie jest metaforą. W obronie ma postać techniczną: rozpoznanie satelitarne, dronowe i naziemne, fuzja danych, rejestry zdolności i zapasów, obraz stanu energetyki, łączności, transportu i służb, ciągła ocena sytuacji społecznej i informacyjnej. Stąd bierze się człon „suwerenna technologia”: model rzeczywistości zbudowany na cudzych sensorach, cudzych chmurach i cudzych modelach jest modelem, którego właścicielem jest ktoś inny.

2.2. Prawo wymaganej różnorodności

Prawo Ashby'ego stanowi, że tylko różnorodność może pochłoniąć różnorodność: regulator musi dysponować repertuarem odpowiedzi nie mniejszym niż repertuar zakłóceń, którym podlega. Przeciwnik XXI wieku dysponuje repertuarem obejmującym uderzenie konwencjonalne, presję nuklearną, saturację dronową, sabotaż infrastruktury, cyberatak, operacje informacyjne, presję migracyjną, energetyczną, finansową i prawną, dywersję oraz zakłócanie nawigacji i łączności.

Z prawa wymaganej różnorodności wynika wprost wielodomenowość obrony oraz — co ważniejsze — wielopodmiotowość. Regulator państwowy nie jest w stanie samodzielnie wytworzyć różnorodności równej różnorodności zagrożeń: nie ma tylu ludzi, tylu punktów obserwacji ani tylu rąk. Różnorodność musi zostać zamplifikowana przez obywateli, samorządy, przedsiębiorstwa, organizacje proobronne i sieci lokalne. Obywatelski system obrony nie jest gestem wobec społeczeństwa — jest jedynym dostępnym sposobem osiągnięcia wymaganej różnorodności regulatora.

2.3. Układ samodzielny i sześć bloków

Marian Mazur opisał układ samodzielny jako taki, który potrafi przeciwdziałać utracie zdolności sterowania. Układ taki składa się z receptorów pobierających informację, korelatora przetwarzającego ją w decyzje, efektorów wykonujących oddziaływania, homeostatu utrzymującego równowagę, akumulatora gromadzącego energomaterię i alimentatora zasilającego układ.

Przełożenie na obronę jest bezpośrednie i wyczerpuje formułę. Receptor to rozpoznanie i C4ISR. Korelator to sztaby, analiza, systemy wspomagania decyzji i modele. Efektor to wojsko, służby i administracja. Homeostat to kontrola konstytucyjna, sądy, audyt i Senat. Akumulator to rezerwy, magazyny, zapasy amunicji, paliw i leków. Alimentator to energetyka i przemysł. Siódmy człon Mazurowski — organizator, czyli organ zdolny zmienić własny program układu — w państwie należy do Narodu i realizuje się przez konstytucję i referendum.

Brak któregoś z bloków niszczy samodzielność układu, a nie tylko obniża jego sprawność. Układ bez alimentatora jest układem cudzego zasilania. Układ bez homeostatu jest układem bez hamulca. Układ bez organizatora jest układem sterowanym z zewnątrz. Formuła naczelna jest zatem cybernetycznym opisem państwa jako układu samodzielnego w warunkach wojny.

2.4. Tor sterowniczy i tor zasilający

Józef Kossecki rozwinął ujęcie Mazura, wprowadzając rozróżnienie toru sterowniczego, którym płynie informacja, i toru zasilającego, którym płynie energomateria. Państwo, które utraciło kontrolę nad torem sterowniczym, wykonuje cudze decyzje; państwo, które utraciło kontrolę nad torem zasilającym, wykonuje cudze warunki. Suwerenność jest pochodną kontroli obu torów jednocześnie.

Stąd wynika, że suwerenna technologia i odporność energetyczna są dwoma różnymi członami formuły, a nie jednym. Nie da się zastąpić jednego drugim. Suwerenne oprogramowanie bez własnej energii jest oprogramowaniem, które nie ma na czym pracować. Własna energia bez suwerennego oprogramowania jest energią, którą ktoś inny bilansuje.

Kossecki wprowadził też dwie miary bezpośrednio użyteczne w obronie. Moc swobodna to zasób, którym układ dysponuje na prowadzenie samodzielnej polityki — w obronie odpowiada jej niezaangażowana rezerwa zdolności, zapasów i mocy produkcyjnych. Czas decyzyjny to czas od zarejestrowania bodźca do wykonania odpowiedzi — struktura organizacyjna obrony powinna być projektowana tak, by go minimalizować. Państwo o zerowej mocy swobodnej nie odstrasza, bo nie ma czym odpowiedzieć; państwo o długim czasie decyzyjnym nie zwycięża, bo jego odpowiedź przychodzi po fakcie.

2.5. Model systemów żywotnych i sygnał algedoniczny

Stafford Beer wykazał, że każdy układ zdolny do przetrwania zawiera pięć współdziałających systemów: operacje, koordynację, zarządzanie bieżące z audytem, rozpoznanie przyszłości oraz tożsamość i politykę. Systemy te muszą istnieć na każdym poziomie rekurencji — w państwie, w regionie, w gminie, w jednostce wojskowej i w zakładzie przemysłowym. Obrona zbudowana wyłącznie na poziomie centralnym nie jest układem żywotnym, lecz jednym wielkim punktem awarii.

Beer opisał także kanał algedoniczny — tor alarmowy omijający hierarchię, przenoszący informację o zdarzeniu krytycznym, dla którego nie przewidziano wskaźnika. W obronie kanał ten decyduje o przeżyciu: pierwsza informacja o dywersji na stacji transformatorowej, o nietypowym ruchu dronów albo o awarii łączności nie przychodzi z centrali, lecz od operatora, dyżurnego, żołnierza rezerwy lub obywatela. Płaski tor informacyjny, opisany w rozdziale IV, jest technicznym wykonaniem tej zasady.

2.6. Pętla obserwacji i przewaga decyzyjna

John Boyd opisał walkę jako rywalizację cykli obserwacji, orientacji, decyzji i działania. Przewagę zdobywa nie ten, kto ma więcej środków, lecz ten, kto szybciej domyka cykl i tym samym zmusza przeciwnika do reagowania na sytuację już nieaktualną. Współczesne pole walki radykalnie zaostrzyło tę zależność: przy powszechnej obserwacji i taniej precyzji różnica kilku minut w pętli sensor–efektor przekłada się na różnicę między trafieniem a stratą własną.

Skracanie pętli wymaga jednak jednoczesnego spełnienia wszystkich sześciu członów. Wymaga regulatora, który zezwala na decyzję na najniższym kompetentnym poziomie; wojska nowego wzoru, zdolnego działać zadaniowo bez czekania na zgodę; suwerennej technologii, bo pętla przechodzi przez cudze systemy tylko za cudzą zgodą; energii zasilającej łączność i obliczenia; produkcji odtwarzającej zużyte środki; oraz obywateli dostarczających obserwacji spoza wojskowej sieci sensorów. Pętla decyzyjna jest miejscem, w którym formuła naczelna spina się w całość.

Cybernetyczna teza rozdziału: **obrona jest sterowaniem, a sterowanie wymaga modelu, różnorodności, dwóch sprawnych torów i krótkiej pętli.**

Każdy człon formuły jest warunkiem koniecznym sterowania, a nie postulatem politycznym.

3. Uzasadnienie systemowe

Teoria systemów pyta o coś innego niż cybernetyka: nie o to, jak układ steruje, lecz o to, jak układ zachowuje się pod obciążeniem, gdzie się załamuje i jak wraca do zdatności. Dla obrony jest to pytanie o odporność.

3.1. Awarie normalne i pułapka ścisłego sprzężenia

Charles Perrow wykazał, że w układach jednocześnie złożonych i ściśle sprzężonych awarie nie są odchyleniem od normy, lecz własnością konstrukcji. Im gęstsze powiązania i im mniejsze luzy między elementami, tym większe prawdopodobieństwo, że lokalne zdarzenie rozejdzie się po całym układzie, zanim ktokolwiek zdąży je zrozumieć.

Polska infrastruktura obronna i cywilna jest dokładnie takim układem: energetyka zależy od łączności, łączność od energetyki, transport od paliw i sterowania, administracja od danych, dane od centrów obliczeniowych, a te od zasilania i chłodzenia. Przeciwnik zdolny wywołać jedno trafne zdarzenie w węźle ściśle sprzężonym uzyskuje efekt nieproporcjonalny do włożonych środków.

Odpowiedź systemowa jest jednoznaczna: rozluźnić sprzężenia i wprowadzić luzy. W praktyce oznacza to rozproszenie zapasów, redundancję łączności, wyspowe zdolności energetyczne, procedury ręczne dla wypadku utraty systemów cyfrowych, lokalne magazyny i zapasowe centra decyzyjne. Cytadele Górskie, opisane w rozdziale VIII, są instytucjonalnym wykonaniem tej zasady, a odporność energetyczna jest jej warunkiem materialnym.

3.2. Organizacje wysokiej niezawodności

Karl Weick i Kathleen Sutcliffe opisali organizacje utrzymujące zdatność mimo ciągłego ryzyka — lotniskowce, elektrownie jądrowe, kontrolę ruchu lotniczego. Wspólne im są: zaabsorbowanie możliwością porażki, niechęć do upraszczania interpretacji, wrażliwość na przebieg operacji, dążenie do odporności oraz przenoszenie decyzji do miejsca największej kompetencji, a nie największego stopnia.

Ostatnia z tych cech jest bezpośrednim uzasadnieniem postulatu zniesienia kultury generalskiego rytuału, opisanego w rozdziale IV. Nie jest to postulat antywojskowy ani egalitarny. Jest to wniosek z badań nad organizacjami, które przez dekady utrzymują bezpieczeństwo w warunkach nieusuwalnego ryzyka: w kryzysie decyzja musi wędrować do kompetencji, a nie kompetencja do decyzji.

3.3. Cztery zdolności odporności i Model 3A

Inżynieria odporności wskazuje cztery zdolności układu odpornego: reagowanie na to, co się zdarzyło, monitorowanie tego, co się zmienia, antycypowanie tego, co może nadejść, oraz uczenie się z tego, co już zaszło. Odporność nie jest zatem stanem, lecz zestawem czynności wykonywanych stale, także w czasie pokoju.

Odpowiada temu porządkujący model [TechnoSanacji](#) — Model 3A: Antycypacja, Absorpcja, Adaptacja. Antycypacja to rozpoznanie, prognoza, wargaming, rejestr ryzyk i progi alarmowe. Absorpcja to zdolność przyjęcia uderzenia bez utraty funkcji krytycznych: rezerwy, redundancja, schrony, rozproszenie, degradacja łagodna zamiast załamania. Adaptacja to zdolność przebudowy w trakcie konfliktu: zmiana konstrukcji, taktyki, produkcji i procedur w cyklach tygodniowych, nie rocznych.

Model 3A jest metodą sprawdzania każdego elementu systemu obrony trzema pytaniami: czy widzimy to zawczasu, czy wytrzymamy uderzenie i czy zdążymy się przebudować. Element, który nie przechodzi wszystkich trzech testów, nie jest zdolnością obronną, lecz kosztem.

3.4. Punkty dźwigni i hierarchia interwencji

Donella Meadows uporządkowała miejsca, w których można ingerować w system, według siły efektu. Najłabsze są zmiany parametrów: budżetów, etatów, limitów. Silniejsze są zmiany struktury przepływów i sprzężeń. Najsilniejsze są zmiany reguł, celów i sposobu myślenia o systemie.

Wniosek dla polityki obronnej jest niewygodny, ale użyteczny: zwiększenie wydatków obronnych jest interwencją parametryczną, a więc najłabszą z dostępnych. Zmiana reguł — tego, co budżet ma kupować, kto decyduje, jak liczy się efekt, komu wolno produkować i kto ponosi odpowiedzialność — daje efekt o rząd wielkości większy przy tych samych pieniądzach. Formuła naczelna jest interwencją na poziomie reguł i celów, dlatego zdefiniowano ją jako zdolność, a nie jako procent produktu krajowego brutto.

3.5. Kruchość, odporność i antykruchość

System kruchy traci funkcję pod obciążeniem. System odporny zachowuje funkcję i wraca do stanu wyjściowego. System antykruchy poprawia się wskutek obciążenia — pod warunkiem że posiada mechanizm uczenia się i zasób pozwalający przeżyć pierwszy wstrząs. Wojna ukraińska jest najlepiej udokumentowanym przykładem antykruchości organizacyjnej: cykl uwaga–błąd–korekta–wdrożenie skrócono tam z lat do tygodni, a konstrukcje dronów i procedury przeciwdziałania zmieniano szybciej, niż przeciwnik zdążył je rozpoznać.

Antykruchość nie jest jednak darmowa. Wymaga zapasu, który pozwala przeżyć pierwsze uderzenie, oraz produkcji, która pozwala wdrożyć wnioski. Państwo bez zapasu uczy się na własnej klęsce; państwo bez produkcji uczy się bez możliwości zastosowania nauki. Zasada „uczyć się szybciej od przeciwnika”, sformułowana w rozdziale IX, jest wykonalna tylko przy jednoczesnym spełnieniu członów o odporności energetycznej i produkcji.

Systemowa teza rozdziału: **obrona jest odpornością,
a odporność wymaga luzów, rozproszenia, decyzji przy kompetencji
oraz zdolności antycypacji, absorpcji i adaptacji.**

Zwiększenie nakładów bez zmiany reguł jest najstabszą z możliwych interwencji.

4. Uzasadnienie sieciowe

Państwo i jego obrona są sieciami: sieciami energetycznymi, transportowymi, teleinformatycznymi, dowodzenia, dostaw i zaufania społecznego. Teoria sieci pozwala powiedzieć o nich rzeczy, których nie widać ani w ujęciu cybernetycznym, ani systemowym — przede wszystkim to, gdzie dokładnie uderzy racjonalny przeciwnik.

4.1. Odporność na awarię, kruchość wobec ataku

Réka Albert, Hawoong Jeong i Albert-László Barabási wykazali w 2000 roku, że sieci o rozkładzie potęgowym — a takimi są niemal wszystkie sieci infrastrukturalne — mają własność, którą określa się jako „odporne, lecz kruche”. Usunięcie losowych węzłów prawie nie wpływa na spójność sieci, bo trafia głównie w węzły peryferyjne. Usunięcie kilku węzłów o najwyższym stopniu rozбивa sieć na niepołączone fragmenty.

Konsekwencja dla obrony jest bezpośrednia. Awaria jest losowa, przeciwnik nie jest. Planowanie odporności na awarie nie daje odporności na atak. Polska sieć energetyczna, telekomunikacyjna, transportowa i administracyjna ma wyraźne huby — i przeciwnik dysponujący rozpoznaniem satelitarnym oraz taniej precyzji zna ich położenie równie dobrze jak my. Obrona musi być planowana wobec ataku inteligentnego na huby, a nie wobec awarii przypadkowej.

Odpowiedź sieciowa jest dwójaka: obniżać koncentrację hubów, tworząc alternatywne węzły i ścieżki, oraz osłaniać te huby, których zdekoncentrować się nie da. System Górskich Cytadel realizuje pierwszy człon tej odpowiedzi — buduje zapasowe węzły decyzyjne, danych i zaopatrzenia poza obszarem najłatwiejszego rozpoznania. Warstwowa obrona powietrzna i ochrona infrastruktury krytycznej realizują drugi.

4.2. Centralność pośrednictwa i wąskie gardła

Miarą znaczenia węzła nie jest tylko liczba jego połączeń, lecz liczba najkrótszych ścieżek, które przez niego przechodzą. Węzeł o wysokiej centralności pośrednictwa może mieć niewiele połączeń, a mimo to jego usunięcie rozcina sieć. Geografia Polski i regionu zawiera kilka takich punktów: przesmyk suwalski w wymiarze lądowym, wąskie gardła korytarzy północ-południe, kluczowe stacje przesyłowe, węzły kolejowe, punkty styku sieci gazowych i kablówce połączenia Bałtyku.

Doktryna obronna, która nie zawiera jawnej listy węzłów o najwyższej centralności pośrednictwa wraz z przypisanym im wariantem obejścia, nie jest doktryną, lecz opisem. Analiza sieciowa dostarcza tu narzędzia ścisłego: dla każdego krytycznego węzła należy wskazać drugą ścieżkę, koszt jej uruchomienia i czas przetoczenia. Tam, gdzie druga

ścieżka nie istnieje, mamy do czynienia z pojedynczym punktem awarii państwa, a jego usunięcie jest zadaniem inwestycyjnym o priorytecie wyższym niż zakup platform.

4.3. Kaskada w sieciach współzależnych

Sergey Buldyrev i współpracownicy wykazali w 2010 roku, że dwie wzajemnie zależne sieci — na przykład energetyczna i teleinformatyczna — załamują się w sposób jakościowo inny niż każda z nich osobno. Awaria przenosi się tam i z powrotem między sieciami, a rozpad następuje skokowo, po przekroczeniu progu, przy usunięciu znacznie mniejszej liczby węzłów niż w sieci pojedynczej.

To jest dokładny opis blackoutu połączonego z paraliżem łączności i administracji. Sterowanie siecią energetyczną wymaga łączności; łączność wymaga zasilania; przywracanie zasilania wymaga sterowania. Państwo, które nie posiada wysp zdolnych do startu bez zasilania zewnętrznego, mikrosieci, zapasowej łączności i procedur ręcznych, ma w tym miejscu próg katastrofalny — punkt, po którego przekroczeniu odbudowa nie postępuje stopniowo, lecz nie postępuje wcale.

Odporność energetyczna nie jest zatem członem formuły z powodów gospodarczych ani klimatycznych. Jest w niej dlatego, że stanowi warunek uniknięcia kaskady w sieciach współzależnych, czyli warunek istnienia toru zasilającego państwa w czasie wojny.

4.4. Od łańcucha rażenia do sieci rażenia

Klasyczny łańcuch rażenia — wykryj, zidentyfikuj, wskaż, uderz, oceń — jest strukturą szeregową. Struktura szeregową ma tyle punktów awarii, ile ogniów: usunięcie jednego przerywa całość. Współczesne doktryny wielodomenowe zastępują łańcuch siecią rażenia, w której każdy sensor może zasilić każdy efektor, a utrata elementu powoduje przekierowanie, a nie przerwanie.

Sieć rażenia jest architekturą sieciową, a nie zakupem. Wymaga wspólnych standardów wymiany danych, otwartych interfejsów, modularności i zdolności do integracji systemów różnych dostawców. Wymaga zatem suwerennej technologii w ścisłym sensie: własności standardu i możliwości zmiany dostawcy. Uzależnienie od jednego dostawcy jest w języku sieciowym dobrowolnym stworzeniem huba o maksymalnej centralności i oddaniem go w cudze ręce.

4.5. Prawo Conwaya i architektura dowodzenia

Melvin Conway zauważył, że struktura projektowanego systemu odwzorowuje strukturę komunikacyjną organizacji, która go buduje. Prawo to działa w obronności bezlitośnie: armia o hierarchii pionowej i słabej komunikacji poziomej zbuduje systemy dowodzenia, które nie wymieniają danych między rodzajami sił zbrojnych, choćby kupiła najlepszy sprzęt. Wynika stąd kolejność, którą doktryna musi uszanować: integracja mandatu i odpowiedzialności poprzedza integrację systemów. Nie da się kupić sieci rażenia dla organizacji zbudowanej z pionów, które nie rozmawiają. Reforma dowodzenia opisana w rozdziale IV jest zatem warunkiem technicznej wykonalności warstw 3–7 architektury, a nie osobnym postulatem organizacyjnym.

4.6. Sieć obywatelska jako amplifikator

Mark Granovetter wykazał, że informację nową przenoszą przede wszystkim więzi słabe — kontakty spoza własnego, gęsto powiązanego środowiska. Organizacja zamknięta widzi to, co już wie. Sieć rozproszona, złożona z obywateli, samorządów, przedsiębiorstw, organizacji proobronnych i szkół, dostarcza obserwacji, których żaden system wojskowy nie zbierze, bo nie znajduje się w tych miejscach.

Ten sam mechanizm działa w obronie kognitywnej. Dezinformacja rozchodzi się w sieci społecznej i tylko w sieci społecznej może zostać powstrzymana. Państwo może dostarczyć wiarygodnych danych i uodpornić przez wcześniejsze ujawnienie mechanizmu manipulacji, lecz nie zastąpi zaufania lokalnego. Obywatelski system obrony jest więc jednocześnie siecią sensorów, siecią efektorów i siecią odporności poznawczej — trzema funkcjami, których scentralizowany aparat nie wytworzy przy żadnym budźecie.

Sieciowa teza rozdziału: **przeciwnik nie uderza losowo, lecz w huby i węzły pośredniczące.**

Odporność wymaga dekoncentracji hubów, drugiej ścieżki dla każdego węzła krytycznego, przerywania kaskady między siecią energii i danych oraz sieci obywatelskiej jako amplifikatora obserwacji.

5. Uzasadnienie militarne

Trzy poprzednie uzasadnienia dotyczyły struktury. Czwarte dotyczy walki: rozstrzyga, czy tak zbudowany system wygrywa starcie z konkretnym przeciwnikiem, w konkretnej geografii, przy konkretnej ekonomii środków.

5.1. Odstraszanie przez odmowę i przez karanie

Glenn Snyder rozróżnił w 1961 roku dwie logiki odstraszania. Odstraszanie przez karanie działa groźbą nieakceptowalnego kosztu wymierzonego po agresji. Odstraszanie przez odmowę działa przekonaniem przeciwnika, że agresja nie osiągnie celu operacyjnego. Thomas Schelling pokazał, że wiarygodność groźby zależy nie od jej wielkości, lecz od tego, czy przeciwnik uzna jej wykonanie za prawdopodobne.

Dla państwa frontowego o ograniczonych zasobach odstraszanie przez odmowę jest logiką pierwszorzędą, a przez karanie — uzupełniającą. Odmowa jest bowiem sprawdzalna: przeciwnik może oszacować gęstość obrony powietrznej, głębokość zapasów, przeżywalność dowodzenia i zdolność społeczeństwa do trwania. Karanie wymaga wiary w cudzą determinację. Doktryna, która stawia wyłącznie na karanie, oddaje rozstrzygnięcie o własnym bezpieczeństwie w ręce cudzej oceny naszej woli.

Trzeci mechanizm — odporność jako odstraszanie — nie ma klasycznego odpowiednika w teorii zimnowojennej, bo dotyczy wojny, w której głównym celem nie są siły zbrojne, lecz spójność państwa. Jeżeli energetyka, administracja, łączność, ochrona zdrowia

i transport działają mimo uderzenia, kampania obliczona na szybkie złamanie woli traci sens ekonomiczny. Odporność zmienia rachunek przeciwnika, nie zwiększając ryzyka eskalacji — jest to jedyny mechanizm odstraszania o tej własności.

5.2. Ekonomia wymiany kosztów

Współczesne pole walki rozstrzyga się w relacji kosztów, a nie w porównaniu katalogów. Dron jednorazowy kosztujący kilkadziesiąt tysięcy dolarów, zwalczany pociskiem przechwytyjącym kosztującym kilka milionów, wygrywa nawet wtedy, gdy zostaje zestrzelony — bo wymusza wymianę korzystną dla atakującego i wyczerpuje magazynek obrońcy. Doświadczenie wojny ukraińskiej oraz starcia raketowo-dronowego z 2025 roku pokazało to z dokumentacją finansową.

Reguła projektowa wymiany kosztów

Każdy tani, masowy środek ataku musi być zwalczany środkiem o koszcie porównywalnym lub niższym: dronem przechwytyjącym, artylerią lufową, walką radioelektroniczną, laserem lub bronią mikrofalową. Drogi pocisk przechwytyjący rezerwuje się dla celów, których inaczej zwalczyć nie można. Naruszenie tej reguły oznacza, że przeciwnik steruje naszym budżetem obronnym za pomocą sklejki i silnika spalinowego.

Z reguły tej wynikają mierniki, których doktryna nie może pomijać: współczynnik wymiany kosztów, koszt zniszczenia celu, koszt obrony obiektu, koszt łańcucha rażenia oraz koszt obejścia systemu przez przeciwnika. Doktryna bez tych mierników nie potrafi odróżnić zdolności od zakupu.

5.3. Głębokość magazynka i tempo odtwarzania

Wayne Hughes wykazał w modelu wymiany salw, że o wyniku starcia rozstrzyga liczba efektywnych salw, jakie strona jest w stanie wyprowadzić i przyjąć, a nie nominalna jakość platform. Model ten przenosi się wprost na obronę powietrzną i raketową: system o doskonałej skuteczności pojedynczego strzału, lecz płytkim zapasie, przegrywa z saturacją.

Stąd dwie wielkości, które muszą być liczone i chronione: głębokość magazynka, czyli liczba dni intensywnej walki pokrywana zapasem, oraz tempo odtwarzania, czyli zdolność wyprodukowania zużytego środka szybciej, niż przeciwnik zdąży zużyć swój. Zaawansowana produkcja militarna i dual use jest w formule właśnie dlatego, że jest jedyną znaną odpowiedzią na obie te wielkości. Zapas bez produkcji jest wielkością malejącą; produkcja bez zapasu nie zdąży.

W tym sensie zdanie „produkcja jest odstraszaniem” nie jest hasłem, lecz wnioskiem z modelu wymiany salw. Przeciwnik szacujący nasze zapasy i nasze linie produkcyjne szacuje, jak długo może prowadzić wojnę na wyczerpanie z korzystnym dla siebie wynikiem. Widoczna, głęboka i szybka produkcja skraca ten horyzont do wartości, przy której kampania traci sens.

5.4. Przejrzyste pole walki i masa precyzji

Powszechna obserwacja — satelitarna, dronowa, radiolokacyjna i elektromagnetyczna — usunęła możliwość ukrycia dużych zgrupowań. To, co zostaje wykryte, zostaje trafione; to, co zostaje trafione tanio, przestaje się optacać. Stephen Biddle wykazał już wcześniej, że o skuteczności nie decyduje sama technika, lecz sposób jej użycia: rozproszenie, maskowanie, wykorzystanie terenu, łączenie broni i inicjatywa niższych szczebli.

Wojsko nowego wzoru jest odpowiedzią na obie te obserwacje jednocześnie. Masa precyzji zastępuje masę platform, bo tania precyzja bije drogą koncentrację. Rozproszone pododdziały zdolne do samodzielnego działania zastępują wielkie zgrupowania, bo zgrupowanie jest celem. Zwalczanie bezzałogowców zyskuje priorytet równy systemom bezzałogowym, bo obie strony dysponują tą samą ekonomią. Walka radioelektroniczna przestaje być wsparciem, a staje się domeną podstawową, bo bez niej cała masa precyzji przeciwnika działa bez zakłóceń.

5.5. Zwyciężanie: zakończenie wojny na własnych warunkach

Trzecia miara formuły — zwyciężanie — wymaga osobnego omówienia, ponieważ jest w polskich dokumentach obronnych najłabiej zdefiniowana. Zwycięstwo państwa broniącego się nie polega na zajęciu cudzego terytorium. Polega na doprowadzeniu przeciwnika do stanu, w którym kontynuowanie agresji jest dla niego droższe niż jej zakończenie na warunkach akceptowalnych dla Polski, oraz na utrzymaniu zdolności państwa do funkcjonowania po zakończeniu konfliktu.

Wynikają stąd trzy wymagania rzadko ujmowane w planowaniu. Po pierwsze, zdolność do prowadzenia wojny długiej: zapasy, produkcja, rezerwy kadrowe, finanse wojenne, ochrona zdrowia i logistyka cywilna liczone w miesiącach, nie w dniach. Po drugie, zdolność do oddziaływania na kalkulację przeciwnika w trakcie konfliktu, a nie tylko przed nim: sterowanie eskalacją, wiarygodne rażenie w głąb, oddziaływanie informacyjne i gospodarcze. Po trzecie, zdolność do odbudowy: państwo, które przetrwało i odstraszyło, lecz nie potrafi odbudować infrastruktury, energetyki i administracji, przegrywa pokój po wygranej wojnie.

Zwyciężanie jest więc członem, który spina pozostałe. Wymaga regulatora zdolnego prowadzić państwo przez wojnę i po niej, obywateli gotowych trwać, wojska zdolnego walczyć długo, technologii, której nikt nie wyłączy, energii, która nie ustanie, i produkcji, która odtwarza straty. Nie da się zwyciężać żadnym pojedynczym członem.

5.6. Obrona totalna: dowód porównawczy

Modele obrony totalnej — fiński, szwedzki, estoński i tajwański — dostarczają dowodu empirycznego dla członu obywatelskiego. Państwa te, dysponując zasobami mniejszymi niż ich przeciwnicy, budują odstraszanie na powszechnym przygotowaniu społeczeństwa, zapasach, schronach, łączności kryzysowej i planach ciągłości działania. Zobowiązania sojusznicze w zakresie odporności oraz europejskie prace nad gotowością cywilną potwierdzają ten kierunek jako standard, a nie wyjątek.

Polska ma w tym zakresie podstawę prawną w postaci regulacji o ochronie ludności i obronie cywilnej, lecz wykonanie pozostaje w fazie początkowej: sieć schronów, zapasy, powszechne szkolenie i systemy ostrzegania wymagają programu o skali porównywalnej z modernizacją techniczną wojska. Człon obywatelski formuły jest zatem nie tylko uzasadniony teoretycznie i empirycznie, lecz jest też miejscem największej luki wykonawczej państwa polskiego.

Militarna teza rozdziału: wygrywa państwo o korzystnej wymianie kosztów, głębokim magazynku, szybkim odtwarzaniu, rozproszonej masie precyzji i społeczeństwie zdolnym trwać.

**Odstraszanie przez odmowę jest sprawdzalne,
odstraszanie przez karanie wymaga wiary,
a zwyciężanie wymaga obu i jeszcze zdolności odbudowy.**

6. Synteza: zbieżność czterech dowodów

Cztery uzasadnienia wychodzą z różnych przesłanek i posługują się różnym aparatem, lecz wskazują te same warunki konieczne. Poniższa tabela zestawia, z czego wynika każdy człon formuły w każdym z czterech porządków dowodowych.

Zbieżność ta ma znaczenie praktyczne, nie tylko retoryczne. Oznacza, że rezygnacja z któregośkolwiek członu nie jest wyborem między konkurencyjnymi szkołami myślenia, lecz naruszeniem warunku, który cztery niezależne teorie uznają za konieczny. Spór o priorytety obronne jest uprawniony; spór o to, czy dany człon jest potrzebny, jest sporem z dowodem.

Człon formuły	Uzasadnienie cybernetyczne	Uzasadnienie systemowe	Uzasadnienie sieciowe	Uzasadnienie militarne
Zdolność Narodu (podmiot)	Amplifikacja różnorodności regulatora ponad zasoby aparatu państwowego.	Odporność wymaga rozproszonych zasobów i lokalnej zdolności działania.	Sieć obywatelska jako amplifikator obserwacji i odporności poznawczej.	Obrona totalna: państwa mniejsze odstraszać przygotowaniem społeczeństwa.
Samodzielne przetrwanie	Układ samodzielny musi mieć wszystkie sześć bloków i własny organizator.	Ciągłość działania mimo awarii normalnych i utraty elementów.	Dekoncentracja hubów i druga ścieżka dla węzła krytycznego.	Przeżywalność dowodzenia, rozproszenie, schrony, rezerwy.
Odstraszanie	Widoczna moc swobodna zmienia kalkulację przeciwnika.	Odporność odbiera sens uderzeniu bez podnoszenia ryzyka eskalacji.	Brak optymalnego celu o wysokiej centralności zniechęca do ataku.	Odstraszanie przez odmowę jako logika sprawdzalna, karanie jako uzupełnienie.
Zwycięzanie	Krótki czas decyzyjny daje inicjatywę i przewagę w pętli.	Antykruchłość: uczenie się w cyklu tygodniowym, nie rocznym.	Sieć rażenia przekierowuje zamiast przerywać po utracie elementu.	Wojna długa, sterowanie eskalacją i zdolność odbudowy po konflikcie.
Sprawcze państwo z regulatorem	Twierdzenie o dobrym regulatorze i wymagana różnorodność.	Decyzja przy kompetencji; homeostat kontrolujący sterującego.	Prawo Conwaya: integracja mandatu przed integracją systemów.	Jednoznaczne dowodzenie, dowodzenie zadaniowe, rejestr ryzyk.
Obywatelski system obrony	Amplifikacja różnorodności i kanał algedoniczny spoza hierarchii.	Rozproszona absorpcja uderzenia i lokalna ciągłość działania.	Siła słabych więzi; obrona kognitywna działa tylko w sieci społecznej.	Rezerwy, obrona cywilna, schrony, medycyna i logistyka społeczna.
Wojsko nowego wzoru	Skrócenie pętli decyzyjnej i przeniesienie decyzji do kompetencji.	Rozluźnienie sprzężeń: rozproszone pododdziały zamiast zgrupowań.	Sieć rażenia zamiast szeregowego łańcucha rażenia.	Masa precyzji, przejrzyste pole walki, zwalczanie bezzałogowców.
Suwerenna technologia	Model rzeczywistości musi należeć do regulatora, nie do dostawcy.	Możliwość zmiany dostawcy jako warunek adaptacji systemu.	Uzależnienie od dostawcy tworzy hub w cudzych rękach.	Przewaga decyzyjna, C4ISR, odporność łączności i nawigacji.
Odporność energetyczna	Tor zasilający jako warunek działania toru sterowniczego.	Luz i redundancja przeciw awarii normalnej w układzie sprzężonym.	Przerwanie kaskady w sieciach współzależnych energii i danych.	Zasilanie dowodzenia, obrony powietrznej, danych i produkcji.
Produkcja militarna i dual use	Alimentator i akumulator układu samodzielnego.	Antykruchłość bez produkcji jest nauką bez zastosowania.	Rozproszone zdolności wytwórcze zamiast pojedynczego zakładu.	Głębokość magazynka i tempo odtwarzania; produkcja jako odstraszanie.

7. Warunki falsyfikacji i mierniki

Doktryna sprawdzalna musi wskazać, co świadczyłoby przeciw niej. Formuła naczelna byłaby fałszywa, gdyby prawdziwe okazało się choć jedno z następujących twierdzeń: że państwo może sterować obroną bez własnego modelu rzeczywistości; że regulator o różnorodności mniejszej niż różnorodność zagrożeń utrzymuje kontrolę; że sieć infrastrukturalna o silnych hubach jest odporna na atak celowany; że system o płytkim zapasie wygrywa z saturacją; albo że państwo bez zdolności odtwarzania strat prowadzi wojnę długą.

Żadne z tych twierdzeń nie znajduje potwierdzenia ani w teorii, ani w doświadczeniu ostatnich lat. Dopóki tak jest, formuła obowiązuje. Aby jednak nie pozostała deklaracją, każdy jej człon otrzymuje mierniki podlegające okresowemu przeglądowi.

Mierniki realizacji formuły

- czas decyzyjny — mierzony czas od zarejestrowania bodźca do wykonania odpowiedzi, na każdym szczeblu i dla każdego typu zdarzenia,
- kompletność modelu rzeczywistości — udział infrastruktury krytycznej, zapasów i zdolności objętych aktualnym, weryfikowalnym obrazem sytuacyjnym,
- moc swobodna — udział zdolności, zapasów i mocy produkcyjnych niezaangażowanych w zadania bieżące,
- współczynnik wymiany kosztów — relacja kosztu zwalczenia celu do kosztu jego użycia przez przeciwnika, dla każdej klasy zagrożenia,
- głębokość magazynka — liczba dni intensywnej walki pokrywana zapasem amunicji, rakiet, paliw, części, leków i komponentów,
- tempo odtwarzania — zdolność produkcji krajowej w horyzontach trzydziestu, czterdziestu i stu osiemdziesięciu dni,
- liczba pojedynczych punktów awarii państwa — węzły krytyczne bez uruchamialnej drugiej ścieżki,
- autonomia energetyczna funkcji krytycznych — czas pracy dowodzenia, łączności, centrów danych i szpitali bez zasilania zewnętrznego,
- zasięg obywatelskiego systemu obrony — udział obywateli objętych szkoleniem, przypisaniem do zadania i dostępem do schronu,
- szybkość uczenia się — czas od zaobserwowania nowej techniki przeciwnika do wdrożenia przeciwdziałania.

Mierniki te mają właściciela, próg alarmowy i termin reakcji. Ich pogorszenie uruchamia obowiązek działania, a nie obowiązek sprawozdania. To rozróżnienie — między sprzężeniem zwrotnym a raportowaniem — jest ostatecznym testem tego, czy państwo posiada regulator, czy tylko administrację obronną.

IV. Model cybernetyczny: państwo z regulatorem

[TechnoRepublika](#) traktuje państwo jako układ samodzielny, który musi sterować sobą w warunkach presji, zakłóceń i niepewności. Dobry regulator musi mieć aktualny model rzeczywistości. W obronie oznacza to pełną świadomość sytuacyjną: dane z satelitów, dronów, radarów, sensorów, cyberprzestrzeni, administracji, energetyki i społeczeństwa.

1. Płaski tor informacyjny

Informacja nie może grzęznąć w sztabowych piramidach, biurokratycznych filtrach i feudalnej kulturze stopni. System obrony musi działać w modelu płaskiego toru informacyjnego: sensor, analiza, decyzja i efekt muszą być połączone w możliwie krótką pętlę. Dane mają trafiać do tego poziomu, który może podjąć decyzję i ponosi za nią odpowiedzialność.

2. Płaski tor zasilający

Energia, amunicja, paliwo, części zamienne, żywność, woda, leki, tężyzna i software muszą być rozmieszczone, zabezpieczone i zdolne do pracy w warunkach przerwania centralnych dostaw. Obrona nie może opierać się na jednym magazynie, jednej sieci, jednym centrum danych, jednym dowództwie i jednym dostawcy.

3. Krótka pętla decyzyjna

Wojna algorytmiczna premiuje krótką pętlę decyzyjną. Kto widzi szybciej, rozumie szybciej, decyduje szybciej i działa szybciej — przejmuje inicjatywę. TechnoRepublika skraca pętlę decyzyjną przez AI decision support, systemy C4ISR, dowodzenie zadaniowe, red teaming, wargaming, stałe ćwiczenia i realną odpowiedzialność dowódców.

4. Zniesienie kultury generalskiego rytuału

W systemie TechnoRepubliki funkcja dowodzenia ma wynikać ze zdolności, odpowiedzialności i aktualnej kompetencji, a nie z rytuału starszeństwa. Docelowo należy ograniczyć ceremonialną hierarchię generalską na rzecz **rotacyjnego dowodzenia zadaniowego**.

Agencjami, brygadami, cytaadelami, zespołami operacyjnymi i programami technologicznymi powinni kierować ci, którzy najlepiej rozumieją zadanie: sierżanci, porucznicy, majorowie, pułkownicy, inżynierowie, operatorzy, analitycy, cybernetycy i menedżerowie misji. Stopień nie może zastępować kompetencji. Hierarchia ma służyć decyzji, a nie opóźniać decyzję.

5. Prawo wymaganej różnorodności

Przeciwnik używa wielu narzędzi: wojska, dywersji, cyberataków, sabotażu, dezinformacji, presji energetycznej, migracyjnej, finansowej, biologicznej i nuklearnej. Regulator państwowy musi posiadać różnorodność co najmniej równą różnorodności

zagrożeń. Dlatego obrona TechnoRepubliki jest wielodomenowa: ląd, powietrze, morze, cyberprzestrzeń, kosmos, spektrum elektromagnetyczne, informacja, gospodarka, energetyka i społeczeństwo.

6. Państwo z regulatorem, a nie państwo zamiast regulatora

Formuła naczelna mówi o sprawczym państwie z regulatorem, nie o państwie-regulatorze. Różnica nie jest stylistyczna. Określenie „państwo-regulator” jest metaforą: opisuje pożądaną cechę całości. Określenie „państwo z regulatorem” jest wymaganiem konstrukcyjnym: żąda, aby w państwie istniał wyodrębniony, wyposażony i rozliczalny podsystem sterowania obroną, mający własny model rzeczywistości, własne kanały alarmowe, własne uprawnienia decyzyjne i imiennie wskazaną odpowiedzialność.

Państwo bez takiego podsystemu nie przestaje mieć instytucji — przestaje mieć sterowanie. Kompetencje rozpraszają się między resorty, informacja krąży bez adresata zdolnego podjąć decyzję, a odpowiedzialność rozmywa się w uzgodnieniach. W czasie pokoju objawia się to opieszałością; w czasie kryzysu — paraliżem.

Regulator obrony Rzeczypospolitej obejmuje zatem: system kierowania obroną państwa z jednoznaczną odpowiedzialnością Prezydenta, stałe centrum sytuacyjne prowadzące aktualny model rzeczywistości, kanały algedoniczne omijające hierarchię, ośrodek analizy strategicznej z wargamingiem i red teamingiem, rejestr ryzyk wojennych z progami alarmowymi i właścicielami, oraz mechanizm kontroli — Senatu, sądów i audytu — który sprawdza samego regulatora. Regulator bez kontroli nie jest regulatorem państwa republikańskiego, lecz ośrodkiem władzy bez homeostatu.

V. Pięć linii wysiłku strategicznego

Linia 1. Wojsko nowego wzoru

Wojsko nowego wzoru jest profesjonalnym rdzeniem systemu obrony, ale nie jest samotną wyspą. Jego zadaniem jest tworzenie efektów militarnych przez integrację ludzi, sensorów, dronów, rakiet, cyberprzestrzeni, sztucznej inteligencji, obrony powietrznej i mobilnych pododdziałów.

Priorytety:

- masa precyzji zamiast masy platform,
- drony rozpoznawcze, uderzeniowe i logistyczne,
- amunicja krążąca i systemy FPV,
- counter-UAS jako priorytet równy systemom dronowym,
- rozproszone oddziały zdolne do samodzielnego działania,
- human-machine teaming,
- elastyczna logistyka,
- maskowanie, dezinformacja taktyczna, fałszywe cele,
- integracja rozpoznania i ognia w krótkiej pętli sensor-to-shooter.

Linia 2. Obywatelski system obrony

Obywatel nie może być widzem wojny informacyjnej, energetycznej i militarnej. Musi być uczestnikiem odporności państwa.

Obywatelski system obrony obejmuje:

- powszechne szkolenie obronne,
- rezerwy terytorialne,
- lokalne zespoły odporności,
- organizacje proobronne,
- edukację kryzysową w szkołach i wspólnotach lokalnych,
- obronę cywilną i ochronę ludności,
- sieć schronów,
- ratownictwo, medycynę taktyczną i logistykę społeczną,
- cyfrowe systemy ostrzegania,
- przygotowanie rodzin, szkół, gmin i zakładów pracy.

Celem nie jest militaryzacja społeczeństwa. Celem jest społeczeństwo, które nie panikuje, nie ulega dezinformacji i wie, co robić w godzinie próby.

Linia 3. Domena cyfrowa: AI, cyberprzestrzeń i kosmos

Domena cyfrowa jest układem nerwowym obrony państwa. Obejmuje:

- suwerenną chmurę obronną,
- krajowe modele AI dla bezpieczeństwa,
- C4ISR i battlefield data fabric,
- rozpoznanie satelitarne,
- odporność PNT/GPS,
- cyberobronę infrastruktury krytycznej,
- aktywne wykrywanie operacji informacyjnych,
- ochronę danych publicznych,
- audyt algorytmów używanych w bezpieczeństwie,
- człowieka w pętli przy decyzjach o użyciu siły.

AI ma wzmacniać decyzję człowieka, nie zastępować odpowiedzialność człowieka. TechnoRepublika odrzuca zarówno naiwny technoentuzjazm, jak i lęk przed technologią. Przyjmuje zasadę: **AI w służbie obywatela i państwa, nie obywatel w służbie algorytmu.**

Linia 4. Tarcza i miecz rakietowy

Polska potrzebuje jednocześnie tarczy i miecza.

Tarcza to:

- warstwowa obrona powietrzna,
- obrona przeciwrakietowa,
- obrona przed dronami,
- ochrona infrastruktury krytycznej,
- obrona centrów danych, energetyki, portów, lotnisk, kolei, szpitali i administracji.

Miecz to:

- długodystansowe ognie,
- rakiety precyzyjne,
- drony dalekiego zasięgu,
- środki oddziaływania cybernetycznego,
- zdolność niszczenia systemów rozpoznania, logistyki i dowodzenia przeciwnika.

Tarcza bez miecza zaprasza do szantażu. Miecz bez tarczy tworzy ryzyko eskalacji bez przeżywalności. TechnoRepublika buduje jedno i drugie, pod kontrolą konstytucyjną i cywilną.

Linia 5. Arsenał przemysłowo-energetyczny

Obrona wymaga własnego arsenału. Nie tylko wojskowego, lecz przemysłowo-energetycznego.

Arsenał TechnoRepubliki obejmuje:

- produkcję amunicji,
- produkcję dronów,
- produkcję rakiet i komponentów,
- elektronikę, sensory i systemy łączności,
- druk 3D i szybkie prototypowanie,
- przemysł dual use,
- magazyny energii,
- wodór i paliwa syntetyczne,
- mikrosieci,
- odporne centra danych,
- zaplecze naprawcze i modernizacyjne,
- rezerwy surowców krytycznych.

Bez energii nie ma danych. Bez danych nie ma dowodzenia. Bez produkcji nie ma odstraszania. Bez przemysłu nie ma suwerenności.

Odporność energetyczna jako warunek obrony

Energia jest torem zasilającym całego systemu obrony i osobnym członem formuły naczelnej. Bez zasilania nie działa łączność, rozpoznanie, dowodzenie, obrona powietrzna, centrum danych, szpital, wodociąg ani produkcja. Sieć energetyczna i sieć teleinformatyczna są wzajemnie zależne, co oznacza, że ich wspólne załamanie następuje skokowo i przy mniejszym uszkodzeniu, niż wynikałoby z analizy każdej z nich osobno.

Odporność energetyczna obrony opiera się na pięciu zdolnościach: rozproszeniu wytwarzania, zdolności pracy wyspowej i uruchomienia bez zasilania zewnętrznego, magazynowaniu energii i paliw, wielonośnikowości oraz sterowalności opartej na własnych danych i własnym oprogramowaniu. Funkcje krytyczne państwa — dowodzenie, łączność, centra danych, szpitale, ujęcia wody, węzły transportowe — muszą mieć określony i sprawdzony czas pracy bez sieci zewnętrznej.

Doktryna energetyczna TechnoRepubliki jest wobec obrony dokumentem komplementarnym: to, co tam nazywa się sterowalnością i ustrojem energetycznym, tutaj jest warunkiem przeżywalności. Energia nie jest sektorem obsługującym obronę. Jest jej częścią.

VI. Zakotwiczenie ustrojowe

Narodowa Obrona Rzeczypospolitej jest bezpośrednio powiązana z ustrojem państwa.

1. Prezydent jako egzekutywa

Prezydent Rzeczypospolitej jako jednoznaczna egzekutywa odpowiada za strategię bezpieczeństwa, kierowanie administracją państwową i ciągłość działania państwa. W czasie kryzysu nie może istnieć chaos kompetencyjny. Odpowiedzialność musi być jasna, szybka i rozliczalna.

2. Senat jako kontrola demokratyczna

Senat sprawuje kontrolę nad systemem obrony: budżetem, agencjami, stanami nadzwyczajnymi, zakupami strategicznymi, algorytmami bezpieczeństwa i użyciem środków przymusu. Obrona sprawcza musi pozostać obroną republikańską.

3. Sądy i prawa obywatelskie

Sądy chronią obywatela przed nadużyciem władzy obronnej. Stany nadzwyczajne nie mogą stać się furtką do państwa nadzoru. Jawność zasad, rozliczalność decyzji, audyt algorytmów i ochrona praw niezbywalnych są warunkiem legitymacji doktryny.

4. Referendum i kontrola obywatelska

W sprawach fundamentalnych dla bezpieczeństwa państwa Naród zachowuje prawo kontroli. Obrona ojczyzny nie może być wyjęta spod podmiotowości obywatelskiej. Państwo ma być silne siłą obywateli, a nie silne przeciw obywatelom.

VII. Architektura siedmiu warstw obrony

Warstwa 1. Państwo-regulator

System kierowania obroną państwa, krótka pętla decyzyjna, ciągłość działania, stany nadzwyczajne z bezpiecznikami, jasna odpowiedzialność Prezydenta, kontrola Senatu i sądów.

Warstwa 2. Obywatel

Obrona powszechna, rezerwy, obrona cywilna, schrony, szkolenia, lokalne systemy odporności, samorządy, szkoły, zakłady pracy, rodziny i wspólnoty.

Warstwa 3. Manewr

Wojsko nowego wzoru: rozproszone, mobilne, wielodomenowe, współpracujące z dronami, robotyką, artylerią, cyberprzestrzenią i systemami AI.

Warstwa 4. Tarcza

IAMD, obrona powietrzna, przeciwrakietowa, counter-UAS, ochrona infrastruktury krytycznej, osłona energetyki, portów, lotnisk, kolei, centrów danych i węzłów administracji.

Warstwa 5. Miecz

Deep strike, długodystansowe ognie, rakiety, drony uderzeniowe, zdolności cybernetyczne i środki zakłócania systemów przeciwnika.

Warstwa 6. Tor zasilający

Energia, przemysł, łańcuchy dostaw, półprzewodniki, paliwa, amunicja, żywność, woda, leki, części zamienne i zdolność szybkiej produkcji.

Warstwa 7. Tor informacyjny

Kosmos, C4ISR, AI, cyberprzestrzeń, odporność kognitywna, łączność, rozpoznanie, fuzja danych, antydezinformacja i aktualny model rzeczywistości.

Zasada spinająca

Warstwy bojowo-technologiczne są skuteczne tylko wtedy, gdy opierają się na państwie z regulatorem i obywatelu. Technologia bez obywatela jest krucha. Obywatel bez państwa jest bezbronny. Państwo bez technologii jest spóźnione. Dopiero ich połączenie tworzy Rzeczpospolitą zdolną do obrony.

VIII. System Górskich Cytadel

Polska jest państwem nizinnym. Jej główne ośrodki administracyjne, przemysłowe, komunikacyjne i energetyczne są narażone na szybkie rozpoznanie, atak raketowy, sabotaż, blackout, cyberatak i presję CBRN: nuklearną, biologiczną i chemiczną. Dlatego [TechnoRepublika](#) proponuje budowę systemu głębokiej odporności strategicznej opartego o pas górski Sudetów i Karpat.

System Górskich Cytadel nie jest projektem ofensywnej militaryzacji gór. Jest programem przeżywalności państwa, ciągłości dowodzenia, ochrony danych, magazynowania strategicznego, odporności CBRN, obrony cywilnej oraz zabezpieczenia infrastruktury krytycznej. Jego szczegóły techniczne muszą pozostać niejawne, zgodne z prawem, interoperacyjne z NATO i poddane kontroli konstytucyjnej.

1. Cytadela Karkonoska

Funkcja: centralne dowództwo państwa, zapasowa siedziba Prezydenta, centrum ciągłości działania egzekutywy, zabezpieczenie zachodnie oraz strategiczne połączenie z kierunkiem niemieckim i czeskim.

Zadania:

- zapasowe centrum kierowania państwem,
- bezpieczne centrum danych prezydenckich i administracyjnych,
- węzeł komunikacji kryzysowej,
- centrum strategicznej analizy sytuacyjnej,
- ośrodek dowodzenia w warunkach zakłócenia stolicy.

2. Cytadela Sudecka

Funkcja: magazyny strategiczne i infrastruktura odporności w Górach Sowich, Wąbrzyskich i Kamiennych; zabezpieczenie korytarza S3, portów Szczecin–Świnoujście oraz osi współpracy z Czechami.

Zadania:

- magazyny energii, paliw, części, żywności, wody i leków,
- centrum cyberbezpieczeństwa infrastruktury krytycznej,
- zaplecze dla energetyki, samorządów i służb,
- ochrona logistyczna południowo-zachodniej Polski,
- hub odbudowy funkcji państwa po uderzeniu infrastrukturalnym.

3. Cytadela Beskidu Zachodniego

Funkcja: kontrola i zabezpieczenie korytarzy A4, A1, A2, portów Gdynia–Gdańsk oraz kierunku Morawy–Śląsk–Małopolska.

Zadania:

- zabezpieczenie osi logistycznych północ–południe i wschód–zachód,
- wsparcie dla przemysłu śląskiego i małopolskiego,
- rozproszone centrum transportu strategicznego,
- zaplecze naprawcze i produkcyjne,
- koordynacja obrony infrastruktury drogowej, kolejowej i energetycznej.

4. Cytadela Tatrzańska

Funkcja: silny ośrodek odporności na osi wschodniej i południowej, z zapleczem dla kierunku Słowacja–Węgry oraz dla strategicznej głębi państwa.

Zadania:

- centrum wysokogórskiej odporności CBRN,
- zaplecze dla rozpoznania i łączności,
- infrastruktura przeżywalności dla kluczowych funkcji państwa,
- wsparcie dla południowego skrzydła obrony,
- zabezpieczenie kierunków karpackich.

5. Cytadela Beskidu Wschodniego

Funkcja: szpica odporności i oddziaływania strategicznego na kierunku wschodnim, obejmującym przestrzeń zagrożeń z obszaru Ukrainy, Rosji i Białorusi.

Zadania:

- wczesne ostrzeżenie i rozpoznanie,
- odporna łączność i zapasowe systemy dowodzenia,
- zabezpieczenie wschodnich korytarzy logistycznych,
- magazyny i zaplecze dla długotrwałej odporności,
- integracja z obroną wschodniej flanki NATO.

System Górskich Cytadel ma trzy sensory: przeżywalność, odstraszenie i ciągłość. Przeciwnik musi wiedzieć, że nawet po uderzeniu w miasta, centra danych, węzły energetyczne i administrację centralną państwo polskie będzie nadal widzieć, decydować, komunikować się, produkować, odpowiadać i trwać.

IX. Zasady wdrożenia

1. Najpierw odporność, potem prestiż

Zakupy prestiżowe nie mogą wyprzedzać zdolności podstawowych: obrony powietrznej, amunicji, dronów, counter-UAS, schronów, rezerw, energetyki, łączności i produkcji.

2. Masa precyzji zamiast masy platform

Nie wolno budować obrony wyłącznie na drogich platformach podatnych na tanią precyzję przeciwnika. Potrzebna jest równowaga: zaawansowane systemy, ale także tania, masowa, odnawialna zdolność rażenia i rozpoznania.

3. Produkować w kraju to, co krytyczne

Polska musi produkować albo współprodukować to, bez czego nie może prowadzić obrony: amunicję, drony, sensory, łączność, systemy energetyczne, software, części zamienne i wybrane komponenty rakietowe.

4. Software-defined defense

Każdy system obronny musi być projektowany jako modułowy, aktualizowalny i interoperacyjny. Przewagę daje nie tylko stal, lecz także kod, dane, aktualizacja i integracja.

5. Obywatel jako uczestnik

Bez obywatela nie ma odporności. Powszechne szkolenie, obrona cywilna, rezerwy, samorządy, szkoły i wspólnoty lokalne są częścią systemu obrony.

6. AI pod prawem i z człowiekiem w pętli

Sztuczna inteligencja wspiera rozpoznanie, analizę i decyzję, ale odpowiedzialność za użycie siły pozostaje po stronie człowieka i państwa prawa.

7. Uczyć się szybciej od przeciwnika

Każda jednostka, agencja, cytadela i program technologiczny musi działać w pętli uczenia: ćwiczenie, błąd, korekta, aktualizacja, wdrożenie. Państwo, które nie uczy się w czasie rzeczywistym, przegrywa z przeciwnikiem adaptacyjnym.

X. Dziesięć haseł Narodowej Obrony TechnoRepubliki

1. **Obrona to system odporności państwa, nie tylko wojsko.**
2. **TechnoRepublika: wojsko, obywatel, AI, energia i produkcja.**
3. **Uczynić agresję nieopłacalną i nierozstrzygalną.**
4. **Masa precyzji zamiast masy platform.**
5. **Produkcja jest odstraszeniem.**
6. **Suwerenność to kontrola danych, energii, software'u i produkcji.**
7. **Drony, rakiety, kosmos — pod kontrolą obywatelską.**
8. **Cytadele Górskie — ciągłość państwa mimo uderzenia.**
9. **AI w służbie obrony, człowiek w pętli decyzji.**
10. **Sprawcza obrona bez militarizmu: siła państwa pod kontrolą Narodu.**

XI. Konkluzja

Obrona Narodowa Rzeczypospolitej jest doktryną państwa, które rozumie realia XXI wieku. Polska nie może bronić się wyłącznie pamięcią historyczną, zakupami katalogowymi i deklaracjami sojuszniczymi. Musi stać się państwem, które samo widzi, samo rozumie, samo produkuje, samo bilansuje energię, samo szkoli obywateli i samo utrzymuje ciągłość działania pod presją.

Rzeczpospolita nie buduje obrony po to, by prowadzić wojny. Buduje ją po to, by wojna przeciw Polsce nigdy się nie opłacała.

To jest sens doktryny: **sprawcze państwo, odporny Naród, suwerenna technologia, własna energia, własna produkcja i demokratyczna kontrola nad siłą.**

Aneks A. Słownik pojęć, terminów i skrótów

Słownik obejmuje pojęcia użyte w niniejszej publikacji. Definicje podano w znaczeniu, w jakim terminy występują w doktrynie Obrony Narodowej Rzeczypospolitej; tam, gdzie termin ma szersze znaczenie ogólne, wskazano jego zastosowanie w dokumencie. Pełne odesłania źródłowe zawiera osobny załącznik bibliograficzny.

A.1. Skróty, akronimy i oznaczenia

Skrót	Rozwinięcie	Znaczenie w dokumencie
A2/AD	Anti-Access / Area Denial — antydzostęp i ograniczanie swobody działania	Zespół zdolności przeciwnika utrudniających wejście sił sojuszników w rejon operacji i swobodę manewru w nim; w warunkach polskich wiązany z obwodem kaliningradzkim i Bałtykiem.
AI	Artificial Intelligence — sztuczna inteligencja	Narzędzie wspomagania rozpoznania, analizy i decyzji; nigdy samodzielny podmiot użycia siły.
C2	Command and Control — dowodzenie i kierowanie	Funkcja regulatora w wymiarze wojskowym: przyjmowanie informacji, podejmowanie decyzji i przekazywanie zadań.
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance	Zintegrowany system dowodzenia, łączności, obliczeń i rozpoznania — techniczne wykonanie modelu rzeczywistości państwa.
CBRN	Chemical, Biological, Radiological, Nuclear	Zagrożenia chemiczne, biologiczne, radiologiczne i nuklearne; przedmiot odporności cytael i obrony cywilnej.
counter-UAS	Counter Unmanned Aircraft Systems	Zwalczanie bezzałogowych statków powietrznych; w doktrynie priorytet równy systemom bezzałogowym.
EW	Electronic Warfare — walka radioelektroniczna	Rozpoznanie, zakłócanie i obrona w widmie elektromagnetycznym; domena podstawowa, nie wsparcie.
FIMI	Foreign Information Manipulation and Interference	Zagraniczna manipulacja informacyjna i ingerencja — atak na tor sterowniczy państwa.
FPV	First Person View	Dron sterowany z widoku operatora, tania masowa amunicja precyzyjna pola walki.
GNSS	Global Navigation Satellite System	Satelitarne systemy nawigacji; przedmiot zakłócania i podszywania, stąd wymóg odporności PNT.

Skrót	Rozwinięcie	Znaczenie w dokumencie
HPM	High Power Microwave — broń mikrofalowa dużej mocy	Efektor obszarowy o niskim koszcie strzału, przeciw rojom bezzałogowców.
IAMD	Integrated Air and Missile Defence	Zintegrowana obrona powietrzna i przeciwrakietowa; warstwa „tarczy”.
ISR	Intelligence, Surveillance, Reconnaissance	Rozpoznanie, dozór i obserwacja — funkcja receptora układu obronnego.
KPI	Key Performance Indicator	Kluczowy wskaźnik wykonania: miernik osiągnięcia efektu, z właścicielem i progiem.
KRI	Key Risk Indicator	Kluczowy wskaźnik ryzyka: miernik wczesnego ostrzegania o odchyleniu zagrażającym zdolności.
MDO	Multi-Domain Operations — operacje wielodomenowe	Prowadzenie działań jednocześnie na lądzie, w powietrzu, na morzu, w cyberprzestrzeni, kosmosie i widmie.
OODA	Observe–Orient–Decide–Act	Pętla decyzyjna Boyda; miarą przewagi jest szybkość jej domykania.
OWA UAV	One-Way Attack UAV	Bezzałogowiec jednorazowego użycia (amunicja krążąca dalekiego zasięgu); narzędzie saturacji.
PNT	Positioning, Navigation and Timing	Pozycjonowanie, nawigacja i czas; warunek działania precyzji, łączności i energetyki.
SATCOM	Satellite Communications	Łączność satelitarna; element toru sterowniczego o wysokiej centralności.
UAV / UGV / USV / UUV	Unmanned Aerial / Ground / Surface / Underwater Vehicle	Platformy bezzałogowe powietrzne, lądowe, nawodne i podwodne.
VSM	Viable System Model — Model Systemów Żywności	Model Beera: pięć systemów koniecznych do przetrwania organizacji na każdym poziomie rekurencji.
3A	Antycypacja – Absorpcja – Adaptacja	Model porządkujący TechnoSanacji; trzy zdolności sprawdzające każdy element systemu obrony.

A.2. Pojęcia cybernetyczne

Pojęcie	Znaczenie w dokumencie
Cybernetyka	Nauka o sterowaniu i komunikacji w układach złożonych (Wiener, 1948). W doktrynie: język opisu obrony jako układu regulacyjnego.
Regulator	Podsystem utrzymujący wybrane zmienne układu w wyznaczonych granicach mimo zakłóceń. W obronie: system kierowania obroną państwa z modelem rzeczywistości, uprawnieniami i odpowiedzialnością.
Twierdzenie o dobrym regulatorze	Conant–Ashby (1970): każdy dobry regulator układu musi być modelem tego układu. Podstawa obowiązku posiadania aktualnego obrazu sytuacyjnego państwa.
Prawo wymaganej różnorodności	Ashby: tylko różnorodność może pochłoniąć różnorodność. Regulator musi mieć repertuar odpowiedzi nie mniejszy niż repertuar zagrożeń — stąd wielodomenowość i wielopodmiotowość obrony.
Amplifikacja różnorodności	Zwiększanie repertuaru regulatora przez włączenie obywateli, samorządów i przedsiębiorstw. Cybernetyczne uzasadnienie obywatelskiego systemu obrony.
Układ samodzielny	Układ zdolny przeciwdziałać utracie zdolności sterowania (Mazur). Składa się z receptora, korelatora, efektora, homeostatu, akumulatora i alimentatora.
Receptor	Blok poboru informacji. W obronie: rozpoznanie satelitarne, dronowe, radiolokacyjne, cyberrozpoznanie, obserwacja obywatelska.
Korelator	Blok przetwarzania informacji w decyzje wraz z pamięcią norm i programów. W obronie: sztaby, analiza, systemy wspomagania decyzji, modele.
Efektor	Blok wykonania oddziaływań. W obronie: wojsko, służby, administracja, przemysł.
Homeostat	Blok samokorekty odróżniający zakłócenie od szumu. W obronie: kontrola konstytucyjna, sądy, Senat, audyt.
Akumulator / alimentator	Bloki gromadzenia i zasilania energomaterią. W obronie: rezerwy i magazyny oraz energetyka i przemysł.
Organizator	Organ zdolny zmienić program własnego układu (Kossecki). W państwie: władza ustrojodawcza i referendum — nie egzekutywa.
Tor sterowniczy	Kanał informacji, którym układ steruje: dane, łączność, kosmos, oprogramowanie, modele, przekaz publiczny.
Tor zasilający	Kanał energomaterii umożliwiający wykonanie: energia, paliwa, amunicja, komponenty, żywność, leki, części.

Pojęcie	Znaczenie w dokumencie
Moc swobodna	Zasób, którym układ dysponuje na samodzielne działanie. W obronie: niezaangażowana rezerwa zdolności, zapasów i mocy produkcyjnych.
Czas decyzyjny	Czas od zarejestrowania bodźca do wykonania odpowiedzi. Struktura obrony ma go minimalizować, a nie chronić hierarchię.
Sygnał algedoniczny	Kanał alarmowy omijający hierarchię (Beer), przenoszący informację o zdarzeniu krytycznym, dla którego nie przewidziano wskaźnika.
Model Systemów Żywnotnych	Pięć systemów Beera: operacje, koordynacja, zarządzanie z audytem, rozpoznanie przyszłości, tożsamość i polityka — obecne na każdym poziomie rekurencji.
Rekurencja	Powtarzalność pełnej struktury sterowania na kolejnych poziomach: państwo, region, gmina, jednostka, zakład. Obrona wyłącznie centralna nie jest układem żywotnym.
Sprzężenie zwrotne	Powrót informacji o wyniku działania w postaci zdolnej zmienić następną decyzję. Sprawozdanie bez obowiązku reakcji nie jest sprzężeniem.
Pętla decyzyjna (OODA)	Cykl obserwacji, orientacji, decyzji i działania. Przewagę uzyskuje strona domykająca cykl szybciej.
Płaski tor informacyjny	Zasada, wedle której dane trafiają wprost do poziomu zdolnego podjąć decyzję i ponoszącego za nią odpowiedzialność.
Płaski tor zasilający	Zasada rozproszenia zaopatrzenia, energii i zapasów tak, by żaden pojedynczy magazyn, sieć ani dostawca nie warunkował działania systemu.
Pojemność kanału	Maksymalna ilość informacji przenoszona przez kanał (Shannon). Każdy zbędny szczebel pośredni wprowadza opóźnienie i szum.
Sterowanie pośrednie	Przejęcie nie organów, lecz programu w korelatorze — przez standardy, oprogramowanie, ekspertów i przekaz. Najgroźniejsza forma utraty suwerenności obronnej.

A.3. Pojęcia systemowe i odpornościowe

Pojęcie	Znaczenie w dokumencie
Odporność (resilience)	Zdolność utrzymania funkcji krytycznych mimo zakłócenia i powrotu do stanu zdadności. W doktrynie: trzeci mechanizm odstraszenia.
Model 3A	Antycypacja, Absorpcja, Adaptacja — trzy pytania testujące każdy element systemu obrony: czy widzimy zawczasu, czy wytrzymamy, czy zdążymy się przebudować.

Pojęcie	Znaczenie w dokumencie
Awaria normalna	Teza Perrowa: w układach złożonych i ściśle sprzężonych awarie są własnością konstrukcji, a nie odchyleniem. Uzasadnia procedury ręczne i luzy.
Ściśle sprzężenie	Stan, w którym elementy układu zależą od siebie bez zapasu czasu i zasobu, przez co zakłócenie rozchodzi się szybciej, niż da się je zrozumieć.
Luz systemowy (slack)	Celowy nadmiar zasobu, czasu lub przepustowości, pochłaniający zakłócenie zamiast przenosić je dalej. Ekonomicznie „nieefektywny”, obronnie konieczny.
Redundancja	Powielenie funkcji krytycznej w niezależnych elementach, tak aby utrata jednego nie usuwała funkcji.
Degradacja łagodna	Projektowanie systemu tak, by pod obciążeniem tracił zdolności stopniowo i w kontrolowanej kolejności, zamiast załamywać się skokowo.
Obrona wielowarstwowa	Zasada, wedle której żadna pojedyncza warstwa nie jest wystarczająca, a każda kolejna przechwytuje to, co przeszło przez poprzednią.
Organizacja wysokiej niezawodności	Organizacja utrzymująca zdatność mimo stałego ryzyka dzięki czujności, niechęci do upraszczania i przenoszeniu decyzji do miejsca kompetencji (Weick, Sutcliffe).
Punkt dźwigni	Miejsce w systemie, w którym mała interwencja daje dużą zmianę (Meadows). Reguła jest silniejszym punktem dźwigni niż parametr budżetowy.
Antykruchość	Własność układu, który poprawia się wskutek obciążenia (Taleb). Wymaga zapasu na przeżycie pierwszego wstrząsu i produkcji zdolnej wdrożyć wnioski.
Pojedynczy punkt awarii	Element, którego utrata usuwa funkcję całego systemu, ponieważ nie istnieje uruchamialna druga ścieżka.
Ciągłość działania	Zdolność państwa do nieprzerwanego wykonywania funkcji krytycznych mimo utraty siedzib, systemów lub zasilania.
Zdolność odbudowy	Zdolność odtworzenia infrastruktury, energetyki i administracji po uderzeniu; warunek zwycięstwa politycznego po wygranej militarnej.
Rejestr ryzyk wojennych	Uporządkowany wykaz ryzyk z opisem, wskaźnikiem wczesnego ostrzegania, właścicielem, budżetem redukcji i wariantem awaryjnym.
Wargaming	Systematyczne rozgrywanie scenariuszy konfliktu w celu wykrycia założeń fałszywych przed ich weryfikacją przez przeciwnika.

Pojęcie	Znaczenie w dokumencie
Red teaming	Celowa krytyka własnych planów z perspektywy przeciwnika; instytucjonalny mechanizm negatywnego sprzężenia zwrotnego.
Net assessment	Porównawcza ocena zdolności własnych i przeciwnika w dłuższym horyzoncie, obejmująca trendy, koszty i zdolność adaptacji.

A.4. Pojęcia sieciowe

Pojęcie	Znaczenie w dokumencie
Sieć bezskalowa	Sieć o rozkładzie potęgowym liczby połączeń, z nielicznymi węzłami o bardzo wielu połączeniach. Taką strukturę mają sieci energetyczne, transportowe i teleinformatyczne.
Odporna, lecz krucha	Własność sieci bezskalowych: znosi losowe awarie, rozpada się przy celowanym uderzeniu w huby (Albert, Jeong, Barabási). Awaria jest losowa — przeciwnik nie jest.
Hub	Węzeł o nieproporcjonalnie dużej liczbie połączeń. Cel pierwszorzędny racjonalnego przeciwnika; przedmiot dekoncentracji lub osłony.
Centralność pośrednictwa	Miara liczby najkrótszych ścieżek przechodzących przez węzeł. Wskazuje wąskie gardła, których usunięcie rozcina sieć mimo niewielkiej liczby połączeń.
Druga ścieżka	Alternatywna trasa przepływu dla węzła krytycznego, o określonym koszcie uruchomienia i czasie przetoczenia. Brak drugiej ścieżki definiuje pojedynczy punkt awarii.
Sieci współzależne	Dwie lub więcej sieci, w których działanie jednej warunkuje działanie drugiej — typowo energetyka i teleinformatyka.
Kaskada awarii	Przenoszenie się uszkodzenia między sieciami współzależnymi, prowadzące do rozpadu skokowego przy uszkodzeniu mniejszym niż próg pojedynczej sieci (Buldyrev i in.).
Praca wyspowa	Zdolność fragmentu sieci energetycznej do samodzielnej pracy po odłączeniu od systemu; przerywa kaskadę.
Uruchomienie bez zasilania zewnętrznego	Zdolność podniesienia systemu energetycznego od zera, bez pomocy sieci; warunek odbudowy po rozległym zaniku zasilania.
Łańcuch rażenia	Szeregowa sekwencja wykrycia, identyfikacji, wskazania, uderzenia i oceny. Ma tyle punktów awarii, ile ogniów.
Sieć rażenia	Architektura, w której każdy sensor może zasilić każdy efektor, a utrata elementu powoduje przekierowanie zamiast przerwania.

Pojęcie	Znaczenie w dokumencie
Prawo Conwaya	Struktura budowanego systemu odwzorowuje strukturę komunikacyjną organizacji, która go tworzy. Integracja mandatu musi poprzedzać integrację systemów.
Uzależnienie od dostawcy	Stan, w którym zmiana dostawcy technologii jest niemożliwa lub nieopłacalna. W ujęciu sieciowym: dobrowolne oddanie huba o maksymalnej centralności.
Siła słabych więzi	Teza Granovettera: informację nową przenoszą kontakty spoza własnego środowiska. Uzasadnia obywatelską sieć obserwacji i pluralizm źródeł.
Odporność kognitywna	Zdolność społeczeństwa do rozpoznania manipulacji i utrzymania spójności poznawczej pod presją informacyjną.
Uodpornianie wyprzedzające	Uprzedzające ujawnienie mechanizmu manipulacji, uodporniające odbiorcę bez konieczności kontroli treści.

A.5. Pojęcia militarne i operacyjne

Pojęcie	Znaczenie w dokumencie
Odstraszanie przez odmowę	Przekonanie przeciwnika, że agresja nie osiągnie celu operacyjnego (Snyder). Logika pierwszorzędna państwa frontowego, bo sprawdzalna.
Odstraszanie przez karanie	Groźba nieakceptowalnego kosztu wymierzonego po agresji. Wymaga wiary przeciwnika w naszą determinację.
Odporność jako odstraszanie	Zniechęcenie przeciwnika przez odebranie sensu uderzeniu: państwo działające mimo presji nie daje się złamać szybko ani tanio.
Produkcja jako odstraszanie	Widoczna, głęboka i szybka zdolność wytwórcza skracająca horyzont, w którym przeciwnik może prowadzić wojnę na wyczerpanie z korzyścią.
Sterowanie eskalacją	Świadome kształtowanie poziomu i tempa konfliktu tak, by nie tracić inicjatywy ani nie przekraczać progów katastrofalnych.
Wymiana kosztów	Relacja kosztu ataku do kosztu obrony. Reguła projektowa: tani środek masowy zwalcza się środkiem o koszcie porównywalnym lub niższym.
Koszt zniszczenia celu	Pełny koszt doprowadzenia do zniszczenia jednego celu, obejmujący rozpoznanie, decyzję, efektor i logistykę.
Głębokość magazynka	Liczba dni intensywnej walki pokrywana zapasem amunicji, rakiet, pocisków przechwytyjących, paliw i części.

Pojęcie	Znaczenie w dokumencie
Tempo odtwarzania	Zdolność wyprodukowania zużytego środka w horyzontach trzydziestu, czterdziestu i stu osiemdziesięciu dni.
Saturacja	Nasycenie obrony liczbą celów przekraczającą jej zdolność jednoczesnego zwalczania; podstawowa metoda przełamania tarczy.
Masa precyzji	Duża liczba tanich środków precyzyjnego rażenia, zastępująca małą liczbę drogich platform.
Amunicja krążąca	Bezzałogowy środek rażenia zdolny do dłuższego przebywania nad rejonem i uderzenia po wykryciu celu.
Przejrzyste pole walki	Stan powszechnej obserwacji, w którym wykrycie zgrupowania jest niemal pewne, a koncentracja staje się celem.
Sensor–efektor	Skrócone połączenie rozpoznania z środkiem rażenia, mierzone czasem od wykrycia do uderzenia.
Wojsko nowego wzoru	Siły zaprojektowane wokół efektu, rozproszenia, taniej precyzji i odpowiedzialności zadaniowej, a nie wokół struktury etatowej i prestiżu platform.
Dowodzenie zadaniowe	Sposób dowodzenia, w którym przełożony wyznacza cel i ograniczenia, a wykonawca dobiera sposób działania; warunek krótkiej pętli decyzyjnej.
Human-machine teaming	Współdziałanie żołnierza z systemami bezzałogowymi i autonomicznymi przy zachowaniu odpowiedzialności człowieka.
Człowiek w pętli / w dowodzeniu	Zasada, wedle której decyzja o użyciu siły pozostaje przy człowieku, który rozumie cel systemu i ponosi odpowiedzialność.
Tarcza	Warstwa obrony: przeciwlotnicza, przeciwrakietowa, przeciw bezzałogowcom oraz ochrona infrastruktury krytycznej.
Miecz	Warstwa oddziaływania: długodystansowe ognie, rakiety precyzyjne, bezzałogowce dalekiego zasięgu, środki cybernetyczne.
Rażenie w głąb	Zdolność uderzania w systemy rozpoznania, logistyki i dowodzenia przeciwnika poza strefą styczności.
Obrona totalna	Model, w którym obrona jest zadaniem całego społeczeństwa i gospodarki, nie tylko sił zbrojnych.
Obrona cywilna	Ochrona ludności, schrony, ostrzeganie, ewakuacja, ratownictwo i logistyka społeczna w warunkach kryzysu i wojny.
Rezerwy	Przeszkoleni obywatele przypisani do zadań obronnych oraz zapasy materiałowe umożliwiające prowadzenie działań długotrwałych.

Pojęcie	Znaczenie w dokumencie
Przemysł dual use	Zdolności wytwórcze użyteczne jednocześnie cywilnie i wojskowo, umożliwiające szybkie przestawienie produkcji.
Cytadela	Rozproszony, chroniony węzeł ciągłości państwa: dowodzenia, danych, zaopatrzenia, odporności CBRN i odbudowy funkcji publicznych.
Państwo frontowe	Państwo położone na głównej osi zagrożenia, dla którego czas ostrzegania jest krótki, a głębia strategiczna ograniczona.

A.6. Pojęcia ustrojowe i programowe TechnoRepubliki

Pojęcie	Znaczenie w dokumencie
TechnoSanacja	Droga naprawy państwa: metoda przejścia od diagnozy do sprawczości, oparta na cybernetycznym ujęciu instytucji.
TechnoRepublika	Cel ustrojowy: państwo sprawcze, przewidujące i rozliczalne wobec obywatela, sterowane w oparciu o dane i odpowiedzialność.
Formuła naczelna	Zdanie definiujące przedmiot dokumentu przez wskazanie miar i warunków koniecznych; podlega uzasadnieniu i falsyfikacji.
Sprawcze państwo z regulatorem	Wymaganie konstrukcyjne: istnienie wyodrębnionego, wyposażonego i rozliczalnego podsystemu sterowania obroną, a nie tylko metafora państwa sprawnego.
Obywatelski system obrony	Zorganizowane uczestnictwo obywateli w obronie: szkolenie, rezerwy, obrona cywilna, lokalne zespoły odporności, sieć ostrzegania.
Suwerenna technologia	Kontrola danych, oprogramowania, modeli, łączy, kosmosu i kluczy kryptograficznych oraz realna możliwość zmiany dostawcy.
Odporność energetyczna	Zdolność zasilania obrony, danych i gospodarki mimo zakłóceń: rozproszenie, praca wyspowa, magazyny, wielonośnikowość, własna sterowalność.
Siedem warstw obrony	Architektura doktryny: państwo-regulator, obywatel, manewr, tarcza, miecz, tor zasilający, tor informacyjny.
Pięć linii wysiłku	Kierunki realizacji: wojsko nowego wzoru, obywatelski system obrony, domena cyfrowa, tarcza i miecz rakietowy, arsenał przemysłowo-energetyczny.
Zasada spinająca	Reguła, wedle której warstwy bojowo-technologiczne są skuteczne wyłącznie na fundamencie sprawczego regulatora i zaangażowanego obywatela.

Pojęcie	Znaczenie w dokumencie
Kontrola republikańska obrony	Nadzór Senatu, sądów i audytu nad budżetem, agencjami, stanami nadzwyczajnymi, zakupami i algorytmami bezpieczeństwa.
Warunek falsyfikacji	Twierdzenie, którego prawdziwość obalałaby doktrynę; jego wskazanie odróżnia doktrynę sprawdzalną od deklaracji.

Załącznik. Bibliografia

Załącznik zawiera podstawy źródłowe uzasadnień cybernetycznego, systemowego, sieciowego i militarnego oraz pozostałych rozdziałów publikacji „Obrona Narodowa”. Pozycje uporządkowano w szesnastu klastrach tematycznych odpowiadających strukturze wywodu, nie porządkowi alfabetycznemu — tak, aby załącznik służył jako mapa literatury dla każdego z członów formuły naczelnej.

B.1. Cybernetyka, teoria sterowania i regulacji

1. Wiener, N. (1948), *Cybernetics: or Control and Communication in the Animal and the Machine*, MIT Press, Cambridge MA.
2. Wiener, N. (1950), *The Human Use of Human Beings: Cybernetics and Society*, Houghton Mifflin, Boston.
3. Ashby, W.R. (1956), *An Introduction to Cybernetics*, Chapman & Hall, Londyn.
4. Ashby, W.R. (1952), *Design for a Brain: The Origin of Adaptive Behaviour*, Chapman & Hall, Londyn.
5. Ashby, W.R. (1958), *Requisite Variety and Its Implications for the Control of Complex Systems*, „Cybernetica” 1(2), s. 83–99.
6. Conant, R.C., Ashby, W.R. (1970), *Every Good Regulator of a System Must Be a Model of That System*, „International Journal of Systems Science” 1(2), s. 89–97.
7. Shannon, C.E. (1948), *A Mathematical Theory of Communication*, „The Bell System Technical Journal” 27(3), s. 379–423 oraz 27(4), s. 623–656.
8. Shannon, C.E., Weaver, W. (1949), *The Mathematical Theory of Communication*, University of Illinois Press, Urbana.
9. Beer, S. (1972), *Brain of the Firm: The Managerial Cybernetics of Organization*, Allen Lane, Londyn.
10. Beer, S. (1979), *The Heart of Enterprise*, John Wiley & Sons, Chichester.
11. Beer, S. (1985), *Diagnosing the System for Organizations*, John Wiley & Sons, Chichester.
12. Beer, S. (1974), *Designing Freedom*, Canadian Broadcasting Corporation, Toronto.
13. Espejo, R., Harnden, R. (red.) (1989), *The Viable System Model: Interpretations and Applications of Stafford Beer's VSM*, John Wiley & Sons, Chichester.
14. Espejo, R., Reyes, A. (2011), *Organizational Systems: Managing Complexity with the Viable System Model*, Springer, Berlin–Heidelberg.
15. Schwaninger, M. (2006), *Intelligent Organizations: Powerful Models for Systemic Management*, Springer, Berlin.
16. von Foerster, H. (2003), *Understanding Understanding: Essays on Cybernetics and Cognition*, Springer, Nowy Jork.
17. Powers, W.T. (1973), *Behavior: The Control of Perception*, Aldine, Chicago.

18. Medina, E. (2011), *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile*, MIT Press, Cambridge MA.
19. Forrester, J.W. (1961), *Industrial Dynamics*, MIT Press, Cambridge MA.
20. Sterman, J.D. (2000), *Business Dynamics: Systems Thinking and Modeling for a Complex World*, Irwin/McGraw-Hill, Boston.

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

21. Mazur, M. (1966), *Cybernetyczna teoria układów samodzielnych*, Państwowe Wydawnictwo Naukowe, Warszawa.
22. Mazur, M. (1970), *Jakościowa teoria informacji*, Wydawnictwa Naukowo-Techniczne, Warszawa.
23. Mazur, M. (1976), *Cybernetyka i charakter*, Państwowy Instytut Wydawniczy, Warszawa.
24. Kossecki, J. (1981), *Cybernetyka społeczna*, Państwowe Wydawnictwo Naukowe, Warszawa (wyd. 1: 1975).
25. Kossecki, J. (1984), *Cybernetyka kultury*, Państwowy Instytut Wydawniczy, Warszawa.
26. Kossecki, J. (1996), *Naukowe podstawy nacjonalizmu*, Wydawnictwo Wyższej Szkoły Pedagogicznej, Kielce.
27. Kossecki, J. (2001), *Wzajemne oddziaływania państw jako układów sterowniczych*, Wydawnictwo Akademii Świętokrzyskiej, Kielce.
28. Kossecki, J. (2005), *Metacybernetyka*, Kielce–Warszawa.
29. Kossecki, J. (2002), *Elementy nowoczesnej wiedzy o sterowaniu ludźmi: socjotechnika, socjocybernetyka, psychocybernetyka*, Wydawnictwo Akademii Świętokrzyskiej, Kielce.
30. Wilsz, J. (2005), *Samosterowność jako właściwość układu autonomicznego*, Wydawnictwo Wyższej Szkoły Pedagogicznej, Częstochowa.
31. Lange, O. (1965), *Wstęp do cybernetyki ekonomicznej*, Państwowe Wydawnictwo Naukowe, Warszawa.
32. Greniewski, H. (1959), *Cybernetyka niematematyczna*, Państwowe Wydawnictwo Naukowe, Warszawa.
33. Zaniewski, Z. (1979), *Cybernetyczne aspekty organizacji i zarządzania*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

B.3. Teoria systemów, niezawodność i inżynieria odporności

34. Bertalanffy, L. von (1968), *General System Theory: Foundations, Development, Applications*, George Braziller, Nowy Jork.
35. Simon, H.A. (1962), *The Architecture of Complexity*, „Proceedings of the American Philosophical Society” 106(6), s. 467–482.
36. Simon, H.A. (1996), *The Sciences of the Artificial*, wyd. 3, MIT Press, Cambridge MA.
37. Perrow, C. (1984), *Normal Accidents: Living with High-Risk Technologies*, Basic Books, Nowy Jork.
38. Weick, K.E., Sutcliffe, K.M. (2007), *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*, Jossey-Bass, San Francisco.
39. Hollnagel, E., Woods, D.D., Leveson, N. (red.) (2006), *Resilience Engineering: Concepts and Precepts*, Ashgate, Aldershot.
40. Hollnagel, E. (2011), *Resilience Engineering in Practice: A Guidebook*, Ashgate, Farnham.
41. Reason, J. (1997), *Managing the Risks of Organizational Accidents*, Ashgate, Aldershot.
42. Leveson, N. (2011), *Engineering a Safer World: Systems Thinking Applied to Safety*, MIT Press, Cambridge MA.
43. Holling, C.S. (1973), *Resilience and Stability of Ecological Systems*, „Annual Review of Ecology and Systematics” 4, s. 1–23.

44. Meadows, D.H. (1999), *Leverage Points: Places to Intervene in a System*, The Sustainability Institute, Hartland.
45. Meadows, D.H. (2008), *Thinking in Systems: A Primer*, Chelsea Green Publishing, White River Junction.
46. Taleb, N.N. (2012), *Antifragile: Things That Gain from Disorder*, Random House, Nowy Jork.
47. Taleb, N.N. (2007), *The Black Swan: The Impact of the Highly Improbable*, Random House, Nowy Jork.
48. Holland, J.H. (1995), *Hidden Order: How Adaptation Builds Complexity*, Addison-Wesley, Reading MA.
49. Snowden, D.J., Boone, M.E. (2007), A Leader's Framework for Decision Making, „Harvard Business Review” 85(11), s. 68–76.
50. Miller, J.H., Page, S.E. (2007), *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, Princeton University Press, Princeton.
51. Scott, J.C. (1998), *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven.

B.4. Teoria sieci i odporność infrastruktury krytycznej

52. Barabási, A.-L., Albert, R. (1999), Emergence of Scaling in Random Networks, „Science” 286(5439), s. 509–512.
53. Albert, R., Jeong, H., Barabási, A.-L. (2000), Error and Attack Tolerance of Complex Networks, „Nature” 406, s. 378–382.
54. Barabási, A.-L. (2016), *Network Science*, Cambridge University Press, Cambridge.
55. Watts, D.J., Strogatz, S.H. (1998), Collective Dynamics of 'Small-World' Networks, „Nature” 393, s. 440–442.
56. Newman, M.E.J. (2018), *Networks*, wyd. 2, Oxford University Press, Oksford.
57. Freeman, L.C. (1979), Centrality in Social Networks: Conceptual Clarification, „Social Networks” 1(3), s. 215–239.
58. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S. (2010), Catastrophic Cascade of Failures in Interdependent Networks, „Nature” 464, s. 1025–1028.
59. Vespignani, A. (2010), The Fragility of Interdependency, „Nature” 464, s. 984–985.
60. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001), Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, „IEEE Control Systems Magazine” 21(6), s. 11–25.
61. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J. (2000), Network Robustness and Fragility: Percolation on Random Graphs, „Physical Review Letters” 85(25), s. 5468–5471.
62. Cohen, R., Erez, K., ben-Avraham, D., Havlin, S. (2001), Breakdown of the Internet under Intentional Attack, „Physical Review Letters” 86(16), s. 3682–3685.
63. Granovetter, M.S. (1973), The Strength of Weak Ties, „American Journal of Sociology” 78(6), s. 1360–1380.
64. Burt, R.S. (1992), *Structural Holes: The Social Structure of Competition*, Harvard University Press, Cambridge MA.
65. Conway, M.E. (1968), How Do Committees Invent?, „Datamation” 14(4), s. 28–31.
66. Castells, M. (1996), *The Rise of the Network Society*, Blackwell, Oksford.
67. Arquilla, J., Ronfeldt, D. (2001), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND Corporation, Santa Monica.
68. Alberts, D.S., Garstka, J.J., Stein, F.P. (1999), *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP, Waszyngton.
69. Metcalfe, B. (2013), Metcalfe's Law after 40 Years of Ethernet, „Computer” 46(12), s. 26–31.

B.5. Teoria odstraszania, strategii i wojny

70. Clausewitz, C. von (1832), *Vom Kriege*, Dümmlers Verlag, Berlin; wyd. pol. *O wojnie*, Wydawnictwo Test, Lublin 1995.
71. Sun Tzu, *Sztuka wojny*, liczne wydania; wyd. pol. Państwowy Instytut Wydawniczy, Warszawa.
72. Snyder, G.H. (1961), *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, Princeton.
73. Schelling, T.C. (1960), *The Strategy of Conflict*, Harvard University Press, Cambridge MA.
74. Schelling, T.C. (1966), *Arms and Influence*, Yale University Press, New Haven.
75. Jervis, R. (1976), *Perception and Misperception in International Politics*, Princeton University Press, Princeton.
76. Mearsheimer, J.J. (1983), *Conventional Deterrence*, Cornell University Press, Ithaca.
77. George, A.L., Smoke, R. (1974), *Deterrence in American Foreign Policy: Theory and Practice*, Columbia University Press, Nowy Jork.
78. Freedman, L. (2004), *Deterrence*, Polity Press, Cambridge.
79. Luttwak, E.N. (1987), *Strategy: The Logic of War and Peace*, Harvard University Press, Cambridge MA.
80. Biddle, S. (2004), *Military Power: Explaining Victory and Defeat in Modern Battle*, Princeton University Press, Princeton.
81. Boyd, J.R. (1987), *A Discourse on Winning and Losing*, materiały wykładowe, U.S. Air Force.
82. Osinga, F.P.B. (2007), *Science, Strategy and War: The Strategic Theory of John Boyd*, Routledge, Londyn.
83. Lanchester, F.W. (1916), *Aircraft in Warfare: The Dawn of the Fourth Arm*, Constable and Company, Londyn.
84. Hughes, W.P. (2000), *Fleet Tactics and Coastal Combat*, wyd. 2, Naval Institute Press, Annapolis (model wymiany salw).
85. Iklé, F.C. (1971), *Every War Must End*, Columbia University Press, Nowy Jork.
86. Wylie, J.C. (1967), *Military Strategy: A General Theory of Power Control*, Rutgers University Press, New Brunswick.
87. Gray, C.S. (1999), *Modern Strategy*, Oxford University Press, Oksford.
88. Kahn, H. (1965), *On Escalation: Metaphors and Scenarios*, Praeger, Nowy Jork.
89. Beaufre, A. (1963), *Introduction à la stratégie*, Armand Colin, Paryż.

B.6. Wojna XXI wieku: doktryny operacyjne i wnioski z konfliktów

90. Royal United Services Institute (2023–2026), serie analiz o rozwoju taktycznym wojny na Ukrainie, w tym *Emergent Combined Arms* oraz *Tactical Developments during the Third Year of the War*, RUSI, Londyn.
91. Center for Strategic and International Studies (2024–2026), analizy pola walki i wojny dronowej, w tym *The Drone War* oraz *War on the Modern Battlefield*, CSIS, Waszyngton.
92. Center for a New American Security (2024–2026), analizy adaptacji sił zbrojnych i mas dronowych, CNAS, Waszyngton.
93. Center for Strategic and Budgetary Assessments (2019–2025), koncepcja mosaic warfare i rozproszonych architektur sił, CSBA, Waszyngton.
94. Hudson Institute (2020–2025), decision-centric warfare — koncepcje dowodzenia zorientowanego na decyzję, Hudson Institute, Waszyngton.
95. NATO Allied Command Transformation (2021–2025), *Multi-Domain Operations Concept* oraz materiały warsztatowe, NATO ACT, Norfolk.
96. International Institute for Strategic Studies (2024–2026), *The Military Balance* oraz analizy dotyczące europejskich zdolności obronnych, IISS, Londyn.

97. CNA (2023–2025), Russian Concepts of Future Warfare, CNA, Arlington.
98. Chatham House (2024–2025), analizy odbudowy potencjału militarnego Rosji, Chatham House, Londyn.
99. Institut français des relations internationales (2024–2025), Mapping the MilTech War — analiza adaptacji technologicznej na Ukrainie, Ifri, Paryż.
100. Ośrodek Studiów Wschodnich (2024–2026), analizy dotyczące wojny na Ukrainie, wojny dronowej i potencjału Rosji, OSW, Warszawa.
101. Polski Instytut Spraw Międzynarodowych (2024–2026), analizy bezpieczeństwa wschodniej flanki, PISM, Warszawa.
102. Fundacja im. Kazimierza Pułaskiego (2024–2026), raporty o modernizacji Sił Zbrojnych RP i współpracy przemysłowej, Warszawa.
103. Swedish Defence Research Agency (2020–2025), analizy A2/AD i obrony regionu bałtyckiego, FOI, Sztokholm.
104. RAND Corporation (2023–2025), Reinforcing Deterrence on NATO's Eastern Flank oraz analizy modernizacji Wojska Polskiego, RAND, Santa Monica.
105. Center for European Policy Analysis (2023–2026), analizy odstraszenia i odporności wschodniej flanki, CEPA, Waszyngton.

B.7. Bezzałogowce, autonomia, zwalczanie dronów i walka radioelektroniczna

106. Royal United Services Institute (2023–2025), Mass Precision Strike — koncepcja taniej masy precyzyjnej, RUSI, Londyn.
107. Center for a New American Security (2022–2025), analizy rojów bezzałogowców i przeciwdziałania im, CNAS, Waszyngton.
108. Joint Air Power Competence Centre (2021–2025), materiały dotyczące zwalczania bezzałogowych statków powietrznych, JAPCC, Kalkar.
109. Center for Strategic and International Studies (2024–2026), analizy saturacji dronowej i efektywności kosztowej uderzeń bezzałogowych, CSIS, Waszyngton.
110. International Institute for Strategic Studies (2026), Uninhabited Aerial Vehicles Dossier, IISS, Londyn.
111. Royal United Services Institute (2023–2025), analizy walki radioelektronicznej i konkurencji w widmie, RUSI, Londyn.
112. Congressional Research Service (2023–2025), Directed Energy Weapons: Background and Issues for Congress oraz raporty o Indirect Fire Protection Capability, CRS, Waszyngton.
113. Kyiv School of Economics / Brave1 (2024–2026), analizy ukraińskiego ekosystemu produkcji bezzałogowców, Kijów.
114. European Parliamentary Research Service (2025–2026), analizy europejskich inicjatyw przeciwdronowych, EPRS, Bruksela.
115. Australian Strategic Policy Institute (2023–2026), Critical Technology Tracker — analizy przewag technologicznych, ASPI, Canberra.

B.8. Obrona powietrzna i raketowa, ekonomia wymiany kosztów

116. Center for Strategic and International Studies (2023–2026), Distributed Defense oraz analizy nowej wojny salw, CSIS, Waszyngton.
117. International Institute for Strategic Studies (2024–2026), analizy zintegrowanej obrony powietrznej i raketowej w Europie, IISS, Londyn.
118. Royal United Services Institute (2023–2025), Rebalancing European Joint Fires, RUSI, Londyn.

119. Jewish Institute for National Security of America (2025), analizy zużycia pocisków przechwytyjących w konflikcie rakietowym 2025 roku, JINSA, Waszyngton.
120. Center for Strategic and International Studies (2023), Empty Bins in a Wartime Environment — analiza zapasów amunicji precyzyjnej, CSIS, Waszyngton.
121. Center for a New American Security (2023–2025), Production Is Deterrence — analizy zdolności wytwórczych jako elementu odstraszania, CNAS, Waszyngton.
122. RAND Corporation (2022–2025), analizy odstraszania zintegrowanego i zarządzania eskalacją, RAND, Santa Monica.
123. Center for Global Security Research (2024–2026), materiały warsztatowe o odstraszaniu i odstraszaniu wewnątrzwojennym, CGSR, Livermore.

B.9. Sztuczna inteligencja, C4ISR i obronność definiowana programowo

124. Karp, A.C., Zamiska, N.W. (2025), The Technological Republic: Hard Power, Soft Belief, and the Future of the West, Crown Currency, Nowy Jork.
125. Atlantic Council (2022–2025), Software-Defined Warfare — koncepcja przewagi programowej w obronności, Atlantic Council, Waszyngton.
126. Center for Security and Emerging Technology (2022–2026), analizy zastosowań sztucznej inteligencji w bezpieczeństwie, CSET, Waszyngton.
127. Special Competitive Studies Project (2023–2025), raporty o dowodzeniu i kierowaniu wspieranym przez AI, SCSP, Arlington.
128. United Nations Institute for Disarmament Research (2023–2026), analizy systemów wspomaganie decyzji opartych na AI w zastosowaniach wojskowych, UNIDIR, Genewa.
129. Stockholm International Peace Research Institute (2024–2026), analizy autonomicznych systemów uzbrojenia i systemów wspomaganie decyzji, SIPRI, Sztokholm.
130. International Committee of the Red Cross (2021–2025), stanowiska dotyczące autonomicznych systemów uzbrojenia i prawa humanitarnego, MKCK, Genewa.
131. National Institute of Standards and Technology (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, Gaithersburg.
132. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji, Dz.U. UE L 2024/1689.
133. Rada Europy (2024), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS nr 225, Wilno.
134. Russell, S. (2019), Human Compatible: Artificial Intelligence and the Problem of Control, Viking, Nowy Jork.

B.10. Cyberbezpieczeństwo, kosmos i odporność nawigacyjna

135. NATO Cooperative Cyber Defence Centre of Excellence (2020–2026), publikacje i materiały doktrynalne, CCDCOE, Tallinn.
136. European Union Agency for Cybersecurity (2024–2026), Threat Landscape — coroczne analizy krajobrazu zagrożeń, ENISA, Ateny.
137. Cybersecurity and Infrastructure Security Agency (2021–2025), Zero Trust Maturity Model oraz wytyczne ochrony infrastruktury krytycznej, CISA, Waszyngton.
138. Center for Strategic and International Studies (2024–2026), Space Threat Assessment — coroczna ocena zagrożeń w domenie kosmicznej, CSIS, Waszyngton.
139. Secure World Foundation (2024–2026), Global Counterspace Capabilities: An Open Source Assessment, SWF, Broomfield.

140. RAND Corporation (2022–2025), analizy odporności segmentu kosmicznego i bazy przemysłowej sektora kosmicznego, RAND, Santa Monica.
141. Aerospace Corporation (2022–2025), analizy odporności systemów pozycjonowania, nawigacji i czasu, El Segundo.
142. European External Action Service (2023–2025), raporty o zagranicznej manipulacji informacyjnej i ingerencji (FIMI), EEAS, Bruksela.
143. NATO Strategic Communications Centre of Excellence (2020–2026), analizy operacji informacyjnych i wojny kognitywnej, Ryga.
144. NATO Allied Command Transformation / Innovation Hub (2021), Cognitive Warfare: An Attack on Truth and Thought, Norfolk.
145. van der Linden, S. (2023), Foolproof: Why Misinformation Infects Our Minds and How to Build Immunity, W.W. Norton, Nowy Jork.
146. Roozenbeek, J., van der Linden, S. (2019), Fake News Game Confers Psychological Resistance Against Online Misinformation, „Palgrave Communications” 5, 65.
147. Thomas, T.L. (2004), Russia's Reflexive Control Theory and the Military, „Journal of Slavic Military Studies” 17(2), s. 237–256.
148. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa (NIS 2), Dz.U. UE L 333/80.
149. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych, Dz.U. UE L 333/164.

B.11. Obrona totalna, obrona cywilna i odporność społeczna

150. Niinistö, S. (2024), Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness, raport dla Komisji Europejskiej, Bruksela.
151. Komisja Europejska (2025), Preparedness Union Strategy, Bruksela.
152. Organizacja Traktatu Północnoatlantyckiego, Artykuł 3 Traktatu Waszyngtońskiego oraz siedem podstawowych wymagań odporności (baseline requirements), NATO, Bruksela.
153. International Institute for Strategic Studies (2024–2025), Civil Defence in Europe, IISS, Londyn.
154. Myndigheten för samhällsskydd och beredskap (2024), Om krisen eller kriget kommer — broszura informacyjna dla ludności, MSB, Sztokholm.
155. Finnish Security Committee (2017, akt. 2024), The Security Strategy for Society — model bezpieczeństwa kompleksowego, Helsinki.
156. International Centre for Defence and Security (2020–2025), analizy bałtyckich modeli obrony ochotniczej i terytorialnej, ICDS, Tallinn.
157. Ministry of National Defense of the Republic of China (2023–2025), All-out Defense Handbook oraz Quadrennial Defense Review, Tajpej.
158. Carnegie Endowment for International Peace (2023–2025), analizy powszechnego obowiązku obronnego i poboru w Europie, Waszyngton.
159. Ustawa z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz.U. 2024 poz. 1907).
160. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz.U. 2022 poz. 655, z późn. zm.).
161. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590, z późn. zm.).

B.12. Przemysł obronny, produkcja i łańcuchy dostaw

162. Center for Strategic and International Studies (2023–2026), analizy odbudowy bazy przemysłowo-obronnej oraz produkcji silników rakietowych, CSIS, Waszyngton.

163. Center for a New American Security (2023–2025), analizy skalowania produkcji obronnej i reformy zamówień, CNAS, Waszyngton.
164. Bruegel (2025), analizy zdolności obronnych Europy i finansowania przemysłu obronnego, Bruegel, Bruksela.
165. European Parliamentary Research Service (2024–2026), Scaling Up EU Arms Production, EPRS, Bruksela.
166. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1525 z 20 lipca 2023 r. w sprawie wspierania produkcji amunicji (ASAP), Dz.U. UE L 185/7.
167. Komisja Europejska (2024), European Defence Industrial Strategy (EDIS) oraz European Defence Industry Programme (EDIP), Bruksela.
168. Stockholm International Peace Research Institute (2025), SIPRI Top 100 Arms-Producing and Military Services Companies oraz Military Expenditure Database, SIPRI, Sztokholm.
169. Center for Security and Emerging Technology (2023–2025), analizy zależności łańcuchów dostaw półprzewodników i komponentów bezzałogowców, CSET, Waszyngton.
170. Royal United Services Institute (2023–2025), analizy łańcuchów dostaw dronów i zależności komponentowych, RUSI, Londyn.
171. Organizacja Traktatu Północnoatlantyckiego (2025), Defence Expenditure of NATO Countries, NATO, Bruksela.
172. Defense Innovation Unit / NATO DIANA (2022–2026), materiały o modelach szybkiego pozyskiwania technologii obronnych, Waszyngton–Bruksela.

B.13. Energetyka jako tor zasilający obrony

173. NATO Science and Technology Organization / Energy Security Centre of Excellence (2020–2025), analizy bezpieczeństwa energetycznego sił zbrojnych i infrastruktury, Wilno.
174. International Energy Agency (2024–2026), Electricity Security oraz analizy elastyczności i magazynowania energii, IEA, Paryż.
175. Agencja Rynku Energii / Polskie Sieci Elektroenergetyczne (2024–2026), materiały o bezpieczeństwie pracy krajowego systemu elektroenergetycznego, Warszawa.
176. European Network of Transmission System Operators for Electricity (2024–2026), analizy odporności systemu i procedur odbudowy zasilania, ENTSO-E, Bruksela.
177. Sandia National Laboratories (2020–2025), analizy mikrosieci i odporności energetycznej obiektów krytycznych, Albuquerque.
178. Węgrzyn, A. (2026), Doktryna Energetyczna TechnoRepubliki Polskiej: energia jako cybernetyczny system operacyjny państwa, TechnoSanacja, Warszawa.
179. Węgrzyn, A. (2026), Permitting projektów energetycznych oraz Sandbox regulacyjny dla strategicznych inicjatyw, TechnoSanacja, Warszawa.

B.14. Polska: strategia, geografia i instytucje bezpieczeństwa

180. Biuro Bezpieczeństwa Narodowego (2020), Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa.
181. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483, z późn. zm.).
182. Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. 1996 nr 106 poz. 492, z późn. zm.).
183. Najwyższa Izba Kontroli (2023–2026), kontrole dotyczące obronności, infrastruktury krytycznej i zarządzania kryzysowego, NIK, Warszawa.
184. Ministerstwo Obrony Narodowej (2024–2026), dokumenty programowe modernizacji technicznej Sił Zbrojnych RP, Warszawa.

- 185. Sieć Badawcza Łukasiewicz (2024–2026), analizy technologii podwójnego zastosowania, Warszawa.
- 186. Instytut Sobieskiego (2024–2026), analizy przemysłu obronnego i polityki bezpieczeństwa, Warszawa.

B.15. Kontrola demokratyczna, prawo i granice władzy obronnej

- 187. Geneva Centre for Security Sector Governance (2015–2025), publikacje o demokratycznej kontroli sił zbrojnych, DCAF, Genewa.
- 188. European Union Institute for Security Studies (2020–2026), analizy nadzoru nad sektorem bezpieczeństwa, EUISS, Paryż.
- 189. Komisja Wenecka (2020), Respect for Democracy, Human Rights and the Rule of Law during States of Emergency, CDL-AD(2020)014, Strasburg.
- 190. Konwencje genewskie z 12 sierpnia 1949 r. wraz z Protokołami dodatkowymi z 1977 r.
- 191. Huntington, S.P. (1957), The Soldier and the State: The Theory and Politics of Civil-Military Relations, Harvard University Press, Cambridge MA.
- 192. Janowitz, M. (1960), The Professional Soldier: A Social and Political Portrait, Free Press, Glencoe.
- 193. Feaver, P.D. (2003), Armed Servants: Agency, Oversight, and Civil-Military Relations, Harvard University Press, Cambridge MA.
- 194. Bovens, M. (2007), Analysing and Assessing Accountability: A Conceptual Framework, „European Law Journal” 13(4), s. 447–468.

B.16. Dokumenty programowe TechnoSanacji i TechnoRepubliki

- 195. Węgrzyn, A. (2026), Manifest TechnoSanacji, TechnoSanacja, Warszawa.
- 196. Węgrzyn, A. (2026), Narodowa Strategia Bezpieczeństwa TechnoRepubliki Polskiej, TechnoSanacja, Warszawa.
- 197. Węgrzyn, A. (2026), Konstytucja TechnoRepubliki Polskiej, TechnoSanacja, Warszawa.
- 198. Węgrzyn, A. (2026), Prezydent — zintegrowana egzekutywa, TechnoSanacja, Warszawa.
- 199. Węgrzyn, A. (2026), Controlling cybernetyczny państwa, TechnoSanacja, Warszawa.
- 200. Węgrzyn, A. (2026), System Informacyjny TechnoRepubliki Polskiej, TechnoSanacja, Warszawa.
- 201. Węgrzyn, A. (2026), Struktura Multi-Agentowa TechnoRepubliki Polskiej, TechnoSanacja, Warszawa.
- 202. Węgrzyn, A. (2026), Program odporności społecznej, gospodarczej i technologicznej państwa, TechnoSanacja, Warszawa.
- 203. Węgrzyn, A. (2026), Infrastruktura odporności państwa, TechnoSanacja, Warszawa.
- 204. Węgrzyn, A. (2026), Program 2G: Gen Z i Seniorzy budują Polskę zdolną do działania, TechnoSanacja, Warszawa.
- 205. Węgrzyn, A. (2026), Diagnoza Rzeczypospolitej Polskiej 2026: państwo w dryfie strategicznym, TechnoSanacja, Warszawa.
- 206. Węgrzyn, A. (2026), Przewodnik TechnoSanacji: idea, pojęcia, definicje, indeksy, TechnoSanacja, Warszawa.
- 207. Destylat (2026), Obrona Narodowa TechnoRepubliki Polskiej — synteza biblioteki wewnętrznej , korpus TechnoSanacja.
- 208. Destylat (2026), Narodowa Obrona TechnoRepubliki Polskiej i zarządzanie ryzykiem wojennym — synteza 611 pozycji korpusu obronnego, TechnoSanacja.
- 209. Destylat (2026), Odporność społeczna, gospodarcza i technologiczna TechnoRepubliki, TechnoSanacja.
- 210. Destylat (2026), Teoria relacji geopolitycznych oraz Strategia geopolityczna TechnoRepubliki Polskiej, TechnoSanacja.

Nota o źródłach

Pozycje klasyczne (klastry B.1–B.5, B.15) podano z pełnym adresem bibliograficznym. Pozycje analityczne instytucji badawczych (klastry B.6–B.14) pochodzą z korpusu źródłowego TechnoSanacji (236 oraz 611 pozycji) — i podano je na poziomie instytucji, tytułu serii lub raportu oraz roku wydania. Publikacje i akty prawne przywołano według stanu na sierpień 2026 r.

Polska, 29.08.2026. – Materiał udostępniony na licencji Creative Commons – Uznanie autorstwa

