

POLSKA AMBITNA

Jak wzmacniać państwo w niestabilnym świecie

KONGRES 590 POLSKA AMBITNA

PUBLIKACJA POKONGRESOWA

POLSKA AMBITNA

Jak wzmacniać państwo w niestabilnym świecie

POLSKA AMBITNA

Jak wzmacniać państwo w niestabilnym świecie

KONGRES SET. POLSKA AMBITNA

PUBLIKACJA POKONGRESOWA

POLSKA AMBITNA.
JAK WZMACNIAĆ PAŃSTWO W NIESTABILNYM ŚWIECIE

PUBLIKACJA POKONGRESOWA

Copyright by Fundacja SET – Security · Energy · Technology

Redakcja:
Fundacja SET - Security - Energy - Technology
www.set.org.pl

Raport wydawany w ramach realizowanego przez Fundację SET projektu:
KONGRES SET. POLSKA AMBITNA

ISBN 978-83-68653-18-2

Wydawca, projekt i produkcja: Capital sp. z o.o.
ul. Kwitnąca 5/6
01–926 Warszawa
tel. 533 496 436
www.capitalbook.pl, sklep@capitalbook.pl

Warszawa 2026

Spis treści

Wprowadzenie. Polska Ambitna *Zespół Fundacji SET* 9

„Żeglowanie jest koniecznością" *Zbigniew Bogucki* 12

Bezpieczeństwo i odporność *Bartosz Grodecki* 16

ROZDZIAŁ I. BEZPIECZEŃSTWO

Wielodomenowe zagrożenia w cyberprzestrzeni. Cyberprzestrzeń jako środowisko konfrontacji technologicznej, informacyjnej i psychologicznej *Kamil Basaj* 22

Strategia bezpieczeństwa Polski w warunkach narastającej niestabilności *Mariusz Błaszczak* 37

Systemy dronowe: strategiczne wyzwanie w budowie bezpieczeństwa Polski *gen. bryg. rez. Mirosław Bryś, Paweł Wiszniewski* 44

Między rynkiem, geopolityką a realną mocą produkcyjną przemysłu obronnego. Wpływ toczących się na świecie konfliktów zbrojnych na zmiany trendów zakupowych *Sebastian Chwałek* 53

Bezpieczeństwo finansowe państwa: między stabilnością makroekonomiczną a erozją bazy podatkowej *dr hab. Ireneusz Dąbrowski, prof. SGH* 65

Odporne państwo – strategiczne wyzwania dla bezpieczeństwa Polski *Zbigniew Hoffmann* 74

Automatyzacja produkcji amunicji z wykorzystaniem systemów opartych o sztuczną inteligencję *dr inż. Przemysław Kowalczuk* 80

Suwerenność gospodarcza – fundament bezpieczeństwa i rozwoju Polski *Jacek Sasin* 91

Bezpieczeństwo polskich portów morskich – od ochrony przed zagrożeniami hybrydowymi do zabezpieczenia strategicznych interesów państwa *Michał Śmigielski* 95

Suwerenność albo zależność. Jak zbudować polską gospodarkę bezpieczeństwa i system odstraszania? *Dariusz Wroński* 102

Cyberbezpieczeństwo jako warunek odporności państwa i akcelerator rozwoju gospodarczego *Tomasz Zdzikot* 108

ROZDZIAŁ II. ENERGIA

Energetyka jądrowa jako fundament bezpieczeństwa i reindustrializacji Polski *Wojciech Dąbrowski* 118

Polska hubem gazowym Europy. Gaz ziemny jako instrument niezależności energetycznej, stabilnej transformacji i regionalnego bezpieczeństwa *Paweł Majewski* 125

Energia jako dobro konstytucyjne *Michał Moskal* 138

Transformacja energetyczna, bezpieczeństwo energetyczne oraz rozwój projektów wiatrowych i gazowych *Maciej Olczak* 145

Inwestycje w infrastrukturę paliwową jako fundament odporności państwa na kryzysy geopolityczne *Paweł Stańczyk* 150

Brak koordynacji transformacji energetycznej i nieokreślony model docelowy polskiego systemu elektroenergetycznego *dr inż. Paweł Szczeszek* 158

Wysokie koszty energii i pogarszająca się konkurencyjność polskiej gospodarki w świetle najnowszych regulacji unijnych i działań państw członkowskich UE *Mateusz Wodejko* 167

Społeczna akceptacja projektów wydobywczych surowców krytycznych jako warunek bezpieczeństwa gospodarczego i transformacji energetycznej Europy *Kasjan Wyligała* 175

Biogaz jako dyspozycyjne źródło energii oraz biometan jako krajowy zasób gazowy *Artur Zawisza* 183

ROZDZIAŁ III. TECHNOLOGIE

Przyszłość krajowej domeny internetowej wobec wyzwań suwerenności technologicznej *prof. Katarzyna Chałubińska-Jentkiewicz* 198

Suwerenność technologiczna. Nowy wymiar polskiej racji stanu *Marietta Gieroń* 205

Czy regulacja AI może być przewagą konkurencyjną? Modele regulacji AI a pozycja Europy i Polski w globalnej rywalizacji technologicznej *dr Karolina Grenda* 226

Polska ambitna w dolinie cieni *Piotr Guział* 244

Cyberbezpieczeństwo ma narodowość. Dlaczego Polska potrzebuje własnego cyberpancerza *Jan Kostrzewa* 257

Czy Polskę stać na Narodowy Program budowy Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa? *ppłk rez. dr inż. Robert Kośla* 264

Dlaczego polski COP 2.0 zaczyna się w szkole, a nie na politechnice, i jak zbudować nasz ekosystem innowacji bez grantozy? *dr Daniel Milewski* 276

Od Centralnego Okręgu Przemysłowego do Cyfrowego Okręgu Przemysłowego – transformacja potencjału strategicznego państwa *Marcin Stachowski, Paweł Turowski* 284

Cyberpotęga czy cyfrowe peryferia? Strategia dla ambitnej Polski *Dariusz Stefaniuk* 311

Autorzy 327

Wprowadzenie. Polska Ambitna

Zespół Fundacji SET

Security-Energy-Technology

Współczesny świat wszedł w okres głębokiej strukturalnej niestabilności. Wojna za wschodnią granicą Polski, narastająca rywalizacja mocarstw, kryzysy energetyczne, presja migracyjna, zagrożenia hybrydowe, cyberataki, dezinformacja oraz gwałtowny rozwój technologii zmieniają podstawowe warunki funkcjonowania państw. Bezpieczeństwo militarne, stabilność finansowa, energetyka, przemysł, infrastruktura, cyfryzacja i suwerenność technologiczna tworzą dziś system naczyń połączonych. Siła państwa zależy od zdolności do skutecznego i zgodnego z narodowymi interesami działania we wszystkich tych obszarach jednocześnie.

Niniejsza publikacja pokonferencyjna powstała z przekonania, że Polska potrzebuje nowego myślenia strategicznego. Nie wystarczy reagować na kolejne kryzysy ani dostosowywać się do decyzji podejmowanych poza naszym krajem. "Polska Ambitna" musi posiadać własną diagnozę geopolityczną, własne instrumenty działania i własną wizję rozwoju. Musi być zdolna do obrony swoich granic, ochrony infrastruktury krytycznej, utrzymania stabilności finansów publicznych, zapewnienia konkurencyjnych i stabilnych cen energii, rozwoju nowoczesnego przemysłu oraz budowy unikalnych kompetencji technologicznych. Bez tych elementów suwerenność pozostanie pojęciem abstrakcyjnym, a rozwój będzie zależny od czynników zewnętrznych.

Autorzy tekstów zebranych w tym tomie pokazują, że bezpieczeństwo nie jest już wyłącznie domeną wojska. Obejmuje także zdolność państwa do finansowania własnych ambicji, utrzymania wiarygodnej waluty, ochrony bazy podatkowej, ograniczania szarej strefy oraz przeciwdziałania zjawiskom, które osłabiają

instytucjonalne fundamenty państwowości. Stabilność makroekonomiczna, przewidywalność regulacyjna i skuteczność fiskalna stają się warunkami realnej sprawczości strategicznej.

Szczególne miejsce w publikacji zajmuje energetyka. Stabilne, dostępne cenowo i odporne na szoki zewnętrzne źródła energii są dziś jednym z najważniejszych warunków bezpieczeństwa państwa i konkurencyjności gospodarki. Energetyka jądrowa, gaz ziemny, odnawialne źródła energii, biogaz, biometan, infrastruktura paliwowa oraz surowce krytyczne nie powinny być traktowane jako odrębne sektory. To zasadnicze elementy jednego systemu odporności państwa. Polska potrzebuje transformacji energetycznej prowadzonej w sposób racjonalny, skoordynowany i podporządkowany długoterminowemu interesowi narodowemu.

Kolejnym, równie istotnym wątkiem jest reindustrializacja. Doświadczenia pandemii, wojny na Ukrainie i kryzysów w globalnych łańcuchach dostaw pokazały, że państwa pozbawione własnych zdolności produkcyjnych stają się podatne na szantaż, zakłócenia dostaw i utratę konkurencyjności. Nowoczesny przemysł, w tym przemysł obronny, energetyczny, cyfrowy i podwójnego zastosowanie, jest nie tylko źródłem wzrostu gospodarczego, lecz także narzędziem bezpieczeństwa. Polska musi budować własne unikalne kompetencje, wzmacniać krajowy kapitał produkcyjny i tworzyć warunki dla rozwoju przedsiębiorstw zdolnych konkurować w sektorach strategicznych na rynkach międzynarodowych.

Osobny obszar stanowi bezpieczeństwo technologiczne. Sztuczna inteligencja, cyberbezpieczeństwo, infrastruktura danych, technologie kwantowe, systemy bezzałogowe, domeny internetowe i własne modele cyfrowe stają się dziś częścią architektury suwerenności państwa. Państwo, które nie kontroluje kluczowych technologii, danych i infrastruktury cyfrowej, ryzykuje trwałe przesunięcie na peryferie globalnej gospodarki. Dlatego w publikacji powraca postulat budowy polskich kompetencji technologicznych. Nie postulujemy izolacji, lecz świadomą współpracę, która ogranicza zależności i wzmacnia podmiotowość.

Wspólnym mianownikiem wszystkich tekstów jest przekonanie, że Polska stoi przed wyborem: może pozostać biernym odbiorcą cudzych rozwiązań, regulacji, technologii i decyzji strategicznych albo stać się państwem aktywnym, sprawczym i odpornym. Państwem, które inwestuje w bezpieczeństwo nie tylko w odpowiedzi na bieżące wyzwania, lecz w celu tworzenia podstaw wieloletniego rozwoju. Państwem, które rozumie, że suwerenność gospodarcza, energetyczna, finansowa, militarna i technologiczna są różnymi wymiarami tej samej racji stanu.

Książka nie jest więc wyłącznie zbiorem diagnoz, lecz próbą sformułowania szerszej odpowiedzi na pytanie, jak wzmacniać państwo w świecie rosnącej niepewności. Odpowiedź wymaga odwagi decyzyjnej, długiego horyzontu myślenia, koordynacji instytucji publicznych, współpracy państwa z biznesem i nauką oraz konsekwencji wykraczającej poza cykl wyborczy. Takie podejście pozwoli Polsce wykorzystać własny potencjał i zbudować pozycję adekwatną do zasobów i aspiracji.

"Polska Ambitna" to nowoczesne państwo zdolne do samodzielnego działania, ale otwarte na strategiczne sojusze. Państwo zakorzenione w NATO i wspólnocie Zachodu, ale świadome własnych żywotnych interesów. Nowoczesne technologicznie, silne gospodarczo, stabilne finansowo, odporne energetycznie i gotowe do obrony swoich obywateli. Od tego, czy uda się taki model państwa konsekwentnie budować, zależy nie tylko tempo rozwoju Polski, lecz także bezpieczeństwo przyszłych pokoleń.

Oddając w Państwa ręce naszą kolejną publikację, wyrażamy nadzieję, iż stanie się ona inspiracją nie tylko do dalszej debaty, ale również do podejmowania stosownych decyzji strategicznych.

„Żeglowanie jest koniecznością”

Zbigniew Bogucki

Szef Kancelarii Prezydenta Rzeczypospolitej Polskiej

To piękne powiedzenie żeglarskie dobrze oddaje istotę myślenia długofalowego. Jeżeli mówimy o strategii, nie możemy patrzeć wyłącznie na to, co jest tu i teraz. Musimy patrzeć dalej: na to, co będzie za rok, za pięć lat, za piętnaście, dwadzieścia lat i w kolejnych dekadach.

Perspektywa tej dyskusji, w sposób szczególny koncentruje się na roku 2035. To nie jest jeszcze horyzont bardzo odległy. To raczej perspektywa średniookresowa, o której musimy myśleć i o której musimy rozmawiać. Jest ona szczególnie związana z kwestią bezpieczeństwa militarnego. Wiąże się to zarówno z informacjami, o których mogę mówić, jak i z tymi, o których mówić nie mogę.

Jeżeli dziś rozmawiamy o bezpieczeństwie, to zwłaszcza w kontekście tego, co od kilku lat dzieje się na Ukrainie, myślimy przede wszystkim o bezpieczeństwie militarnym: o polskiej armii, polskich służbach mundurowych i całym systemie obronnym państwa. I rzeczywiście jest to fundament, filar polskiego bezpieczeństwa.

Obok bezpieczeństwa militarnego niezwykle ważne jest to, co od samego początku swojej prezydentury, od 6 sierpnia 2025 r., robi Prezydent Karol Nawrocki, czyli budowanie sojuszy bezpieczeństwa. Przede wszystkim ze Stanami Zjednoczonymi, oczywiście bez wykluczania innych partnerów. Partnerzy europejscy, partnerzy z Sojuszu Północnoatlantyckiego są ważni i są blisko nas. Jednak każdy, kto ma choćby podstawowe rozeznanie w kwestiach bezpieczeństwa wojskowego, doskonale wie, że ponad 60 procent potencjału Sojuszu Północnoatlantyckiego stanowi armia Stanów Zjednoczonych. To ich technologie, ich żołnierze, ich sprawność, mobilność i decyzyjność mają fundamentalne znaczenie.

Dlatego tak istotna była kolejna wizyta Pana Prezydenta w Stanach Zjednoczonych i cała strategia budowania sojuszu opartego nie tylko na płaszczyźnie administracyjnej, wojskowej i państwowej, ale także na relacjach osobistych. Wielu tego nie rozumie, o czym świadczą bieżące komentarze. Tymczasem jeżeli istnieją relacje osobiste między liderami, w tym przypadku między Prezydentem Rzeczypospolitej Polskiej Karolem Nawrockim a Prezydentem Stanów Zjednoczonych Donaldem Trumpem, to w naturalny sposób łatwiej rozmawiać o sprawach najtrudniejszych. Jeżeli takich relacji nie ma, trudno rozmawia się nawet o rzeczach prostych.

Prezydent Nawrocki jest liderem. Prezydent rozumie, czym jest strategia, czym jest myślenie długofalowe i czym jest myślenie wykraczające poza jedną kadencję: prezydencką, sejmową czy senacką. Do kwestii bezpieczeństwa nie możemy podchodzić w sposób doraźny. Musimy patrzeć szerzej, z odpowiednim namysłem i z właściwą perspektywą.

Nasze urzędy i funkcje przemijają, a Polska ma trwać. Polska jest czymś więcej niż nawet najwyższy urząd w państwie i najwyższe godności. Polska to sztafeta pokoleń, która zaczęła się wiele wieków temu. Miała swoje piękne i wspaniałe karty, ale miała także losy tragiczne.

To powinno być dla nas wielką nauką. Nasze urzędy się kończą, kadencje parlamentu przemijają, zmieniają się prezydenci i premierzy.

Wszystko płynie. A my mamy dopłynąć, wracając do marynistycznych nawiązań, do portu, który nazywa się: bezpieczna, ambitna Polska. Każdego dnia, każdego miesiąca, każdego roku i każdej dekady powinniśmy dopływać właśnie do tego portu. Bez ambicji trudno wyobrazić sobie jakiekolwiek strategiczne myślenie. Jeżeli ktoś jest pozbawiony ambicji, nie ma nawet zdolności myślenia o strategii. Nie ma też narzędzi do tego, aby organizować i prowadzić tego rodzaju rozmowy.

Do tej pory koncentrowałem się przede wszystkim na bezpieczeństwie militarnym, ale musimy pamiętać również o bezpieczeństwie zdrowotnym i żywnościowym.

Ktoś mógłby zapytać: gdzie pole polskiego rolnika, a gdzie dywizje polskiej armii? Tymczasem to wszystko jest systemem naczyń połączonych. Musi to rozumieć i rozumie to Prezydent Rzeczypospolitej. Dobrze byłoby, abyśmy my wszyscy jako ludzie zaangażowani w sprawy publiczne, sprawujący różnego rodzaju urzędy, ale także jako eksperci zajmujący się poszczególnymi branżami i dziedzinami bezpieczeństwa – również to rozumieli.

Musimy potrafić otwierać się na różne obszary bezpieczeństwa. One się przenikają i powinny się uzupełniać. Jeżeli myślimy strategicznie o bezpieczeństwie

energetycznym, nie możemy zapominać o rolnictwie. Jeżeli myślimy o bezpieczeństwie militarnym, nie możemy zapominać o kwestiach energetycznych. To wszystko tworzy jeden system naczyń połączonych.

Myślę, że takiego podejścia bardzo brakuje dziś obozowi władzy, który dzierży stery rządu w Polsce. Brakuje myślenia holistycznego, wykraczającego nie tylko poza bieżący czas, ale także poza wąskie granice jednego resortu, jednej polityki czy interesu jednej partii politycznej. Jeżeli mówimy o bezpieczeństwie, powinniśmy wychodzić poza ramy partyjne, poza ramy czasu, w którym aktualnie jesteśmy, i poza skondensowane myślenie resortowe, które – jak wiemy – wiele spraw utrudnia.

Zapewniam, że Prezydent Rzeczypospolitej zrobi wszystko, aby sprawy związane z polskim bezpieczeństwem i naszymi sojuszami były traktowane jako rzecz niepodważalna. Pan Prezydent nie będzie przejmował się różnego rodzaju trudnościami czy przeszkodami stawianymi niestety także tutaj, w Polsce. Interes Rzeczypospolitej jest bowiem czymś więcej. Interes i trwałość Rzeczypospolitej są ważniejsze. Prezydent, jako gwarant ciągłości władzy państwowej, ma w tym zakresie szczególną odpowiedzialność. Jestem przekonany, że Pan Prezydent Karol Nawrocki ma pełną świadomość tej wielkiej odpowiedzialności.

Przy Prezydencie i w Kancelarii Prezydenta funkcjonują różnego rodzaju Rady zajmujące się poszczególnymi dziedzinami życia społecznego, państwowego i publicznego. Każda twórcza wymiana myśli jest jednak potrzebna. Także po to, aby doradcy Pana Prezydenta mogli podzielić się swoją refleksją i skonfrontować ją z opiniami tych, którzy nie są obecni w Pałacu Prezydenckim, ale mają wiedzę, doświadczenie i kompetencje. Wszystko po to, aby wypracować jak najlepsze rozwiązania.

Żeglujmy więc. Żeglujmy ku strategii, która pokazuje nam coś więcej niż tylko najbliższy horyzont. Chodzi o to, abyśmy potrafili spojrzeć dalej niż tylko na to, co jest bezpośrednio przed nami.

Na koniec jeszcze jedna refleksja. Aby patrzeć dalej, musimy wiedzieć, skąd przychodzimy. Musimy znać naszą tradycję, naszą kulturę, nasze doświadczenia historyczne i wartości, którymi żyły pokolenia Polaków. To one zapewniły nam możliwość życia w bezpiecznym, wolnym i suwerennym kraju.

Tylko strategia odwołująca się do tych doświadczeń i do naszej specyfiki narodowej, a szerzej także do specyfiki cywilizacji Zachodu, może być strategią pełną. Cywilizacja Zachodu jest dziś gwarantem świata bezpiecznego, świata sprawiedliwego, a powiedziałbym także: świata normalnego. Do budowania strategii potrzebny jest więc także powrót do refleksji nad tym, skąd przychodzimy i jaka jest nasza historia.

Jeżeli mój głos choćby w minimalnym stopniu stanie się cegiełką do dalszych przemyśleń i refleksji, przynajmniej dla części z Państwa, to uznam, że moje dzisiejsze wystąpienie oraz czas spędzony z Państwem były czasem dobrze wykorzystanym.

Dziękuję bardzo.

Bezpieczeństwo i odporność

Bartosz Grodecki

Bartosz Grodecki, Szef Biura Bezpieczeństwa Narodowego

Szanowni Państwo,

bardzo dziękuję za zaproszenie na Kongres SET – Polska Ambitna.

Sama tematyka tego spotkania dobrze pokazuje, jak bardzo zmieniło się współczesne myślenie o bezpieczeństwie państwa. Jeszcze kilkanaście lat temu bezpieczeństwo, energetyka, gospodarka czy technologie były traktowane jako odrębne obszary polityki publicznej. Dziś coraz wyraźniej widzimy, że tworzą one jeden wspólny system strategiczny.

Żyjemy w epoce turbulencji strategicznych. Wojna wróciła do Europy, rywalizacja mocarstw ponownie stała się głównym mechanizmem porządku międzynarodowego, a presja polityczna, gospodarcza i technologiczna coraz częściej zastępuje klasyczny konflikt zbrojny.

Rosyjska agresja przeciwko Ukrainie pokazała, że bezpieczeństwo nie może być już rozumiane wyłącznie w kategoriach militarnych. Współczesna konfrontacja toczy się równocześnie w energetyce, gospodarce, cyberprzestrzeni, logistyce, technologii i przestrzeni informacyjnej. Państwa konkurują o odporność społeczeństw, kontrolę nad technologiami i zdolność do funkcjonowania pod długotrwałą presją.

Dlatego bezpieczeństwo musi być traktowane jako zdolność całego państwa do działania w warunkach kryzysu i niepewności. Nie wystarczy nowoczesna armia, jeśli państwo nie potrafi utrzymać produkcji, zabezpieczyć infrastruktury, chronić systemu finansowego i zapewnić ciągłości funkcjonowania administracji.

W tym kontekście odporność należy rozumieć jako zdolność państwa, społeczeństwa i gospodarki do zapobiegania zagrożeniom, absorbowania ich skutków, utrzymania kluczowych funkcji oraz szybkiej odbudowy po kryzysie. Nie jest to wyłącznie

zdolność do przetrwania wstrząsu, lecz zdolność do zachowania sprawczości, adaptacji i dalszego rozwoju pomimo występujących zagrożeń.

Wojna na Ukrainie pokazała, że o zdolności państwa do prowadzenia długotrwałej obrony decydują nie tylko siły zbrojne, lecz również przemysł, energetyka, logistyka, infrastruktura transportowa oraz zdolność utrzymania funkcjonowania administracji publicznej. Współczesna wojna stała się testem odporności całego państwa, a nie wyłącznie jego armii. O odporności państwa decyduje więc nie tylko potencjał militarny, ale także siła gospodarki, sprawność instytucji oraz zdolność społeczeństwa do funkcjonowania pod presją.

To oznacza konieczność odejścia od myślenia, w którym bezpieczeństwo i rozwój są odrębnymi obszarami polityki państwa. W rzeczywistości są one tym samym procesem strategicznym. Silna gospodarka wzmacnia bezpieczeństwo, a bezpieczeństwo jest warunkiem trwałego rozwoju. Państwo, które nie posiada własnych zdolności przemysłowych, technologicznych i energetycznych, będzie stopniowo tracić swoją podmiotowość.

Szczególnego znaczenia nabiera dziś potencjał produkcyjny i technologiczny państwa. Wchodzimy w epokę geopolityki przemysłowej, w której o pozycji państw decydować będzie zdolność do produkcji uzbrojenia, kontroli technologii, utrzymywania łańcuchów dostaw i szybkiego zwiększania potencjału w czasie kryzysu.

Jeżeli w XX wieku o sile państw decydowały przede wszystkim stal, energia i zdolności przemysłowe, to w XXI wieku do tych czynników dołączyły dane, sztuczna inteligencja, zdolności obliczeniowe, cyberbezpieczeństwo oraz technologie podwójnego zastosowania. Państwa, które utracą zdolność do tworzenia i kontrolowania tych technologii, będą stopniowo traciły również zdolność do samodzielnego kształtowania swojej polityki bezpieczeństwa.

Coraz częściej przewaga strategiczna wynika nie z pojedynczych przełomowych technologii, lecz ze zdolności do integrowania danych, sztucznej inteligencji, technologii cyfrowych i potencjału przemysłowego w jeden spójny ekosystem bezpieczeństwa i rozwoju.

Dlatego inwestycje w przemysł obronny, energetykę, logistykę, technologie podwójnego zastosowania czy sztuczną inteligencję nie mogą być traktowane wyłącznie jako koszty. Są inwestycją w strategiczną trwałość państwa.

To szczególnie ważne właśnie w środowisku takim jak dzisiejszy Kongres, gdzie spotykają się przedstawiciele administracji, biznesu, nauki i sektora technologicznego. Współczesnego bezpieczeństwa nie da się już budować wyłącznie decyzją

administracyjną. Państwo musi nauczyć się działać razem z przemysłem, sektorem energetycznym, operatorami infrastruktury krytycznej, środowiskiem naukowym i firmami technologicznymi.

Polska musi również myśleć o bezpieczeństwie w wymiarze regionalnym. Polska dysponuje dziś wyjątkową szansą połączenia potencjału gospodarczego, położenia geograficznego oraz rosnącej roli politycznej w Europie Środkowej w jeden spójny projekt wzmacniania bezpieczeństwa i rozwoju regionu.

Nasze położenie geograficzne sprawia, że znajdujemy się w centrum jednego najważniejszych obszarów strategicznych Europy. Oś Północ-Południe, łącząca region Morza Bałtyckiego z Morzem Czarnym, staje się jednym z najważniejszych korytarzy strategicznych Europy. To właśnie tutaj koncentrują się inwestycje infrastrukturalne, energetyczne, logistyczne i wojskowe, które będą wpływać na bezpieczeństwo całego regionu.

Nie oznacza to osłabienia znaczenia NATO czy relacji transatlantyckich. Wręcz przeciwnie. NATO pozostaje fundamentem bezpieczeństwa Polski, a strategiczne partnerstwo ze Stanami Zjednoczonymi ma kluczowe znaczenie dla odstraszania Rosji. Jednocześnie Unia Europejska pozostaje istotnym filarem bezpieczeństwa i odporności państw europejskich, szczególnie w obszarze gospodarki, infrastruktury, energetyki, przemysłu i technologii. W interesie Polski leży wzmacnianie europejskiego potencjału w sposób komplementarny wobec NATO i więzi transatlantyckich, a nie konkurencyjny wobec nich.

Musimy również przyjąć, że presja ze strony Rosji będzie miała charakter trwały. Obejmuje ona działania militarne, cyberataki, sabotaż, operacje dezinformacyjne, instrumentalizację migracji oraz próby destabilizacji społecznej. Granica między pokojem a konfliktem staje się coraz mniej wyraźna. Dlatego odporność społeczna, sprawność instytucji państwowych i zdolność szybkiego reagowania mają znaczenie strategiczne.

W tym świecie szczególnej wartości nabiera wspólnota polityczna. Państwo odporne to państwo, którego obywatele rozumieją zagrożenia, ufają instytucjom i są gotowi współuczestniczyć w wysiłku na rzecz bezpieczeństwa. Bezpieczeństwo narodowe nie może być zadaniem wyłącznie administracji czy sił zbrojnych. Musi stać się wspólnym projektem państwa i społeczeństwa.

Warunkiem powodzenia takiej polityki jest jednak myślenie wykraczające poza rytm bieżącej polityki. Budowa odporności państwa nie odbywa się w perspektywie jednej kadencji. Budowa odporności państwa nie odbywa się w perspektywie jednej kadencji. Wymaga ciągłości strategicznej, stabilnych priorytetów i zdolności

do prowadzenia wieloletnich inwestycji w bezpieczeństwo, przemysł, energetykę, edukację i technologie.

Szanowni Państwo,

wchodzimy w epokę, w której bezpieczeństwo nie będzie mierzone wyłącznie wielkością armii, lecz zdolnością państwa do utrzymania swojej sprawczości w warunkach długotrwałej presji.

O sile państw będą decydowały nie pojedyncze systemy uzbrojenia, ale zdolność integrowania potencjału militarnego, gospodarczego, technologicznego i społecznego w jeden spójny system odporności.

Dlatego najważniejszym zadaniem Polski nie jest dziś wyłącznie zwiększanie wydatków na bezpieczeństwo czy rozwijanie poszczególnych sektorów gospodarki. Jest nim budowa państwa zdolnego do integrowania potencjału militarnego, gospodarczego, technologicznego i społecznego w jeden spójny system odporności.

Państwa, które będą potrafiły to zrobić, nie tylko przetrwają okres globalnej niestabilności, ale również wykorzystają go do wzmocnienia swojej pozycji międzynarodowej.

To właśnie jest istota współczesnego bezpieczeństwa i odporności.

Dziękuję za uwagę.

ROZDZIAŁ I.
BEZPIECZEŃSTWO

Wielodomenowe zagrożenia w cyberprzestrzeni Cyberprzestrzeń jako środowisko konfrontacji technologicznej, informacyjnej i psychologicznej

Kamil Basaj

Abstrakt

Współczesna cyberprzestrzeń nie może być analizowana wyłącznie jako techniczna domena funkcjonowania systemów teleinformatycznych. Jest ona równocześnie środowiskiem komunikacji społecznej, akumulacji danych, profilowania psychologicznego, dystrybucji treści, kształtowania emocji oraz oddziaływania na procesy decyzyjne. W tym sensie cyberprzestrzeń staje się nie tylko domeną operacyjną, lecz także przestrzenią poznawczą, w której przeciwnik może modelować percepcję sytuacji, testować podatności społeczne i instytucjonalne oraz integrować działania techniczne z operacjami wpływu. Artykuł rozwija zarys publikacji dotyczący wielodomenowych zagrożeń w cyberprzestrzeni, ze szczególnym uwzględnieniem rosyjskiego modelu działań aktywnych, operacji informacyjno-psychologicznych oraz powiązań między cyberatakami, sabotażem, dezinformacją, presją psychologiczną i zarządzaniem percepcją odbiorców.

Słowa kluczowe: cyberprzestrzeń, dezinformacja, FIMI, operacje wpływu, środki aktywne, Rosja, działania psychologiczne, bezpieczeństwo informacyjne, odporność państwa, aktywna obrona.

1. Wprowadzenie: od domeny technicznej do środowiska poznawczego

Cyberprzestrzeń przez wiele lat opisywano przede wszystkim jako obszar funkcjonowania sieci, infrastruktury teleinformatycznej, systemów przetwarzania danych oraz usług cyfrowych. Takie ujęcie pozostaje kluczowe i potrzebne, ale jest już niewystarczające. Współczesne konflikty pokazują, że cyberprzestrzeń nie jest wyłącznie polem ataku na serwery, sieci, systemy przemysłowe, łańcuchy dostaw czy skrzynki pocztowe. Jest środowiskiem, w którym dane, emocje, narracje, zachowania społeczne, algorytmy i decyzje instytucjonalne wzajemnie się przenikają.

NATO formalnie uznało cyberprzestrzeń za domenę operacyjną podczas szczytu w Warszawie w 2016 roku, wskazując, że Sojusz musi bronić się w niej tak skutecznie, jak w domenach lądowej, powietrznej i morskiej. To rozstrzygnięcie miało znaczenie doktrynalne, lecz obecna praktyka operacyjna wymaga dalszego rozszerzenia tej perspektywy. Cyberprzestrzeń jest bowiem domeną technologiczną, ale jednocześnie środowiskiem informacyjnym i poznawczym. To w niej przeciwnik może gromadzić dane o odbiorcach, identyfikować ich wrażliwości, sprawdzać reakcje na bodźce, dostosowywać przekazy do mikrogrup i uruchamiać sekwencje presji psychologicznej.

W tym sensie zagrożenia w cyberprzestrzeni mają charakter wielodomenowy. Cyberatak może być jedynie pierwszym elementem szerszej operacji. Kradzież danych może służyć kompromitacji, szantażowi, selektywnemu wyciekowi, delegitymizacji instytucji albo tworzeniu materiału dla późniejszej kampanii propagandowej. Atak DDoS może mieć znaczenie nie tylko techniczne, lecz także psychologiczne, jeżeli zostanie zsynchronizowany z narracją o niewydolności państwa. Sabotaż infrastruktury może być połączony z aktywnością kont w mediach społecznościowych, komentarzami, przeciekami, fałszywymi interpretacjami i pozornie spontaniczną paniką informacyjną.

Z tej perspektywy nie można rozdzielać bezpieczeństwa cyberprzestrzeni od bezpieczeństwa informacyjnego, kontrwywiadu, ochrony infrastruktury krytycznej, odporności społecznej oraz komunikacji strategicznej państwa. Przeciwnik nie działa w podziale na resortowe lub instytucjonalne silosy. Łączy środki techniczne, osobowe, propagandowe, psychologiczne, dywersyjne i dyplomatyczne w jeden proces oddziaływania. Dlatego odpowiedź państwa również musi mieć charakter zintegrowany.

2. Dezinformacja jako proces kontroli percepcji, a nie wyłącznie fałszywa informacja

Jednym z podstawowych niedoborów analitycznych jest redukowanie dezinformacji do prostego rozróżnienia między informacją prawdziwą i fałszywą. Takie podejście bywa użyteczne w edukacji medialnej, fact-checkingu lub szybkiej weryfikacji treści, ale nie wystarcza do analizy operacji prowadzonych przez aktorów państwowych. W praktyce przeciwnik może wykorzystywać informacje prawdziwe, częściowo prawdziwe, wyrwane z kontekstu, zmanipulowane, opóźnione, selektywnie ujawnione albo zestawione w taki sposób, aby wywołać określony efekt psychologiczny.

Z perspektywy operacyjnej dezinformacja jest procesem kształtowania poglądu odbiorcy w warunkach kontrolowanych przez adwersarza. Jej celem nie jest wyłącznie przekazanie fałszu, lecz doprowadzenie odbiorcy do interpretacji, emocji lub decyzji zgodnej z intencją przeciwnika. Kluczowe jest zatem nie tylko pytanie, czy dana treść jest prawdziwa, lecz także: kto ją wprowadza, w jakim momencie, przez jakie kanały, do jakich grup, w jakiej sekwencji, z jakimi równoległymi bodźcami i z jakim oczekiwanym skutkiem.

Tak rozumiana dezinformacja ma charakter procesowy. Nie jest pojedynczym komunikatem, lecz ciągiem działań. Może zaczynać się od cyberataku, wycieku dokumentów, prowokacji fizycznej, fałszywego alarmu, incydentu granicznego, podpalenia, publikacji w kontrolowanym medium albo pozornie oddolnego komentarza w mediach społecznościowych. Dopiero suma tych zdarzeń tworzy obraz operacji.

Właśnie dlatego Zachód coraz częściej posługuje się pojęciem FIMI, czyli foreign information manipulation and interference – zagranicznej manipulacji informacją i ingerencji. Pojęcie to jest szersze niż klasyczna dezinformacja, ponieważ obejmuje także koordynację zachowań, manipulowanie infrastrukturą informacyjną, podszywanie się, wykorzystywanie luk platformowych, wzmacnianie określonych treści oraz wpływanie na debatę publiczną poprzez środki jawne i ukryte.

Z tej perspektywy najważniejszym przedmiotem analizy nie jest pojedyncza informacja, lecz architektura oddziaływania. Analityk powinien badać, czy określone zdarzenia są elementem większej sekwencji. Dotyczy to zarówno cyberataków, jak i gróźb, podpaleń, aktów dywersji, przecieków, kampanii narracyjnych, aktywności botów, działań kont pozornie niezależnych, reakcji mediów propagandowych oraz presji kierowanej wobec konkretnych osób.

3. Wielodomenowość rosyjskiego modelu oddziaływania

Rosyjskie działania wpływu mają głębokie zakorzenienie w tradycji sowieckich środków aktywnych. Ich istotą było nie tylko rozpowszechnianie propagandy, lecz wpływanie na decyzje przeciwnika, rozbijanie zaufania społecznego, kompromitowanie liderów, wzmacnianie konfliktów wewnętrznych i wytwarzanie fałszywego obrazu rzeczywistości. Współczesna Rosja nie zrezygnowała z tych metod. Przeciwnie, dostosowała je do środowiska cyfrowego, algorytmicznego i sieciowego.

Nowością nie jest więc sama logika oddziaływania, lecz skala, tempo, precyzja i automatyzacja. Cyberprzestrzeń umożliwia szybkie testowanie przekazów, profilowanie grup odbiorców, tworzenie wielu wariantów tej samej narracji, dystrybucję treści w różnych językach oraz równoczesne prowadzenie operacji jawnych, półjawnych i ukrytych. W praktyce rosyjski aparat wpływu może integrować działania oficjalnych mediów państwowych, portali proxy, kont pozornie niezależnych, grup w komunikatorach, kanałów wideo, influencerów, środowisk radykalnych, sieci blogów, komentarzy i „przecieków".

Wojna Rosji przeciwko Ukrainie dobitnie pokazuje, że cyberoperacje nie funkcjonują w izolacji. Są powiązane z działaniami kinetycznymi, wojskowymi, dyplomatycznymi, gospodarczymi i psychologicznymi. W praktyce oznacza to, że atak na system informatyczny może zostać wykorzystany jako narzędzie operacji psychologicznej. Przykładowo kompromitacja skrzynki pocztowej osoby publicznej nie musi służyć wyłącznie pozyskaniu informacji. Może być początkiem kampanii, która obejmuje selektywne ujawnianie korespondencji, mieszanie dokumentów prawdziwych z fałszywymi, publikację materiałów w kanałach proxy, inspirowanie pytań medialnych, budowanie presji na instytucję, wzmacnianie teorii spiskowych oraz rozbijanie zaufania do procesu decyzyjnego.

Podobnie akt sabotażu fizycznego może być komponentem operacji wpływu. Samo zdarzenie wywołuje lęk, ale dopiero jego interpretacja w środowisku informacyjnym nadaje mu znaczenie strategiczne. Przeciwnik może sugerować, że państwo jest bezradne, infrastruktura niechroniona, sojusze nieskuteczne, elity ukrywają prawdę, a obywatele powinni utracić zaufanie do instytucji. W takiej sytuacji celem nie jest wyłącznie fizyczna szkoda, lecz psychologiczny efekt powtarzalności, niepewności i paraliżu. Doskonałym przykładem tego typu modeli działania są operacje zastraszania (tzw paraliżowania). Jednym z kluczowych modeli psychologicznych wykorzystywanych przez Rosję w operacjach wielodomenowych jest presja przez

zastraszanie. Nie polega ona wyłącznie na emisji agresywnych komunikatów propagandowych, lecz na łączeniu działań informacyjnych, cyberataków, demonstracji siły, prowokacji, sabotażu, gróźb oraz aktywności w domenie fizycznej w jeden mechanizm oddziaływania na percepcję odbiorców. Celem takiej operacji jest wywołanie lęku, niepewności, poczucia bezradności oraz przekonania, że dalszy opór wobec Rosji lub wspieranie Ukrainy wiąże się z nadmiernym kosztem.

Charakterystyczną cechą tego modelu jest działanie rozproszone. Pozornie niezależne zdarzenia – ruchy wojsk, groźby nuklearne, cyberataki, incydenty infrastrukturalne, kampanie propagandowe czy wypowiedzi rosyjskich decydentów – wzajemnie się wzmacniają i tworzą wrażenie narastającego, nieuchronnego zagrożenia. Rosja wykorzystuje również odwrócenie logiki zdarzeń, przedstawiając własną agresję jako reakcję obronną, a działania NATO, Ukrainy lub Zachodu jako rzekomą prowokację. W ten sposób budowany jest obraz Rosji jako „oblężonej twierdzy", co służy zarówno legitymizacji działań zewnętrznych, jak i dyscyplinowaniu społeczeństwa wewnątrz państwa.

Przykładem takiego podejścia są operacje informacyjno-psychologiczne oparte na groźbie katastrofy nuklearnej, szantażu energetycznym czy eksponowaniu brutalności działań wojennych. Ich celem nie jest wyłącznie przekazanie określonej narracji, lecz wywołanie emocjonalnej reakcji: strachu o bezpieczeństwo rodziny, stabilność ekonomiczną, dostęp do energii lub ryzyko eskalacji wojny. W ten sposób lęk ma zostać przekształcony w presję społeczną i polityczną, prowadzącą do ograniczenia gotowości Zachodu do wspierania Ukrainy oraz do osłabienia odporności społeczeństw demokratycznych.

Zjawisko to można określić jako element szerszej „metody paraliżowania". Jej istotą jest doprowadzenie odbiorcy do stanu obniżonej sprawczości, przeciążenia informacyjnego i przekonania, że każda decyzja wiąże się z wysokim ryzykiem. Dlatego analiza rosyjskich operacji wpływu nie może ograniczać się do prostowania fałszywych informacji. Musi obejmować ocenę całego układu działań: narracji, cyberataków, aktywności fizycznej, prowokacji, presji emocjonalnej i oczekiwanego efektu psychologicznego.

4. Cyberatak jako element operacji psychologicznej

W klasycznym podejściu cyberatak analizowany jest m. in. przez pryzmat podatności, wektora wejścia, eskalacji uprawnień, utrzymania dostępu, eksfiltracji danych

i skutków technicznych. To konieczne, ale niepełne. W operacjach wielodomenowych równie ważne jest pytanie, jak przeciwnik zamierza wykorzystać techniczny efekt ataku do osiągnięcia skutku psychologicznego lub politycznego.

Dobrym przykładem są ataki na skrzynki pocztowe. Z technicznego punktu widzenia mogą obejmować przejęcie danych logowania, wykorzystanie słabych procedur uwierzytelniania, phishing, socjotechnikę lub dostęp uzyskany przez osobę trzecią. Z perspektywy operacji wpływu istotniejsza jest jednak sekwencja po kompromitacji. Przeciwnik może dokonać selekcji materiałów, wybrać fragmenty najbardziej podatne na manipulację, zbudować wokół nich narrację, opublikować je w kanałach o kontrolowanej wiarygodności, a następnie uruchomić pozornie spontaniczną dyskusję społeczną.

Taki model może przebiegać etapowo. Najpierw następuje rozpoznanie celu: jego roli, relacji, zwyczajów komunikacyjnych, podatności psychologicznych i znaczenia dla danej instytucji. Następnie przeciwnik pozyskuje dostęp do danych albo buduje przekonanie, że taki dostęp posiada. W kolejnym kroku dokonuje selekcji materiału. Nie musi publikować wszystkiego. Często skuteczniejsze jest ujawnienie małego fragmentu, który można interpretować w wielu kierunkach i wokół którego można wytworzyć napięcie.

Następnie pojawia się warstwa narracyjna. Materiał techniczny staje się „dowodem" na wcześniej przygotowaną tezę. Teza może dotyczyć rzekomej korupcji, zdrady, niekompetencji, zależności od obcego państwa, ukrywania prawdy albo konfliktu wewnątrz instytucji. W tym momencie cyberatak przestaje być incydentem technicznym. Staje się narzędziem presji poznawczej.

Ostatnią fazą jest dystrybucja i wzmacnianie. Treści trafiają do mediów społecznościowych, kanałów komentatorskich, portali alternatywnych, środowisk radykalnych, kont automatycznych lub półautomatycznych, a także do odbiorców, którzy z powodów emocjonalnych lub politycznych są gotowi nadać im dalszy zasięg. W takiej sekwencji cyberatak jest tylko początkiem. Właściwa operacja odbywa się w przestrzeni interpretacji.

Dlatego analiza incydentu cybernetycznego powinna obejmować nie tylko analitykę techniczną, lecz także analizę narracyjną, analizę dystrybucji, badanie zachowań sieciowych, ocenę synchronizacji czasowej, identyfikację wzmacniaczy oraz rozpoznanie oczekiwanego efektu psychologicznego. Bez tego państwo może prawidłowo opisać wektor techniczny, ale nie zrozumieć celu operacji.

5. Model etapowy dystrybucji i oddziaływania w polskojęzycznej infosferze

Opisany w zarysie model oddziaływania można przedstawić jako piramidę dystrybucji i przekształcania treści. Jego istotą jest stopniowe przeprowadzanie materiału od źródła kontrolowanego przez przeciwnika do środowisk, w których treść zaczyna funkcjonować jako pozornie organiczna opinia społeczna.

Pierwszy etap polega na wprowadzeniu patogenu informacyjnego do polskojęzycznej infosfery. Źródłem może być portal, kanał lub medium będące częścią rosyjskiego aparatu propagandowego albo jego szarej strefy. Na tym poziomie zasięg nie musi być duży. Funkcją źródła pierwotnego jest implementacja przekazu i stworzenie punktu odniesienia dla dalszej multiplikacji.

Drugi etap obejmuje powielanie treści na innych stronach internetowych. Materiał może być nieznacznie zmieniany: modyfikowany jest tytuł, skracany lead, usuwane są najbardziej widoczne ślady źródła albo dodawane elementy lokalnego kontekstu. Celem nie jest jeszcze pełna wiarygodność, lecz rozproszenie śladów i zwiększenie liczby punktów dostępu do przekazu.

Trzeci etap to przeniesienie treści do blogosfery i przestrzeni opinii. Tutaj materiał przestaje być prostą kopią komunikatu propagandowego. Zaczyna funkcjonować jako komentarz, interpretacja, osobista refleksja albo głos „niezależnego" autora. To ważny moment, ponieważ treść zostaje odłączona od pierwotnego źródła i opatrzona pozorem autentyczności.

Czwarty etap obejmuje wykorzystanie mediów społecznościowych. Treść jest dystrybuowana przez konta, grupy, strony, profile tematyczne i użytkowników, których aktywność może być autentyczna, inspirowana, opłacana albo w pełni kontrolowana. Na tym poziomie przeciwnik dostosowuje przekaz do języka grupy, jej emocji i uprzedzeń. Ta sama narracja może mieć kilka wariantów: patriotyczny, antyelitarny, antyukraiński, antyzachodni, antysystemowy, konserwatywny, radykalny lub pozornie ekspercki.

Piąty etap to aktywność w obszarach wymiany opinii. Chodzi o komentarze pod artykułami, dyskusje na forach, reakcje pod wpisami osób publicznych, grupy lokalne i zamknięte kanały komunikacji. Tutaj następuje mieszanie treści propagandowych z organicznymi emocjami społecznymi. Przeciwnik nie musi wytwarzać całej dyskusji. Wystarczy, że podsunie bodźce, które uruchomią istniejące napięcia.

Szósty etap polega na tworzeniu mikroobszarów informacyjnych. Są one dedykowane konkretnym grupom, osobom lub środowiskom o rozpoznanych podatnościach. W polskim kontekście mogą to być obszary dotyczące historii, relacji polsko-ukraińskich, bezpieczeństwa granic, migracji, kosztów wsparcia Ukrainy, zaufania do NATO albo sporów politycznych. Mikroobszar nie jest przypadkową grupą dyskusyjną. Jest środowiskiem poznawczym, w którym przeciwnik testuje, utrwala i wzmacnia określone reakcje.

Siódmy etap to skoordynowana dystrybucja z wykorzystaniem liderów opinii. Lider może być realną osobą, agentem wpływu, kontem pozornie niezależnym, influencerem, ekspertem, anonimowym profilem, grupą społecznościową albo bytem wirtualnym. Kluczowe jest to, że w oczach odbiorców posiada pewien autorytet. W tym momencie treść, która powstała w środowisku propagandowym, może wrócić do debaty publicznej jako „temat społeczny", „głos obywateli" albo „oddolna reakcja".

Ósmy etap obejmuje wyspecjalizowane operacje psychologiczne wobec wydarzeń, instytucji lub konkretnych osób. Na tym poziomie przeciwnik może prowadzić profilowanie i targetowanie, sprawdzać reakcje na bodźce, kierować presję wobec decydentów, wzmacniać lęk, budować poczucie osamotnienia albo testować odporność komunikacyjną instytucji. Nie chodzi już wyłącznie o rozpowszechnienie treści. Chodzi o uzyskanie zachowania: rezygnacji, błędu, opóźnienia decyzji, konfliktu wewnętrznego, utraty zaufania albo zmiany stanowiska.

Model ten pokazuje, że operacja wpływu nie jest prostą kampanią propagandową. Jest procesem budowy środowiska poznawczego. Przeciwnik nie tylko przekazuje informację, lecz organizuje warunki, w których odbiorca ma uznać określoną interpretację za własną.

6. Cyberprzestrzeń jako przestrzeń ekonomiki operacji

Każda operacja ofensywna ma swoją ekonomikę. Przeciwnik kalkuluje koszty, ryzyka, spodziewany efekt, możliwość zaprzeczenia, trwałość skutków i prawdopodobieństwo wykrycia. Z tego powodu nie zawsze wybiera najbardziej zaawansowane technicznie środki. Często korzysta z prostszych, tańszych i mniej ryzykownych metod: socjotechniki, aktywów osobowych, fizycznego dostępu do infrastruktury, korupcji, werbunku, presji, kompromitacji lub wykorzystania zaniedbań proceduralnych.

To ważne dla rozumienia cyberbezpieczeństwa. Nie można zakładać, że kompromitacja systemu wynika wyłącznie z ataku technicznego prowadzonego zdalnie.

Dostęp do infrastruktury może zostać uzyskany dzięki osobie wewnątrz organizacji, wykonawcy, podwykonawcy, serwisantowi, pracownikowi ochrony, dostawcy lub przypadkowo wykorzystanej luce organizacyjnej. W takim modelu cyberatak jest efektem wcześniejszej operacji osobowej albo fizycznej.

Również działania psychologiczne mają swoją ekonomikę. Przeciwnik może wybrać niewielki incydent, jeżeli wie, że zostanie on społecznie przeskalowany. Nie musi wywoływać realnej katastrofy. Czasami wystarczy wytworzyć przekonanie, że katastrofa jest możliwa, instytucje są bezradne, a obywatele nie mają dostępu do prawdy. W środowisku wysokiej polaryzacji i niskiego zaufania społecznego mały bodziec może wywołać duży efekt.

Cyberprzestrzeń jest dla takich działań wyjątkowo użyteczna. Pozwala tanio testować narracje, szybko mierzyć reakcje, obserwować zachowania odbiorców i dostosowywać przekaz. Daje możliwość skalowania działań przy niskim koszcie krańcowym. Umożliwia tworzenie pozoru masowości, pozoru spontaniczności oraz pozoru konsensusu społecznego.

7. Algorytmy, sztuczna inteligencja i nowa skala operacji wpływu

W ostatnich latach znaczenie cyberprzestrzeni jako środowiska operacji wpływu zwiększyło się z powodu rozwoju narzędzi sztucznej inteligencji, systemów generatywnych i algorytmicznej dystrybucji treści. AI nie tworzy zupełnie nowej logiki działań wpływu, ale radykalnie przyspiesza procesy, które wcześniej wymagały większych zasobów ludzkich.

Przeciwnik może szybciej generować warianty językowe, tworzyć treści dostosowane do wielu grup, tłumaczyć materiały z mniejszą liczbą błędów, symulować lokalny styl wypowiedzi, produkować grafiki, syntetyczne obrazy, nagrania, komentarze i scenariusze narracyjne. Może też automatyzować monitoring reakcji odbiorców i na tej podstawie optymalizować przekaz.

Nie oznacza to, że człowiek znika z procesu operacyjnego. Przeciwnie, rola operatora może przesunąć się z ręcznego tworzenia treści na projektowanie sekwencji oddziaływania, wybór celów, ocenę reakcji i podejmowanie decyzji o eskalacji. AI staje się narzędziem przyspieszenia, a nie samodzielnym podmiotem operacji.

Szczególne znaczenie mają również ataki algorytmiczne. Nie muszą one obecnie polegać na masowym eksponowaniu informacji w obszarze platformy. Mogą wykorzystywać jej naturalne mechanizmy rekomendacyjne, emocjonalny charakter zaangażowania, premiowanie konfliktu, szybkość reakcji i podatność użytkowników na treści skrajne. W takim modelu przeciwnik nie nasyca masowo propagandą środowisko informacyjne funkcjonujące w obszarze danej platformy, lecz eksploatuje jej logikę społeczną i ekonomiczną – algorytm doboru treści.

8. Konsekwencje dla analizy bezpieczeństwa

Jeżeli cyberprzestrzeń jest środowiskiem technologicznym, informacyjnym i poznawczym, to analiza zagrożeń musi mieć charakter interdyscyplinarny. Nie wystarczy osobna analiza techniczna, osobna analiza medialna i osobna analiza kontrwywiadowcza. Potrzebna jest zdolność łączenia danych z różnych domen.

Analityk powinien badać równocześnie: incydenty techniczne, aktywność sieciową, źródła narracji, wzorce dystrybucji, zachowania obiektów, reakcje grup społecznych, synchronizację czasową, powiązania z wydarzeniami fizycznymi, wypowiedzi oficjalnych przedstawicieli państwa adwersarza, aktywność kanałów propagandowych oraz wpływ na proces decyzyjny. Dopiero taki obraz pozwala ocenić, czy mamy do czynienia z przypadkową kumulacją zdarzeń, czy z operacją skoordynowaną.

Ważne jest również odejście od statycznego rozumienia środowiska informacyjnego. Środowisko to powinno być analizowane dynamicznie, jako zmieniający się układ relacji, kanałów, emocji, tematów i podatności. Przeciwnik może przechodzić od jednego tematu do drugiego, testować reakcje, porzucać nieskuteczne narracje i wzmacniać te, które wywołują oczekiwany efekt. Dlatego system analityczny państwa powinien być zdolny do szybkiego wykrywania anomalii, porównywania kampanii, mapowania mikrośrodowisk oraz oceny psychologicznego celu operacji.

Nie mniej istotna jest ostrożność atrybucyjna. Nie każde działanie prorosyjskie jest bezpośrednio sterowane przez państwo rosyjskie. Nie każda fałszywa informacja jest elementem operacji. Nie każdy radykalny komentarz jest działaniem wrogiego aktora. Jednak brak pewności atrybucyjnej nie powinien prowadzić do paraliżu analitycznego. Państwo może oceniać wzorce, korelacje, spójność narracyjną, synchronizację, powtarzalność i zgodność efektu z interesem adwersarza.

9. Odpowiedzialność sektora bezpieczeństwa państwa

Wielodomenowy charakter zagrożeń wymaga rewizji sposobu myślenia o odpowiedzialności za bezpieczeństwo cyberprzestrzeni. Nie może ona być wyłącznie zadaniem specjalistów od systemów teleinformatycznych. Musi obejmować również komunikację strategiczną, odporność społeczną, ochronę procesów decyzyjnych, kontrwywiad, bezpieczeństwo infrastruktury krytycznej, analizę danych, psychologię społeczną i współpracę z sektorem prywatnym.

W praktyce oznacza to potrzebę rozbudowy zespołów zdolnych do pracy na styku wielu domen. Ekspert techniczny powinien rozumieć, że incydent może mieć konsekwencje narracyjne. Analityk dezinformacji powinien rozumieć podstawową logikę cyberataków. Specjalista komunikacji kryzysowej powinien wiedzieć, jak przeciwnik może wykorzystać opóźnienie informacyjne. Decydent powinien otrzymywać nie tylko raport o incydencie, lecz także ocenę możliwego efektu psychologicznego i politycznego.

Polska dysponuje wyjątkowo silnym, choć nadal niewystarczająco promowanym międzynarodowo, środowiskiem eksperckim w obszarze cyberbezpieczeństwa, analizy operacji wpływu, komunikacji strategicznej oraz bezpieczeństwa środowiska informacyjnego. Kompetencje polskich specjalistów były kształtowane nie tylko w warunkach akademickich i technologicznych, lecz przede wszystkim w bezpośredniej bliskości realnych zagrożeń generowanych przez Federację Rosyjską, w tym operacji dezinformacyjnych, cyberataków, presji psychologicznej, działań hybrydowych oraz prób destabilizacji państw wschodniej flanki NATO. To doświadczenie daje Polsce szczególną przewagę poznawczą i operacyjną: polscy eksperci nie analizują tych zagrożeń wyłącznie jako abstrakcyjnych modeli, lecz jako zjawiska obserwowane, dokumentowane i dekomponowane w praktyce.

Miarą jakości tych kompetencji jest fakt, że polscy specjaliści są szeroko zatrudniani i angażowani na rynkach zachodnich, a ich wiedza jest wykorzystywana przez sektor bezpieczeństwa państw NATO, podmioty infrastruktury krytycznej, instytucje publiczne oraz firmy technologiczne. Dotyczy to zarówno zespołów Red Team, prowadzących zaawansowane testy penetracyjne systemów teleinformatycznych i procesów bezpieczeństwa, jak również ekspertów wspierających budowę odporności organizacji na operacje wpływu, kampanie dezinformacyjne, działania psychologiczne i skoordynowane ataki wielodomenowe. Polskie zespoły są cenione nie tylko za kompetencje techniczne, lecz także za zdolność łączenia perspektywy

cyberbezpieczeństwa, kontrwywiadu, analizy środowiska informacyjnego i komunikacji strategicznej. To właśnie ta interdyscyplinarność stanowi jedną z najważniejszych przewag polskiego środowiska eksperckiego.

Problemem pozostaje jednak ograniczona zdolność państwa, sektora eksperckiego i instytucji publicznych do systemowego promowania tych kompetencji na arenie międzynarodowej. Polska zbyt często występuje jako zaplecze eksperckie dla zachodnich struktur bezpieczeństwa, a zbyt rzadko jako państwo aktywnie definiujące standardy, metodologie i dobre praktyki w obszarze cyberodporności oraz przeciwdziałania operacjom wpływu. Tymczasem doświadczenia polskich analityków, zespołów Red Team, specjalistów cyberbezpieczeństwa i ekspertów komunikacji strategicznej powinny być traktowane jako zasób strategiczny państwa. Polska powinna znacznie odważniej prezentować własne metody analityczne, doświadczenia operacyjne i osiągnięcia jako wkład w budowę sojuszniczych standardów ochrony cyberprzestrzeni, bezpieczeństwa środowiska informacyjnego oraz odporności procesów decyzyjnych w państwach demokratycznych. W tym obszarze nie jesteśmy wyłącznie odbiorcą dobrych praktyk Zachodu, lecz możemy być ich współtwórcą, eksporterem i jednym z państw wyznaczających kierunek rozwoju nowoczesnych zdolności bezpieczeństwa.

10. Aktywna obrona jako zdolność analityczna i odpornościowa

Pojęcie aktywnej obrony w kontekście wielodomenowych zagrożeń nie powinno być rozumiane wyłącznie jako symetryczne prowadzenie operacji ofensywnych. W ujęciu państwa demokratycznego aktywna obrona oznacza przede wszystkim zdolność do wczesnego wykrywania, rozpoznawania, zakłócania skuteczności przeciwnika, ograniczania efektów psychologicznych, wzmacniania odporności i odbierania adwersarzowi inicjatywy informacyjnej.

Aktywna obrona zaczyna się od świadomości sytuacyjnej. Państwo musi wiedzieć, jakie narracje są wprowadzane, przez jakie kanały, do jakich grup, z jakimi bodźcami fizycznymi i technicznymi są powiązane oraz jaki efekt psychologiczny mają wywołać. Następnie musi być zdolne do szybkiej oceny, czy odpowiedź powinna mieć charakter techniczny, komunikacyjny, prawny, dyplomatyczny, kontrwywiadowczy, edukacyjny czy operacyjny.

Ważnym elementem aktywnej obrony jest także odporność poznawcza instytucji. Przeciwnik często nie musi przekonać całego społeczeństwa. Wystarczy, że wywoła niepewność w małej grupie decydentów, doprowadzi do opóźnienia reakcji, wzajemnych oskarżeń, chaosu komunikacyjnego albo konfliktu kompetencyjnego. Dlatego instytucje powinny ćwiczyć nie tylko reakcję techniczną, ale również reakcję informacyjną i psychologiczną.

Aktywna obrona wymaga również zdolności do dekompozycji operacji. Trzeba umieć rozłożyć kampanię na komponenty: źródła pierwotne, kanały multiplikacji, wzmacniacze, mikrogrupy, liderów opinii, narracje, bodźce emocjonalne, wydarzenia fizyczne, elementy techniczne oraz możliwy cel końcowy. Dopiero taka dekompozycja pozwala ograniczyć skuteczność przeciwnika bez ujawniania mu pełnego zakresu własnych metod i zdolności.

11. Rekomendacje dla systemu bezpieczeństwa

Po pierwsze, cyberbezpieczeństwo powinno być rozumiane szerzej niż ochrona systemów teleinformatycznych. Ochrona sieci, danych i infrastruktury pozostaje fundamentem, ale nie wyczerpuje problemu. Konieczne jest rozbudowanie analityki informacyjnej, psychologicznej i kontrwywiadowczej do oceny incydentów cybernetycznych w relacji do aktywności adwersarza w innych domenach.

Po drugie, państwo powinno rozwijać stałą zdolność mapowania środowiska informacyjnego. Nie chodzi o kontrolę debaty publicznej, lecz o rozpoznanie wrogich operacji manipulacyjnych, które wykorzystują debatę jako środowisko prowadzenia działań. Taka zdolność musi być oparta na zasadach państwa prawa, ochronie wolności słowa i przejrzystych procedurach.

Po trzecie, potrzebne są międzyinstytucjonalne zespoły analityczne łączące kompetencje cyber, FIMI, komunikacji strategicznej, OSINT, kontrwywiadu, psychologii społecznej i ochrony infrastruktury krytycznej. Współczesny przeciwnik działa wielodomenowo, dlatego analiza prowadzona w izolacji zawsze będzie spóźniona lub niepełna.

Po czwarte, należy rozwijać rozbudowane i realistyczne ćwiczenia obejmujące nie tylko atak techniczny, ale także równoległy wyciek danych, kampanię narracyjną, presję medialną, ataki algorytmiczne, sabotaż fizyczny, reakcję polityczną i komunikację kryzysową. Tylko takie scenariusze odzwierciedlają realny charakter zagrożeń.

Po piąte, Polska powinna rozwijać własne standardy bezpieczeństwa środowiska informacyjnego i promować je międzynarodowo. Posiadamy doświadczenia wynikające z położenia geopolitycznego, presji rosyjskich operacji wpływu, wojny informacyjnej wokół Ukrainy oraz udziału w ćwiczeniach sojuszniczych. Ten kapitał powinien zostać przekształcony w trwałą przewagę kompetencyjną.

12. Zakończenie

Cyberprzestrzeń nie jest już wyłącznie domeną komputerów, sieci i danych. Jest środowiskiem walki o percepcję. Współczesny adwersarz, zwłaszcza państwowy, nie oddziela cyberataków od dezinformacji, sabotażu od narracji, wycieku danych od kompromitacji, a propagandy od działań psychologicznych. Łączy je w sekwencje, których celem jest wpływ na decyzje, emocje, zaufanie i zachowania społeczne.

Modele psychologiczne leżące u podstaw rosyjskich operacji wpływu wynikają z określonego założenia operacyjnego: rzeczywistość społeczna i polityczna nie jest dla odbiorcy dostępna w sposób w pełni obiektywny, lecz jest interpretowana przez pryzmat percepcji, emocji, doświadczeń, lęków, oczekiwań i wcześniej ukształtowanych wyobrażeń. Z tej perspektywy celem operacji wpływu nie jest jedynie przekazanie fałszywej informacji, ale ukształtowanie takiego obrazu sytuacji, który doprowadzi odbiorcę do decyzji zgodnej z intencją adwersarza. W rosyjskiej tradycji działań informacyjno-psychologicznych szczególne znaczenie ma tu koncepcja zarządzania refleksyjnego, rozumiana jako wpływanie na sposób rozumowania przeciwnika poprzez dostarczanie mu odpowiednio dobranych bodźców, przesłanek i interpretacji, tak aby sam uznał określoną decyzję m. in. za racjonalną, konieczną lub bezalternatywną. Operacja wpływu nie musi więc polegać na prostym narzuceniu odbiorcy gotowej tezy. Polega na takim modelowaniu środowiska informacyjnego, aby odbiorca samodzielnie doszedł do wniosków korzystnych dla przeciwnika. W tym sensie brak obiektywizmu w środowisku operacyjnym nie jest słabością analizy, lecz jednym z fundamentów rosyjskiego podejścia do oddziaływania: skoro percepcja rzeczywistości jest podatna na kształtowanie, to przedmiotem operacji staje się nie tylko informacja, lecz cały proces jej interpretowania przez człowieka, instytucję lub społeczeństwo.

Dlatego bezpieczeństwo cyberprzestrzeni musi być rozumiane jako część szerszego bezpieczeństwa środowiska informacyjnego. Ochrona systemów

teleinformatycznych jest konieczna i kluczowa ale niewystarczająca. Państwo musi chronić także procesy poznawcze, decyzyjne i komunikacyjne. Musi rozpoznawać nie tylko ataki, ale również ich psychologiczne cele. Musi analizować nie tylko treści, ale również sekwencje, kanały komunikacji, model oddziaływania i oczekiwane efekty.

Rosyjski model działań wpływu pokazuje, że klasyczne środki aktywne nie zniknęły. Zostały przeniesione do cyberprzestrzeni, przyspieszone przez algorytmy, wzmocnione przez sztuczną inteligencję i zintegrowane z działaniami fizycznymi. To rzeczywiście „nowe wino w starych bukłakach": dawna logika manipulacji percepcją funkcjonuje dziś w środowisku cyfrowym, które zwiększa jej skalę, szybkość i precyzję.

Największym wyzwaniem dla Polski nie jest samo rozpoznanie, że takie operacje istnieją. To już wiemy. Kluczowe jest zbudowanie stałej, instytucjonalnej zdolności do ich dekompozycji, przeciwdziałania i ograniczania skutków. Polska posiada kompetencje, ekspertów i doświadczenie, aby nie tylko bronić się przed tego typu zagrożeniami, lecz także współtworzyć międzynarodowe standardy bezpieczeństwa informacyjnego i cyberodporności. To będzie jednym z priorytetów nowoczesnego systemu bezpieczeństwa Polski.

Strategia bezpieczeństwa Polski w warunkach narastającej niestabilności

Mariusz Błaszczak

Abstrakt

Tekst analizuje uwarunkowania strategiczne Polski jako państwa frontowego NATO w obliczu narastającej niestabilności geopolitycznej. Autor wskazuje na kluczowe wyzwania: konieczność dokończenia programów modernizacji sił zbrojnych, budowę systemu aktywnych rezerw, wzmocnienie krajowego przemysłu obronnego oraz rozwijanie zdolności do działania w środowisku hybrydowym. Podkreśla, że nowoczesne bezpieczeństwo wymaga nie tylko potencjału militarnego, ale również sprawnej administracji, odpornej infrastruktury krytycznej i świadomego społeczeństwa.

Słowa kluczowe: bezpieczeństwo narodowe, strategia obronna, modernizacja armii, NATO, Polska, zagrożenia hybrydowe, przemysł obronny

Współczesne środowisko bezpieczeństwa charakteryzuje się bezprecedensową niestabilnością. Trwająca agresja reżimu Putina na Ukrainę, narastająca rywalizacja mocarstw, rozwój zagrożeń hybrydowych, kryzysy energetyczne oraz gwałtowne zmiany technologiczne powodują, że bezpieczeństwo staje się podstawowym warunkiem rozwoju gospodarczego i społecznego państwa.

Polska znajduje się dziś na geopolitycznej granicy świata euroatlantyckiego. Położenie na wschodniej flance NATO daje nam wyjątkową odpowiedzialność, ale jednocześnie stwarza szansę na budowę pozycji jednego z najważniejszych państw

regionu. Warunkiem wykorzystania tej szansy jest konsekwentna realizacja strategii wzmacniania potencjału obronnego, gospodarczego i technologicznego kraju.

Kongres SET „Polska Ambitna. Jak wzmacniać państwo w niestabilnym świecie?" zgromadził ekspertów, naukowców, polityków, przedsiębiorców i przedstawicieli mediów, których wspólnym celem było wypracowanie rekomendacji dla dalszego rozwoju Polski w perspektywie najbliższych lat. W centrum debaty – za co jestem bardzo wdzięczny – znalazły się kwestie bezpieczeństwa narodowego, modernizacji sił zbrojnych, rozwoju przemysłu obronnego, odporności państwa na zagrożenia hybrydowe oraz znaczenia strategicznych sojuszy. Wspólna diagnoza tego, że właśnie obszar bezpieczeństwa jest absolutnie kluczowy dla dalszego rozwoju Ojczyzny, stanowi fundament naszej wspólnej pracy na rzecz budowy silnego, nowoczesnego i odpornego państwa. W świecie narastającej niestabilności geopolitycznej, rosnącej konkurencji gospodarczej oraz dynamicznych zmian technologicznych bezpieczeństwo przestało być jedynie jednym z elementów polityki państwa – stało się warunkiem koniecznym rozwoju społecznego, gospodarczego i cywilizacyjnego. Bez bezpiecznych granic, sprawnych instytucji, nowoczesnej armii, stabilnych źródeł energii oraz odporności na zagrożenia hybrydowe nie jest możliwe skuteczne realizowanie ambitnych celów rozwojowych. Dlatego uczestników Kongresu SET połączyło przekonanie, że inwestycje w bezpieczeństwo należy traktować nie jako koszt, lecz jako strategiczną inwestycję w przyszłość Polski, jej suwerenność, konkurencyjność oraz bezpieczeństwo kolejnych pokoleń Polaków.

Jednym z najważniejszych wyzwań stojących przed Polską pozostaje dokończenie największego programu modernizacji technicznej w historii Sił Zbrojnych RP. W latach rządów Prawa i Sprawiedliwości rozpoczęto bezprecedensowy proces wzmacniania potencjału wojskowego państwa. Zawarto kontrakty m.in. na pozyskanie samolotów F-35, czołgów Abrams i K2, armatohaubic K9, systemów Patriot, śmigłowców AW149 i Black-Hawk, a także wieloprowadnicowych wyrzutni rakiet HIMARS oraz Chunmoo, armatohaubic Krab, moździerzy Rak, satelit, dronów Wizjer, Warmate, MQ9 czy systemu antydronowego SkyControl.. Dzięki przyjęciu Ustawy o Obronie Ojczyzny oraz utworzeniu Funduszu Wsparcia Sił Zbrojnych możliwe było uruchomienie inwestycji, które przez lata pozostawały poza zasięgiem finansowym państwa. Polska stała się liderem wydatków obronnych w NATO w relacji do PKB oraz państwem budującym jedną z najsilniejszych armii lądowych Europy. Obecnie kluczowym zadaniem jest przejście od etapu zakupów sprzętu do budowy pełnej gotowości operacyjnej armii. Oznacza to integrację nowych systemów uzbrojenia,

szkolenie personelu, rozwój infrastruktury wojskowej oraz zapewnienie odpowiedniego zabezpieczenia logistycznego.

Niepokój budzi jednak wyhamowanie części programów modernizacyjnych przez obecny rząd. Dotyczy to między innymi opóźnień w realizacji kolejnych etapów programu HIMARS czy braku odpowiedniej dynamiki w zawieraniu nowych kontraktów wykonawczych. W sytuacji, gdy zagrożenie ze strony Rosji pozostaje realne, każda zwłoka w modernizacji wojska oznacza osłabienie potencjału odstraszania. Krytycznej oceny wymaga również promowany przez instytucje unijne i bezrefleksyjnie przyjęty przez obecny rząd mechanizm pożyczkowy SAFE. Choć przedstawiany jest jako narzędzie wspierające europejskie zdolności obronne, w praktyce opiera się na modelu zadłużeniowym zwiększającym zależność państw od wspólnotowych mechanizmów finansowych. Polska nie może dopuścić do sytuacji, w której tempo modernizacji własnych sił zbrojnych będzie uzależnione od politycznych decyzji podejmowanych poza Warszawą. Fundamentem bezpieczeństwa powinny pozostać krajowe zdolności finansowania obronności oraz strategiczna współpraca z najważniejszymi sojusznikami.

Doświadczenia wojny na Ukrainie jednoznacznie pokazują, że nawet najnowocześniejsze technologie nie zastąpią odpowiednio licznej armii oraz dobrze wyszkolonych rezerw. Państwa zdolne do długotrwałej obrony muszą dysponować nie tylko profesjonalnymi siłami operacyjnymi, lecz także szerokim zapleczem osobowym. Polska powinna kontynuować rozpoczęty w ostatnich latach proces zwiększania liczebności Sił Zbrojnych RP. Szczególne znaczenie ma rozwój dobrowolnych form służby wojskowej, które pozwalają budować potencjał obronny bez konieczności przywracania obowiązkowego poboru. Niezbędne jest jednocześnie zahamowanie spadku dynamiki naboru obserwowanego w ostatnim okresie oraz przywrócenie ambitnych celów związanych z budową armii liczącej ponad 300 tysięcy żołnierzy.

Równolegle należy stworzyć nowoczesny system aktywnych rezerw. Powinien on opierać się na regularnych szkoleniach, specjalizacjach wojskowych oraz trwałym związaniu rezerwistów z jednostkami wojskowymi. Warto rozważyć wprowadzenie systemu zachęt finansowych dla żołnierzy aktywnej rezerwy, które zwiększałyby atrakcyjność służby i pozwalały utrzymywać wysoki poziom gotowości. Ważnym elementem tego modelu powinno być utworzenie wyspecjalizowanych struktur odpowiedzialnych za koordynację szkolenia rezerw oraz dalsze wzmacnianie Wojsk Obrony Terytorialnej, które w ostatnich latach stały się jednym z filarów polskiego systemu bezpieczeństwa.

Nowoczesna armia nie może funkcjonować bez silnego zaplecza przemysłowego. Dlatego rozwój polskiego przemysłu obronnego powinien zostać uznany za jeden z priorytetów strategicznych państwa. Każda decyzja zakupowa musi być poprzedzona szczegółową analizą możliwości wykorzystania potencjału krajowych przedsiębiorstw. W przypadkach, w których polski przemysł jest zdolny do realizacji zamówienia, powinien otrzymywać pierwszeństwo, nawet jeśli wymaga to dłuższego procesu produkcyjnego lub większych nakładów inwestycyjnych. Już wiele miesięcy temu przedstawiłem propozycję programu „Polska armia, polski sprzęt". Będzie to zbiór nowych regulacji, które pozwolą na realne preferowanie zakupów z polskiego przemysłu zbrojeniowego. Przed każdym zakupem – czy to uzbrojenia czy też elementu wyposażenia indywidualnego żołnierzy – niezbędna będzie szczegółowa analiza dotycząca możliwości pozyskania danego sprzętu z polskich zakładów. Niezbędne jest zwiększenie produkcji amunicji wielkokalibrowej, rozwój zdolności w zakresie systemów rakietowych, bezzałogowców, elektroniki wojskowej oraz nowoczesnych systemów rozpoznania. Polska powinna konsekwentnie budować kompetencje technologiczne pozwalające na samodzielne utrzymanie potencjału obronnego w warunkach długotrwałego konfliktu. Wzmocnienia wymaga również Agencja Uzbrojenia, która powinna stać się centralnym podmiotem odpowiedzialnym nie tylko za zakupy sprzętu, ale także za koordynację badań i rozwoju, testowanie nowych technologii oraz współpracę z przemysłem. Jednocześnie potencjał krajowych przedsiębiorstw powinien być uwzględniany już na etapie strategicznego planowania rozwoju Sił Zbrojnych RP.

Współczesne konflikty coraz częściej przybierają formę działań poniżej progu wojny. Cyberataki, kampanie dezinformacyjne, sabotaż infrastruktury krytycznej czy wykorzystywanie presji migracyjnej stały się stałym elementem polityki państw agresywnych. Polska musi budować odporność państwa i społeczeństwa na tego rodzaju zagrożenia. Wymaga to stworzenia zintegrowanego systemu zarządzania kryzysowego, który będzie łączył działania administracji rządowej, samorządów, służb mundurowych oraz wojska. Szczególne znaczenie powinno mieć rozwijanie zdolności cyberobronnych oraz skutecznego przeciwdziałania dezinformacji. Konieczne jest stworzenie jednolitego systemu monitorowania zagrożeń hybrydowych, wykorzystującego nowoczesne technologie, sztuczną inteligencję oraz krajowe kompetencje technologiczne. Równie ważna pozostaje rozbudowa obrony cywilnej. Polska potrzebuje powszechnego modelu odporności społecznej angażującego obywateli, organizacje społeczne, samorządy i instytucje państwowe. Tylko takie podejście

pozwoli skutecznie reagować na sytuacje kryzysowe oraz zwiększy zdolność państwa do funkcjonowania w warunkach zagrożenia.

Bezpieczeństwo Polski jest nierozerwalnie związane z członkostwem w NATO oraz strategicznym partnerstwem ze Stanami Zjednoczonymi. To właśnie współpraca polsko-amerykańska była w ostatnich latach fundamentem budowy realnej siły odstraszania na wschodniej flance Sojuszu. Rządy Prawa i Sprawiedliwości konsekwentnie wzmacniały ten kierunek, doprowadzając do bezprecedensowego zwiększenia obecności wojsk amerykańskich w Polsce, utworzenia wysuniętego dowództwa V Korpusu Armii USA w Poznaniu, rozbudowy infrastruktury wojskowej oraz podpisania strategicznych kontraktów zbrojeniowych. Dzięki temu Polska stała się najważniejszym partnerem Stanów Zjednoczonych w Europie Środkowo-Wschodniej oraz kluczowym filarem bezpieczeństwa całego regionu. Niestety, po zmianie władzy obserwujemy systematyczne osłabianie relacji polsko-amerykańskich. Obecny rząd, kierując się politycznymi uprzedzeniami wobec dorobku poprzedników i podporządkowując swoją politykę zagraniczną oczekiwaniom największych państw Unii Europejskiej, doprowadził do wyraźnego schłodzenia kontaktów z najważniejszym sojusznikiem Polski. Zamiast wzmacniać strategiczne partnerstwo z Waszyngtonem, rząd Donalda Tuska konsekwentnie marginalizuje kierunek amerykański, próbując zastąpić go iluzorycznymi koncepcjami budowy europejskiej autonomii strategicznej. Jedną z najpoważniejszych konsekwencji tej polityki jest osłabienie politycznego znaczenia Polski w relacjach transatlantyckich. Nie ulega wątpliwości, że gdyby nie aktywność Prezydenta Rzeczypospolitej Polskiej Karola Nawrockiego, który zabiegał o utrzymanie wojskowej obecności USA w Polsce, pozycja naszego kraju byłaby dziś znacznie słabsza. To właśnie działania Prezydenta pozwoliły zachować ciągłość strategicznego dialogu oraz utrzymać amerykański kontyngent wojskowy na terytorium Rzeczypospolitej. Polska nie może pozwolić sobie na eksperymenty w obszarze bezpieczeństwa. Historia ostatnich dekad jednoznacznie pokazuje, że jedynym państwem zdolnym do zapewnienia skutecznego odstraszania militarnego wobec rosyjskiego imperializmu pozostają Stany Zjednoczone. Dlatego konieczny jest powrót do aktywnej i ambitnej polityki wzmacniania relacji polsko-amerykańskich, odbudowy zaufania w relacjach z Waszyngtonem oraz dalszego rozwijania współpracy wojskowej, technologicznej i energetycznej. Polska powinna ponownie stać się najbliższym sojusznikiem USA w regionie, a nie państwem biernie oczekującym na decyzje podejmowane w Berlinie czy Brukseli. Silny sojusz ze Stanami Zjednoczonymi pozostaje bowiem nie tylko gwarancją bezpieczeństwa

militarnego, ale także jednym z najważniejszych instrumentów wzmacniania polskiej suwerenności i podmiotowości na arenie międzynarodowej.

Nowoczesne państwo musi być przygotowane do funkcjonowania w warunkach kryzysu, konfliktu zbrojnego oraz długotrwałej presji hybrydowej. Współczesna obronność nie ogranicza się wyłącznie do potencjału militarnego, ale obejmuje również zdolność państwa do utrzymania ciągłości działania instytucji publicznych, gospodarki oraz kluczowych usług dla obywateli. Oznacza to konieczność systemowego dostosowania infrastruktury transportowej, energetycznej, teleinformatycznej i logistycznej do wymogów bezpieczeństwa narodowego. Szczególnego znaczenia nabiera rozwój infrastruktury podwójnego zastosowania (dual-use infrastructure), która w czasie pokoju służy rozwojowi gospodarczemu, a w sytuacji zagrożenia może zostać wykorzystana do realizacji zadań obronnych. Drogi ekspresowe, autostrady, linie kolejowe, porty morskie, terminale przeładunkowe, lotniska cywilne i wojskowe oraz sieci telekomunikacyjne powinny być projektowane i modernizowane z uwzględnieniem wymogów operacyjnych Sił Zbrojnych RP oraz wojsk sojuszniczych. Jednym z najważniejszych wyzwań stojących przed Polską jest rozwój zdolności w obszarze Military Mobility, czyli wojskowej mobilności. Inicjatywa ta, realizowana zarówno w ramach NATO, jak i Unii Europejskiej, zakłada eliminowanie infrastrukturalnych, administracyjnych i prawnych barier utrudniających szybkie przemieszczanie wojsk oraz sprzętu wojskowego pomiędzy państwami sojuszniczymi. Polska, jako państwo frontowe NATO, odgrywa w tym systemie rolę kluczowego hubu logistycznego dla całej wschodniej flanki Sojuszu. Wymaga to dalszych inwestycji w sieć transportową zdolną do przenoszenia ciężkiego sprzętu wojskowego, rozbudowy przepraw mostowych o odpowiedniej nośności, modernizacji infrastruktury kolejowej oraz zwiększania przepustowości portów morskich i lotniczych. Szczególną rolę odgrywa również tzw. Host Nation Support (HNS), czyli system wsparcia państwa-gospodarza dla wojsk sojuszniczych. Polska musi rozwijać zdolności związane z przyjęciem, rozmieszczeniem, zaopatrzeniem i zabezpieczeniem logistycznym dużych zgrupowań wojsk NATO, które w sytuacji kryzysowej mogłyby zostać szybko przerzucone na wschodnią flankę. Obejmuje to zarówno przygotowanie infrastruktury wojskowej, magazynowej i paliwowej, jak również zdolności do koordynacji działań administracji cywilnej i wojskowej. Kluczowym elementem bezpieczeństwa pozostaje również ochrona infrastruktury krytycznej. Ostatnie lata pokazały, że obiekty energetyczne, sieci przesyłowe, gazociągi, terminale LNG, systemy teleinformatyczne, centra danych czy infrastruktura satelitarna stają się pierwszoplanowymi celami działań

sabotażowych, cyberataków oraz operacji dywersyjnych. Polska musi budować wielowarstwowy system ochrony infrastruktury krytycznej, integrujący zdolności wojskowe, służby specjalne, administrację publiczną oraz operatorów strategicznych zasobów państwa. Skuteczna logistyka wojskowa i rozwój zdolności Military Mobility są dziś równie istotnym elementem odstraszania jak liczebność armii czy nowoczesne uzbrojenie. Zdolność do szybkiego przerzutu wojsk własnych i sojuszniczych, utrzymania ciągłości dostaw oraz zapewnienia funkcjonowania państwa w warunkach konfliktu stanowi jeden z najważniejszych czynników budujących wiarygodność obronną Polski oraz całego NATO na wschodniej flance Sojuszu.

Silne państwo wymaga nie tylko nowoczesnej armii, ale również świadomego i przygotowanego społeczeństwa. Budowa kultury bezpieczeństwa narodowego powinna stać się jednym z najważniejszych celów polityki publicznej w nadchodzącej dekadzie. Niezbędne jest rozwijanie edukacji proobronnej i patriotycznej już od najmłodszych lat. Programy nauczania powinny w większym stopniu uwzględniać zagadnienia związane z bezpieczeństwem państwa, reagowaniem kryzysowym, zagrożeniami hybrydowymi oraz podstawami obronności. Wzorem państw takich jak Finlandia należy organizować regularne ćwiczenia z udziałem obywateli, administracji publicznej i wojska. Pozwoli to zwiększyć odporność społeczną, poprawić koordynację działań w sytuacjach kryzysowych oraz budować zaufanie między instytucjami państwa a obywatelami. Ważnym elementem powinno być również wykorzystanie nowoczesnych narzędzi cyfrowych do informowania społeczeństwa o zagrożeniach i sposobach reagowania na sytuacje kryzysowe. Rozbudowa systemów ostrzegania, edukacji cyfrowej oraz przeciwdziałania dezinformacji stanie się jednym z filarów bezpieczeństwa państwa w XXI wieku.

Współczesne wyzwania wymagają od Polski strategicznego myślenia oraz konsekwentnej realizacji długofalowych celów. Bezpieczeństwo narodowe nie może być przedmiotem krótkoterminowych sporów politycznych. Musi stać się wspólnym projektem państwa, realizowanym ponad podziałami. Dokończenie modernizacji Sił Zbrojnych RP, budowa licznej armii i nowoczesnych rezerw, rozwój przemysłu obronnego, wzmacnianie odporności na zagrożenia hybrydowe, utrzymanie strategicznego partnerstwa ze Stanami Zjednoczonymi oraz budowa kultury bezpieczeństwa narodowego stanowią kluczowe kierunki działań dla Polski w najbliższych latach. Tylko państwo silne militarnie, odporne społecznie, nowoczesne technologicznie i zakorzenione w trwałych sojuszach będzie w stanie skutecznie chronić swoje interesy oraz zapewnić obywatelom bezpieczeństwo i warunki do dalszego rozwoju.

Systemy dronowe: strategiczne wyzwanie w budowie bezpieczeństwa Polski

gen. bryg. rez. Mirosław Bryś,

Paweł Wiszniewski

ABSTRAKT:

Artykuł analizuje rewolucję dronową jako strategiczne wyzwanie dla bezpieczeństwa Polski. Autorzy wskazują, że doświadczenia ukraińskiego pola walki fundamentalnie zmieniły logikę bezpieczeństwa – drony stają się ekwiwalentem i mnożnikiem siły tradycyjnych systemów. Omawiają skrócenie cyklu bojowego, premiowanie państw zdolnych do szybkiej integracji cywilnego i wojskowego potencjału technologicznego oraz wyzwania w zakresie budowy systemów przeciwdronowych i krajowego przemysłu.

Słowa kluczowe: systemy dronowe, UAV, bezpieczeństwo Polski, rewolucja bezzałogowa, drony bojowe, obrona powietrzna, przemysł obronny

Wprowadzenie

Ukraina funkcjonuje dziś jako najszybsze i najbardziej efektywne laboratorium innowacji we współczesnej sztuce wojennej. Nie dlatego, że prowadzi uporządkowany program badawczy w warunkach pokoju, lecz dlatego, że pod presją wojny wysokiej intensywności wytworzyła bezprecedensowy rytm adaptacji technicznej,

organizacyjnej i taktycznej. To właśnie tam, na oczach całego świata, testowane są nowe relacje między tanim środkiem bojowym a kosztownym celem, między rozpoznaniem a rażeniem, między improwizacją a przemysłem, między oprogramowaniem a fizyczną platformą. Wojna rosyjsko-ukraińska potwierdziła, że bezzałogowce nie są dodatkiem do klasycznych sił zbrojnych, ale jednym z głównych determinantów skuteczności działań bojowych .

Dla Polski oznacza to konieczność zasadniczej rewizji myślenia o bezpieczeństwie państwa. Systemy dronowe i antydronowe nie mogą być traktowane jako wąski sektor modernizacji technicznej, ograniczony do wybranych programów zakupowych czy pojedynczych projektów przemysłowych. Są one nową warstwą funkcjonowania wojska, obrony granicy, ochrony infrastruktury krytycznej, bezpieczeństwa wewnętrznego i odporności państwa w warunkach kryzysu. Kto nie zbuduje własnego ekosystemu bezzałogowego, ten będzie w przyszłym konflikcie działał wolniej, przy uboższej świadomości pola walki i drożej od przeciwnika .

W polskich warunkach stawka jest szczególna. Państwo frontowe NATO, sąsiadujące z obszarem najbardziej intensywnej wojny w Europie od 1945 roku, nie może ograniczyć się do biernej obserwacji cudzych doświadczeń. Musi przetworzyć je na własne zdolności operacyjne, przemysłowe i doktrynalne. W praktyce oznacza to potrzebę budowy narodowej architektury bezzałogowej: od rozpoznania i rażenia, przez logistykę i świadomość sytuacyjną, aż po walkę radioelektroniczną, SIGINT, obronę antydronową i system szybkiego testowania nowych rozwiązań.

Rewolucja bezzałogowa i jej sens strategiczny

Współczesna rewolucja dronowa nie polega jedynie na pojawieniu się nowych platform latających, pływających czy pełzających. Jej istota tkwi w zmianie całej ekonomii pola walki. Relatywnie tanie systemy bezzałogowe mogą wykrywać, śledzić i niszczyć cele o nieporównywalnie wyższej wartości, a przy tym wymuszają stałą obecność sensorów nad przestrzenią operacyjną. Oznacza to, że zanikają tradycyjne bezpieczne strefy zaplecza taktycznego. Stanowiska artylerii, wozy dowodzenia, kolumny logistyczne, składy paliw, przeprawy i elementy infrastruktury stają się widoczne i podatne na uderzenie szybciej niż kiedykolwiek wcześniej .

Drugim wymiarem tej zmiany jest skrócenie cyklu bojowego. Dron przekazuje obraz, wykrywa emisję, identyfikuje cel, wspiera decyzję ogniową albo sam staje się

efektorem. W rezultacie przewagę uzyskuje ten, kto potrafi połączyć sensory, łączność, analizę danych, system dowodzenia i środek rażenia w jeden spójny układ. Sama platforma nie wystarcza. O przewadze rozstrzyga szybkość obiegu informacji i zdolność adaptacji do przeciwdziałania przeciwnika. Dlatego system bezzałogowy jest dzisiaj bardziej siecią niż pojedynczym statkiem powietrznym.

Trzeci aspekt ma charakter ustrojowy. Rewolucja dronowa premiuje państwa zdolne do szybkiego sprzęgania armii, przemysłu, uczelni, laboratoriów i użytkowników frontowych. Wojna na Ukrainie pokazała, że sztywne, wieloletnie cykle pozyskiwania uzbrojenia są zbyt wolne wobec tempa zmian technologicznych. Rozwiązanie, które po sześciu miesiącach na froncie okazuje się skuteczne, po kolejnych sześciu może wymagać głębokiej modyfikacji z powodu zmian w zakłócaniu, wykrywaniu, automatyzacji lub taktyce użycia. Państwo, które nie potrafi uczyć się w takich cyklach, przegrywa nie tylko technologicznie, ale operacyjnie.

Polska baza zdolności: atuty i bariery

Polska dysponuje już pewnymi elementami przyszłego systemu bezzałogowego. Wojsko wprowadza do służby krajowe zestawy mini przeznaczone do rozpoznania obrazowego, wskazywania celów i wsparcia działań pododdziałów, a także systemy poszukiwawczo-uderzeniowe integrowane z artylerią i cyfrowym dowodzeniem ogniem. Równolegle rozwijana jest najniższa warstwa obrony antydronowej, projektowana jako uzupełnienie szerszej architektury obrony powietrznej państwa. To są ważne fundamenty, bo pokazują, że w Polsce istnieje zdolność nie tylko do kupowania gotowych produktów, ale również do rozwijania własnych kompetencji w obszarze rozpoznania, rażenia i ochrony wojsk .

Nie wolno jednak mylić fundamentu z systemem dojrzałym. Dotychczasowy przebieg części programów bezzałogowych, Laboratoriów Dronowych, itp. pokazał, że polski model pozyskiwania sprzętu bywa zbyt wolny, zbyt sformalizowany i zbyt słabo zsynchronizowany z dynamiką współczesnego pola walki. Pojawiały się opóźnienia, korekty założeń, a także krytyka części rozwiązań jako niedostosowanych do realiów wojny nasyconej dronami i walką radioelektroniczną. To ważna lekcja: w sektorze bezzałogowym sukces nie zależy wyłącznie od zdolności uruchomienia programu, ale od zdolności ciągłego modernizowania go w krótkim rytmie .

Jednocześnie Polska posiada zasoby, które mogą przesądzić o powodzeniu takiej transformacji. Należą do nich kompetencje instytutów wojskowych i uczelni technicznych, doświadczenie zakładów przemysłowych, rozwijający się sektor prywatny, zaplecze informatyczne, elektronika, łączność, automatyka, analiza danych oraz specjalizacje z pogranicza cyberbezpieczeństwa i SIGINT. Kluczowy problem nie dotyczy więc wyłącznie technologii, lecz organizacji państwowej: czy te zdolności zostaną spięte w jeden narodowy ekosystem, czy pozostaną rozproszone między projektami, resortami i zamówieniami o zbyt małej skali .

Lekcja ukraińska dla Polski

Najważniejsza lekcja z Ukrainy brzmi: bezzałogowce są dziś zasobem zużywalnym, a nie elitarnym dodatkiem do pola walki. Ich wartość wynika z masy, dostępności, zdolności szybkiego wdrażania zmian i umiejętności łączenia ich z rozpoznaniem, ogniem pośrednim oraz walką radioelektroniczną. To wymusza odejście od myślenia kategorią małej liczby kosztownych platform na rzecz warstwowego portfela środków: od bardzo tanich dronów do działań bezpośrednich, przez systemy rozpoznawcze i amunicję krążącą, po bardziej zaawansowane środki operujące w środowisku zagłuszanym. Obecnie Ukraińskie Wojska Systemów Bezzałogowych (USF) składają się z 12 brygad co stanowi około 2,5% Sił Zbrojnych Ukrainy, ale odpowiadają za 36,5% wszystkich uderzeń bojowych. Ponadto wykonały uderzenia na 20-cia rafinerii ropy naftowej, co stanowi 25% rosyjskiej infrastruktury naftowej.

Druga lekcja dotyczy znaczenia warstwy niewidzialnej. Na Ukrainie o przeżywalności platformy coraz częściej decyduje nie aerodynamika, lecz zdolność pracy w zakłóconym środowisku elektromagnetycznym, jakość oprogramowania, elastyczność łączności, tempo aktualizacji oraz umiejętność ukrycia własnej sygnatury. Innymi słowy: nowoczesny system dronowy jest jednocześnie systemem informacyjnym i elektromagnetycznym. Polska powinna wyciągnąć z tego wniosek strategiczny i kierować większą część inwestycji nie tylko w same platformy, ale także w oprogramowanie, algorytmy, kryptografię, sensory, nawigację odporną na zakłócenia, wykrywanie emisji i integrację danych.

Trzecia lekcja ma wymiar instytucjonalny. Ukraińskie doświadczenia są już przenoszone do ćwiczeń sojuszniczych, w których operatorzy i specjaliści z frontu wspierają NATO w doskonaleniu rozpoznania oraz zwalczania małych systemów

bezzałogowych. To dowód, że wiedza powstająca na wojnie nie jest wiedzą lokalną, lecz staje się standardem odniesienia dla zachodnich armii. Polska powinna więc stworzyć trwałe mechanizmy przejmowania tej wiedzy: wspólne laboratoria, poligony testowe, programy przemysłowe i ścieżki eksperymentalne, w których praktycy frontowi, analitycy i konstruktorzy pracują razem nad rozwiązaniami dostosowanymi do realiów Europy Środkowo-Wschodniej .

Systemy antydronowe jako nowa warstwa obrony państwa

Budowa własnych zdolności bezzałogowych ma sens tylko wtedy, gdy rozwijana jest równolegle narodowa zdolność obrony przed dronami przeciwnika. W warunkach konfliktu wysokiej intensywności zagrożone są nie tylko związki taktyczne wojsk lądowych, ale także lotniska, bazy logistyczne, składy amunicji, sieci energetyczne, terminale paliwowe, węzły telekomunikacyjne, granica państwowa i elementy infrastruktury krytycznej. Oznacza to, że problem C-UAS wykracza poza klasyczne siły zbrojne i staje się zagadnieniem bezpieczeństwa całego państwa .

Najpoważniejszym błędem byłoby utożsamienie obrony antydronowej wyłącznie z pojedynczym środkiem kinetycznym. Skuteczna obrona musi być warstwowa i ekonomicznie racjonalna. Powinna łączyć radary krótkiego zasięgu, pasywne sensory, optoelektronikę, rozpoznanie emisji, zakłócanie, podszywanie sygnału, efektory bardzo krótkiego zasięgu, osłonę ważnych obiektów oraz procedury ograniczające własną widoczność elektromagnetyczną. Celem nie jest jedynie zestrzelenie pojedynczego drona, ale rozbicie całego łańcucha jego działania: od operatora, przez transmisję danych, po integrację z ogniem przeciwnika.

W tym miejscu rośnie znaczenie SIGINT i walki radioelektronicznej. Kto potrafi wykrywać, klasyfikować i analizować sygnały związane z pracą systemów bezzałogowych, ten zyskuje przewagę zarówno defensywną, jak i ofensywną. Może nie tylko zakłócać lub przejmować platformy, lecz także identyfikować nawyki działania operatorów, schematy taktyczne i strukturę ugrupowania przeciwnika. Dla Polski jest to szczególnie ważne, ponieważ właśnie na styku dronów, rozpoznania elektromagnetycznego i obrony infrastruktury krytycznej może powstać jedna z najbardziej obiecujących narodowych specjalizacji bezpieczeństwa.

Kierunki działania dla Polski

Pierwszym zadaniem państwa powinno być opracowanie narodowej strategii dronowej, która nie będzie dokumentem resortowym, lecz całościową koncepcją bezpieczeństwa. Taka strategia musi objąć jednocześnie siły zbrojne, ochronę granicy, bezpieczeństwo infrastruktury krytycznej, wykorzystanie cywilne oraz sektor podwójnego zastosowania. Chodzi o stworzenie jednego porządku działania dla różnych obiegów technologii, finansowania i regulacji. Bez tego państwo będzie rozwijało odrębne inicjatywy wojskowe, przemysłowe i cywilne, które nie złożą się w spójny system odporności. W praktyce strategia dronowa powinna określać priorytetowe klasy platform, architekturę C-UAS, standardy interoperacyjności, zasady ochrony danych, model współpracy z przemysłem oraz ścieżki użycia technologii cywilnych w strukturach bezpieczeństwa państwa .

Drugim kierunkiem musi być stworzenie szybkiej ścieżki zakupowo-testowej dla systemów bezzałogowych i antydronowych. W tej domenie nie działa klasyczny model wieloletniego pozyskania, w którym specyfikacja jest zamrażana na początku programu, a sprzęt trafia do użytkownika po latach. Potrzebny jest system krótkich cykli: testów poligonowych, wniosków użytkowników, poprawy wersji, wdrożeń ograniczonych serii i ponownej oceny. Tylko taki mechanizm pozwoli utrzymać zgodność sprzętu z realiami walki elektronicznej oraz zmieniającą się taktyką użycia. Polska ma już przesłanki do takiego podejścia, bo w debacie resortowej pojawia się koncepcja „rewolucji dronowej" i nasycenia wojska systemami bezzałogowymi; teraz trzeba nadać temu trwałą formę instytucjonalną i budżetową .

Trzecim zadaniem jest systemowe włączenie doświadczeń ukraińskich do polskich programów badawczo-rozwojowych, szkolenia i definiowania wymagań operacyjnych. Nie chodzi o bierne kopiowanie cudzych konstrukcji, lecz o stworzenie mechanizmu stałego transferu wiedzy z najbardziej dynamicznego pola walki współczesnego świata. Polska powinna organizować wspólne zespoły eksperymentalne, zapraszać praktyków frontowych do programów szkoleniowych, prowadzić wspólne testy odporności na zakłócenia oraz rozwijać partnerstwa przemysłowe z podmiotami, które sprawdziły swoje rozwiązania w wojnie. Wnioski z Ukrainy powinny być obecne nie na marginesie analiz, lecz w samym centrum procesu tworzenia wymagań dla nowych systemów.

Czwarty kierunek dotyczy struktury inwestycji. Polska nie może popełnić błędu typowego dla państw przywiązanych do klasycznego myślenia sprzętowego, czyli

skupienia nadmiernej uwagi na samym płatowcu. O powodzeniu w wojnie dronowej coraz częściej decydują oprogramowanie, sztuczna inteligencja, systemy wspomagania decyzji, nawigacja w środowisku zakłóconym, łączność odporna na degradację, SIGINT, walka radioelektroniczna i integracja w ramach jednej sieci dowodzenia, uzupełnione o nowoczesne zaplecze logistyczne w postaci druku przyrostowego druku 3D/wytwarzania przyrostowego. To właśnie tam powstaje realna przewaga. Państwo, które ograniczy się do składania platform z importowanych komponentów, nie zbuduje suwerenności technologicznej. Państwo, które opanuje warstwę kodu, danych, analityki i elektromagnetyki oraz 3D/wytwarzania przyrostowego uzyska zdolność trwałej adaptacji.

Piątym obszarem jest rozwój krajowej produkcji masowej tanich efektorów i platform zużywalnych, w tym amunicji krążącej oraz prostszych systemów bezzałogowych przeznaczonych do działań bezpośrednich. Wojna na Ukrainie pokazała, że siłę tworzy nie tylko kilka zaawansowanych systemów, ale przede wszystkim zdolność masowego odtwarzania strat i utrzymywania wysokiego tempa użycia. To wymaga innej filozofii przemysłowej: krótszych serii, większej elastyczności, standaryzacji komponentów i zdolności do szybkiego zwiększania produkcji. Jeżeli Polska chce zbudować odporność na długotrwały konflikt, musi posiadać własną bazę przemysłową zdolną do wytwarzania tysięcy środków, a nie wyłącznie pojedynczych, wysoko wycenionych systemów specjalistycznych.

Szóstym wymogiem strategicznym jest budowa wielowarstwowego systemu C-UAS obejmującego wojska operacyjne, obronę terytorialną, granicę państwową i infrastrukturę krytyczną. W tym obszarze nie wystarczy zabezpieczenie pojedynczych jednostek wojskowych. Potrzebna jest architektura narodowa, która łączy rozpoznanie, wykrywanie, ostrzeganie, zakłócanie, neutralizację i zarządzanie incydentami. Tylko wtedy możliwa będzie obrona rozproszonych obiektów i ruchomych związków taktycznych w środowisku nasyconym dronami. Szczególne znaczenie ma tutaj włączenie do systemu również podmiotów odpowiedzialnych za bezpieczeństwo infrastruktury krytycznej, ponieważ przyszły kryzys lub wojna nie ograniczą się do klasycznego frontu.

Siódmym kierunkiem powinno być tworzenie trwałych konsorcjów łączących przemysł prywatny, duże podmioty państwowe, instytuty badawcze, uczelnie techniczne i wojskowych użytkowników końcowych. W sektorze bezzałogowym przewaga rodzi się na styku różnych kompetencji: lotniczych, elektronicznych, programistycznych, materiałowych, analitycznych i operacyjnych. Żaden pojedynczy podmiot

nie będzie w stanie samodzielnie utrzymać pełnego spektrum innowacji. Państwo powinno więc działać jako architekt ekosystemu, który tworzy wspólne standardy, zamawia rozwiązania modułowe, finansuje prototypowanie i wymusza interoperacyjność. Tylko w takim modelu można uniknąć jednoczesnego rozproszenia wysiłku i monopolizacji innowacji przez jedną instytucję lub grupę interesu.

Ósmą osią wysiłku państwa musi być rozwój polityki eksportowej wobec państw flanki wschodniej i Europy Środkowej. Jeśli Polska zbuduje własny, wiarygodny ekosystem bezzałogowy oparty na doświadczeniach pola walki, zyska nie tylko zdolność obronną, lecz również instrument wpływu regionalnego. Państwa regionu będą potrzebowały relatywnie tanich, kompatybilnych z NATO i szybko modernizowanych systemów rozpoznawczych, uderzeniowych i antydronowych. Polska może stać się dostawcą takich rozwiązań, pod warunkiem, że wcześniej sama zbuduje odpowiednią skalę produkcji, mechanizmy serwisowe i zaplecze badawczo-rozwojowe. W ten sposób sektor bezzałogowy może stać się jednym z filarów polskiej specjalizacji strategicznej: jednocześnie wojskowej, przemysłowej i geopolitycznej.

Zakończenie

Ukraina realnie stała się najbardziej brutalnym, a zarazem najszybszym laboratorium innowacji we współczesnej sztuce wojennej. Wojna rosyjsko-ukraińska jest coraz częściej opisywana przez analityków właśnie jako przestrzeń skrajnej presji operacyjnej, w której równolegle testowane są nowe taktyki, technologie i modele organizacyjne, szczególnie w obszarze systemów bezzałogowych, rozpoznania oraz C-UAS. Pole walki funkcjonuje tam jak gigantyczny poligon porównawczy: rozwiązania komercyjne, improwizowane, wojskowe i sojusznicze są niemal natychmiast weryfikowane przez przeciwnika, a cykl „pomysł–wdrożenie–kontrdziałanie" trwa nie lata, lecz tygodnie. Z perspektywy zewnętrznych obserwatorów Ukraina stała się więc nie tylko miejscem przyspieszonej innowacji sprzętowej – obejmującej drony, walkę radioelektroniczną i sensory – ale także przestrzenią głębokiej rewizji myślenia strategiczno-operacyjnego, redefiniującej znaczenie manewru, maskowania, rozproszenia, logistyki oraz zarządzania polem walki nasyconym sensorami.

Wojna za polską granicą pokazała, że systemy bezzałogowe zmieniają naturę współczesnego pola walki szybciej niż większość tradycyjnych kategorii uzbrojenia. Dla Polski nie jest to problem obserwowany z zewnątrz, lecz bezpośrednie wyzwanie

strategiczne. Państwo, które chce skutecznie odstraszać, bronić terytorium i zachować autonomię decyzji w czasie kryzysu, musi zbudować własną zdolność do projektowania, produkcji, integrowania i zwalczania systemów bezzałogowych na dużą skalę.

Polska posiada ku temu podstawowe warunki: zaplecze inżynierskie, potencjał przemysłowy, rosnące zainteresowanie państwa i wyjątkowe położenie geostrategiczne. Brakuje jednak nie tyle wiedzy o kierunku zmian, ile dostatecznie szybkiej decyzji o skali działania. W świecie, w którym Ukraina stała się najbardziej dynamicznym laboratorium innowacji wojskowej, Polska nie może pozostać jedynie obserwatorem. Powinna stać się najbliższym, najbardziej kompetentnym i najlepiej zorganizowanym beneficjentem tej lekcji.

Między rynkiem, geopolityką a realną mocą produkcyjną przemysłu obronnego. Wpływ toczących się na świecie konfliktów zbrojnych na zmiany trendów zakupowych

Sebastian Chwałek

Abstrakt:

Artykuł analizuje wpływ toczących się konfliktów zbrojnych na trendy zakupowe i możliwości produkcyjne przemysłu obronnego. Autor konfrontuje narrację o „rozpędzonej machinie produkcyjnej" z danymi rynku kapitałowego po korekcie lat 2025–2026. Omawia niespójność między zapotrzebowaniem a możliwościami produkcyjnymi, geopolityczne napięcia w łańcuchach dostaw i nowe priorytety: amunicja, systemy przeciwlotnicze, drony.

Słowa kluczowe: przemysł obronny, rynek zbrojeniowy, geopolityka, produkcja amunicji, trendy zakupowe, Ukraina, bezpieczeństwo europejskie

1.

Za naszą wschodnią granicą kolejny rok toczy się konwencjonalny konflikt zbrojny, a każdy jego miesiąc odsłania nowe etapy – szczególnie w zakresie techniki walki i technologii używanych przez obie strony. Na ten temat powiedziano już niemal

wszystko, oprócz jednego: obie strony uczą się nawzajem nowej formy wojny – elektroniczno-robotyczno-autonomicznej. Niezależnie od sporów wśród obserwatorów i ekspertów widać, że sam rynek zbrojeniowy bardzo się zmienia – albo przynajmniej sugeruje, że się zmienia – a o przewadze coraz częściej decydują rozwiązania hybrydowo-sieciowe, łączące arsenały elektroniczne z bronią kinetyczną. Czy mamy więc do czynienia z nową erą tej branży? Czy na tle światowych trendów Polska wypada dobrze? A może to tylko przejściowy impuls rozwojowy dla przemysłu obronnego?

W mediach często widzimy nagłówki o kolejnych inwestycjach i podpisanych umowach na dostawy sprzętu dla poszczególnych armii. Rzadziej pojawiają się informacje o kłopotach – nawet u największych graczy. Komunikaty giełdowe spółek z tej branży zazwyczaj prowadzą do „zielonych" wzrostów, a w Polsce, szczególnie w ostatnich miesiącach, na parkiecie widać wyraźne trendy wzrostowe dzięki przemyślanym decyzjom notowanych podmiotów obronnych. Tylko nieliczne z tych sygnałów dotyczą jednak poważnych zakupów dających nadzieję na dużą, długoletnią produkcję. Sporo wątpliwości pojawiło się wokół programu SAFE, który w oficjalnym przekazie obozu rządzącego ma być cudownym lekarstwem i impulsem rozwojowym. Już kilka dni po jego wdrożeniu – wątpliwym pod względem formalno-prawnym – pojawiły się pierwsze niepokojące sygnały: o wyższych kosztach obsługi długu, o nieprzemyślanych zakupach, o niekorzystnych zapisach w umowach pośpiesznie podpisywanych przez podmioty zmuszane wizją braku dalszych zamówień. Krajowy rynek znalazł się w niekomfortowej sytuacji, zwłaszcza jeśli chodzi o czas, jaki otrzymuje na realizację tych umów. Narzucone z góry przez UE ramy czasowe dla świadomych uczestników rynku jawią się jako mało realne. Nie jest to teza wynikająca z subiektywnych odczuć światopoglądowych, lecz z realnych doświadczeń branży – i nie jest to wyłącznie polskie odczucie, lecz sygnał płynący już od dużych europejskich graczy.

Ostatnie kilka lat to szczególny okres na całym globie. Nie trzeba być wybitnym analitykiem, by zauważyć, że rok 2019 i „szalejąca" pandemia dały początek wielu niepokojącym zjawiskom. Odczuwalny do dziś zastój produkcji, w powiązaniu z zerwaniem globalnych łańcuchów dostaw, obnażył uzależnienie największych koncernów przemysłowych – także z sektora obronnego – od zagranicznych poddostawców. Pogoń za maksymalizacją zysków, cięciem kosztów i wpisywaniem się w eko-trendy doprowadziła do utraty stabilnej produkcji na rynkach macierzystych. Likwidacja linii produkcyjnych i brak wykwalifikowanej kadry oznaczały utratę kompetencji wytwarzania niektórych komponentów – co szybko odbiło się na zdolnościach produkcyjnych w kolejnym okresie.

Wybuch wojny na Ukrainie, poprzedzony działaniami hybrydowymi na granicy polsko-białoruskiej i zaognieniem sytuacji na Bliskim Wschodzie, spotęgował te problemy. Zwiększone zapotrzebowanie na sprzęt wojskowy, błyskawicznie pustoszejące magazyny poszczególnych państw oraz braki materiałowe wynikające z ograniczeń geopolitycznych uwidoczniły ogromny popyt – i równie wielki problem z jego zaspokojeniem. Dziś jesteśmy już po interwencji USA w Iranie i w trakcie działań zbrojnych obejmujących kilka państw regionu. Oficjalnie wiemy, że w ciągu zaledwie kilku dni operacji siły amerykańskie zużyły spore zapasy środków bojowych, a pojawiające się komunikaty wskazują na poważne problemy przemysłu USA z tempem produkcji niektórych efektorów. W Europie nie jest lepiej – największe koncerny zmagają się z dostosowaniem zdolności do potrzeb rynku, a zwłaszcza własnych armii. Lata pokoju w naszym regionie, w połączeniu z politycznym przeświadczeniem rządów o „erze wiecznego spokoju i szczęśliwości", doprowadziły do likwidacji zdolności produkcyjnych w wielu kategoriach uzbrojenia. Dziś – mimo ogromnych zabiegów – otwarcie tego potencjału na nowo bywa bardzo trudne, a czasem wręcz niemożliwe.

W przestrzeni publicznej niezmiennie pojawiają się tezy o rozpędzonej machinie produkcyjnej. W niektórych kategoriach to nawet prawda, ale gdy zajrzymy za kulisy, okazuje się, że regionalni producenci opierają swoje zdolności na fabrykach i podwykonawcach z Republiki Południowej Afryki, Indii czy szerzej – Dalekiego Wschodu. Surowce i półprodukty również w znacznej mierze pozyskuje się spoza obszaru europejskiego. Nawet rodzimy zamawiający przekonał się, jak „europejska" bywa amunicja kalibru 155 mm jednego z naszych bliskich sąsiadów: producent ten, mimo wydajnej linii produkcyjnej ulokowanej poza Europą, nie był w stanie dostarczyć zamówionego towaru z powodów politycznych. Podawane ilościowo zdolności są oczywiście wykonalne – pod warunkiem że nic nie zakłóci międzynarodowego łańcucha dostaw i że egzotyczni z punktu widzenia odbiorcy poddostawcy wyprodukują komponenty. I nie ma tu znaczenia, czy mówimy o dostawcach amerykańskich, czy niemieckich, ani jaki jest status własnościowy poszczególnych zakładów – choć, ku zaskoczeniu, prywatny właściciel bywał mniej zainteresowany utrzymaniem realnych zdolności na terenie własnego kraju, gdy generowało to wyższe koszty. Dziś część rządów chce odzyskać lub zwiększyć kontrolę właścicielską nad przemysłem obronnym. W ramach globalizacji rozproszono produkcję po całym globie i nawet przy pełnym zaangażowaniu nie ma pewności, czy uda się skorzystać ze wszystkich zasobów. Odbudowa fabryk na terenie Europy napotyka na oczywiste przeszkody: brak wykwalifikowanego personelu, a czasem w ogóle rąk do pracy, koszty pracy i energii, ceny lokalnych surowców,

wreszcie wyśrubowane wymogi środowiskowe. Tam, gdzie lokalne zdolności podtrzymywano choćby na minimalnych obrotach, ich odtworzenie i rozbudowa są realniejsze niż powrót do całkowicie „wygaszonego pieca".

Spoglądając na powrót do wielkiej produkcji przez pryzmat rynku kapitałowego, warto przypomnieć, że po gwałtownych skokach od lutego 2022 roku indeks STOXX Europe Aerospace & Defense wzrósł o kilkaset procent, a sektor zaczął wyceniać prognozowane zyski znacznie wyżej niż szeroki STOXX Europe 600. Rok 2026 przyniósł jednak wyraźną zmianę nastrojów. Branżowi analitycy określają go mianem „okresu konsolidacji", w którym entuzjazm wobec rosnących budżetów obronnych ustępuje miejsca twardej selekcji spółek według ich fundamentów.

Liczby mówią same za siebie. Po rekordowym 2025 roku – gdy europejski indeks lotniczo-obronny zyskał kilkadziesiąt procent – początek 2026 roku przyniósł stabilizację, a momentami nawet lekkie spadki: na koniec maja 2026 r. STOXX Europe Aerospace & Defense był „pod kreską" w ujęciu od początku roku, podczas gdy szeroki STOXX Europe 600 pozostawał na plusie. Nawet wybuch wojny w Iranie nie wywołał trwałych wzrostów. Inwestorzy rewidują swoje decyzje, oczekując twardych dowodów na wzrost zysków, a to nie będzie łatwe: spore zamówienia przy napiętych terminach dostaw mogą okazać się w dłuższej perspektywie raczej obciążeniem niż atutem. Eksperci rynku finansowego zwracają też uwagę na rosnące koszty opracowywania nowych rozwiązań, wymuszone ciągle zmieniającym się charakterem działań zbrojnych.

Ciekawym odniesieniem z perspektywy południowo-wschodniej Europy był świetny debiut Czechoslovak Group (CSG) na giełdzie w Amsterdamie. Na wejściu spółka osiągnęła ponad 30-procentowy wzrost i wycenę w okolicy 43 miliardów dolarów, przewyższając SAAB i Leonardo. Dość szybko jednak kurs spadł o blisko 14%, a kapitalizacja stopniała do około 37 mld dolarów. Spadek apetytu inwestorów w jeszcze większym stopniu dotknął innych europejskich producentów. Nawet niemiecki Rheinmetall – symbol obronnej hossy – odnotował widoczną przecenę po przedstawieniu mniej optymistycznych prognoz sprzedaży. To pokazuje, jak wygląda faktyczny potencjał „dużych" graczy zmuszonych restrykcjami giełdowymi do podawania faktów, a nie marketingowych i politycznych deklaracji. Wśród zwolenników niemieckiego podmiotu dominuje przeświadczenie o tymczasowości zawirowań, ale bardzo trafnie ujęli to już wcześniej analitycy JPMorgan Chase & Co: w latach 2022–2025 założenia inwestycyjne opierano na potencjale wzrostu wynikającym z historycznych możliwości Niemiec, dziś zaś inwestorzy koncentrują się wyłącznie na realizacji. Rynek rozlicza spółki z dostarczonego sprzętu i zysków – a nie z planów i chęci.

Za oceanem jest podobnie. Notowania amerykańskiego sektora lotniczo-obronnego – śledzone choćby przez ETF iShares U.S. Aerospace & Defense (ITA), oparty na indeksie Dow Jones U.S. Select Aerospace & Defense – po styczniowych wzrostach wróciły do znacznie niższych poziomów. Pojawiają się te same opinie o zbyt optymistycznych założeniach wycen. Amerykański sektor kosmiczny i obronny opiera się na znacznie wyższych mnożnikach prognozowanych zysków niż reszta rynku (rzędu trzydziestokrotności wobec dwudziestokrotności). I tu argumentem ostrożności jest dynamicznie zmieniające się pole walki. Rynek zastanawia się, którzy producenci dają lepszą perspektywę: czy tanie drony wyprą drogie systemy rakietowe? Czy to już koniec gwałtownych zmian w taktyce walki, a tym samym w wyścigu technologicznym? Nasi sojusznicy z USA, podobnie jak rynek europejski, patrzą dziś wyłącznie na realne dane, a nie na obietnice i deklaracje.

Na europejskim podwórku nawet niemiecki „Der Spiegel" zauważa problemy z tempem produkcji u kontynentalnych potentatów. Biorąc pod uwagę znaczący wzrost ilościowy produkcji w Rosji, Unia Europejska wciąż nie ma się czym pochwalić. Również Kiloński Instytut Gospodarki Światowej (IfW Kiel) wskazuje, że produkcja zbrojeniowa w Europie powinna być znacznie wyższa, a analitycy ostrzegają, że niedostatek badań może doprowadzić do opóźnień technologicznych.

Nie od dziś wiadomo jednak, że ilość nie zawsze idzie w parze z jakością – i tak też należy traktować porównanie poziomu produkcji Rosji oraz krajów UE. Wysokie ceny jednostkowe zaawansowanego technologicznie sprzętu produkowanego przez państwa NATO dodatkowo komplikują obraz. W porównaniu z okresem początkowym koncerny europejskie produkują więcej amunicji i systemów artyleryjskich – kosztem np. czołgów czy systemów rakietowych. Wyraźne zaangażowanie widać w obszarze systemów bezzałogowych różnych klas i przeznaczeń. Eksperci z brukselskiego Instytutu Bruegla wskazują, że europejski przemysł obronny musiałby zwiększyć produkcję nawet pięciokrotnie, aby dorównać Rosji. Przytaczane dane mówią, że w pierwszym kwartale 2025 roku Rosja wyprodukowała ponad 400 czołgów – choć zdecydowana większość to zmodernizowane starsze konstrukcje, głównie T-90M. Głośno zapowiadany, przełomowy T-14 Armata, zaprezentowany w 2015 roku, doczekał się jedynie kilkudziesięciu egzemplarzy. To pokazuje, że mimo olbrzymich wydatków i zaangażowania całego państwa Rosja mierzy się z ograniczeniami finansowymi i technologicznymi, co – na szczęście dla cywilizowanego świata – stawia przyszłość jej zbrojeniówki pod znakiem zapytania. Nie można jednak lekceważyć przeciwnika, sporadycznie wspieranego technologicznie przez ideowych sojuszników z Dalekiego Wschodu.

2.

Skoro oczywiste jest już, że cały zachodni przemysł zbrojeniowy zmaga się z poważnymi ograniczeniami – niedostosowanymi łańcuchami dostaw, niedoborami wykwalifikowanych pracowników oraz dekadami „bezinwestycyjnego pokoju" – warto spojrzeć na rodzimy przemysł właśnie przez ten pryzmat. Podobnie jak reszta Europy i USA, Polska odczuwa braki surowców, komponentów elektronicznych (zwłaszcza półprzewodników) oraz specjalistycznych materiałów wybuchowych i chemicznych. Decyzje sprzed lat o likwidacji zdolności do produkcji nitrocelulozy w Pionkach do dziś odbijają się na naszej samodzielności w wytwarzaniu prochów. Podobnie pozbyliśmy się kompetencji w produkcji silników spalinowych do pojazdów ciężarowych i sprzętu ciężkiego w Warszawie i Mielcu. Czy decyzje te były przemyślane – i czy ktoś pomógł nam je podejmować, kusząc nowoczesnymi zachodnimi rozwiązaniami – można się tylko domyślać. Wiele wojskowych rozwiązań podzieliło los innych branż polskiej gospodarki, a utrata kompetencji na dekady zatrzymała rozwój, a wraz z nim – bezpieczeństwo i odporność. Dziś różne ośrodki przemysłowe i uniwersyteckie próbują odtwarzać projekty jednostek napędowych, lecz nie idzie to w parze z zainteresowaniem państwa jako potencjalnego klienta.

Także czas oczekiwania na półprodukty od zagranicznych producentów utrudnia szybką realizację zamówień. W praktyce żaden kraj – lub bardzo niewiele państw – nie jest dziś w stanie produkować całości uzbrojenia na własne potrzeby. Największe koncerny świata korzystają z rozwiązań różnych dostawców, bo tak przez dekady ułożono system produkcji oparty na optymalizacji kosztów; nikt nie kontroluje całego łańcucha wartości, a w centrum uwagi staje dziś autonomia przemysłowa i sterowność bezpieczeństwa. Trzeba pamiętać, że dzisiejszy poziom naszpikowania sprzętu skomplikowanymi rozwiązaniami – w pociskach manewrujących czy całych systemach obrony powietrznej – generuje znacznie dłuższe cykle produkcyjne niż jeszcze kilka dekad temu. Przemysł zakłada, że odbudowa amerykańskich zapasów pocisków po konfliktach zajmuje od trzech do nawet kilkunastu lat. Nie powinno to dziwić tych, którzy znają arkana technologii i procesów produkcji: nie da się nagle zwielokrotnić produkcji bez nowych linii montażowych i parku maszynowego. To wymaga czasu i znacznych nakładów, a także pozyskania kadr zdolnych obsłużyć nowoczesną infrastrukturę. Nie wszędzie możliwa jest pełna automatyzacja, a sztuczna inteligencja – choć konieczna i już stosowana – nie uleczy wszystkich problemów produkcyjnych. Nie pomaga też presja rządów na szybsze dostawy, nakładanie kar czy straszenie utratą kontraktów.

Tam, gdzie przemysł traktuje swoje zadania poważnie, wystarczy dialog i wsparcie – po obu stronach są przecież ludzie, którzy mają w gruncie rzeczy ten sam cel.

Liderem polskiego rynku zbrojeniowego jest państwowy koncern PGZ, który – mimo różnych zawirowań i wbrew opiniom wielu przeciwników – rozwija swój potencjał i inwestuje w nowe rozwiązania, by sprostać oczekiwaniom Wojska Polskiego. Warto przypomnieć, że przez ostatnie kilka lat rodzimy koncern prowadził konsekwentną politykę inwestycyjną. Łączne nakłady inwestycyjne wszystkich spółek Grupy Kapitałowej w latach 2018–2021 wahały się w przedziale od 270 do 430 mln zł, by w 2022 roku skokowo wzrosnąć do ponad 670 mln zł (z prognozą utrzymania tego poziomu w 2023 r.) – co wiązało się ze zwiększeniem możliwości produkcyjnych spółek, m.in. dzięki przyśpieszeniu inwestycji w PCO S.A., MESKO S.A. i HSW S.A. finansowanych ze środków wsparcia. Dzięki tym nakładom powstały m.in.: nowoczesna komora bezechowa (pozwalająca badać największe systemy radarowe) w PIT-RADWAR, budynek biurowo-produkcyjny w PCO S.A., najnowocześniejsze w Europie centrum serwisowania rakiet NSM w WZE, hangar do obsługi cywilnych statków powietrznych w WZL 2, a także rozbudowa potencjału produkcyjnego amunicji wielko– i średniokalibrowej w Dezamecie w ramach programów Krab, Kryl, Rak i Tytan.

Na koniec 2023 roku PGZ S.A. nadzorowała już 11 projektów inwestycyjnych, mających zwiększyć możliwości produkcyjne spółek Grupy o łącznej wartości 2,3 mld zł, będących na różnych etapach realizacji – w tym m.in.:

- MESKO S.A. – zwiększenie potencjału produkcyjnego amunicji mało-, średnio- i wielkokalibrowej oraz rakiet;
- PIT-RADWAR S.A. – budowa nowoczesnej hali montażu finalnego i serwisu o powierzchni ok. 10 000 m² (Mazowieckie Centrum Produkcyjno-Serwisowe „Kobyłka"), zakończona w grudniu 2023 r.;
- PGZ HWIL – budowa laboratorium Hardware-in-the-Loop (jednego z trzech w Europie) w ramach offsetowych umów wykonawczych, umożliwiającego badania i symulacje rakiet o dużych rozmiarach;
- PGZ Stocznia Wojenna sp. z o.o. – ustanowienie potencjału produkcyjnego (infrastruktury, narzędzi, procesów, technologii oraz zasobów ludzkich) jako bazy do budowy trzech fregat w ramach programu Miecznik;
- FB Łucznik – zwiększenie mocy wytwórczych poprzez budowę nowej hali produkcyjnej wraz z robotyzacją procesów;
- HSW S.A. – projekt inwestycyjny związany z akwizycją zasobów LGDM i AUTOSAN.

W 2023 roku wydano zgody korporacyjne na kolejnych 8 inwestycji o łącznej wartości 5 120 mln zł.

W latach 2015–2023 Grupa PGZ przeszła znaczącą metamorfozę finansowo-ekonomiczną i organizacyjną – mimo trudnych warunków gospodarczych (pandemia, inflacja, wojna na Ukrainie). Przychody wzrosły o 118% między 2015 a 2022 rokiem (z 3 826 mln zł do 8 355 mln zł), z czego niemal 1,5 mld zł stanowił eksport – aż 18,6% całości. Prognozowano dalszy dynamiczny wzrost przychodów (powyżej 11 000 mln zł za 2023 r.), związany z toczącymi się procesami inwestycyjnymi i rosnącym portfelem zamówień. Przychody eksportowe miały wzrosnąć z 1 484 mln zł za 2022 r. do około 1,66 mld zł w 2023 r. (dane na październik), z prognozą ok. 1,8 mld zł na koniec roku. Poprawę efektywności najlepiej oddaje wskaźnik EBITDA – prognozowany wzrost o ponad 200% między 2015 (390 mln zł) a 2023 rokiem (1 224 mln zł) – świadczący o rosnącej rentowności operacyjnej: z jednej strony coraz wyższe przychody, z drugiej optymalizacja kosztów i niższe koszty jednostkowe. Rosła też wartość wieloletnich umów z MON i jednostkami podległymi: w 2021 roku podpisano je na ponad 9,5 mld zł, w 2022 roku na ponad 15,2 mld zł, a do października 2023 roku na blisko 14,3 mld zł.

W ramach rosnącego zaangażowania Grupy PGZ powołano nowe podmioty, m.in. PGZ Serwis Orzeł TOB na Ukrainie (zarejestrowany 22 września 2022 r.) oraz Polsko-Brytyjską Spółkę Okrętową. W 2022 roku, w obliczu kolejnych decyzji rządu o zwiększeniu finansowania modernizacji sił zbrojnych, koncern przyśpieszył przygotowania do następnego etapu rozbudowy potencjału. HSW S.A. ustanawiała dodatkowe moce produkcji Krabów oraz NBPWP Borsuk, zwiększała produkcję luf L44 (Leopard) i budowała zdolność wytwarzania pojazdów K9/K9PL do ponad 50 sztuk rocznie; oddział Autosan rozwijał pojazdy 4×4, a Jelcz sp. z o.o. zwiększał zdolności do 2000 pojazdów rocznie. MESKO S.A. dążyło do produkcji ponad 2 tys. zestawów PIORUN rocznie oraz pięciokrotnego wzrostu produkcji amunicji 155 mm i 120 mm, a kluczowym elementem planu pozostawała odbudowa produkcji nitrocelulozy. Plany obejmowały też polonizację pocisków BRIMSTONE, CAMM oraz wyrzutni HIMARS, a także produkcję spłonek. PIT-RADWAR rozwijał potencjał wytwarzania radarów, systemów pasywnej lokalizacji, stacji radiolokacyjnych, urządzeń kierowania uzbrojeniem i anten. WZM tworzyły zdolność obsługi czołgów Abrams oraz linię montażu K2, Bumar-Łabędy – drugą linię Krabów (do min. 50 sztuk rocznie), a Zakłady Mechaniczne „Tarnów" zwiększały produkcję elementów systemu Pilica, wyrzutni i kontenerów rakiet CAMM, broni strzeleckiej oraz siłowników do rakiet Patriot. Dezamet zwiększał moce produkcji

amunicji 120 mm RAK i 155 mm (m.in. w wersji do K9), a H. Cegielski-Poznań S.A. przygotowywał się do produkcji korpusów podwozi i wież czołgów K2PL. W 2023 roku procesy te wymagały nakładów szacowanych na około 12 mld zł; odpowiednie wnioski skierowano do MAP i ostatecznie do funduszy nadzorowanych przez KPRM. Dziś wiele z tych projektów zostało niestety wstrzymanych lub całkowicie zmienionych.

Wstrzymano również procesy rozpoczęte w ramach Narodowej Rezerwy Amunicyjnej, której celem było zwiększenie mocy produkcji amunicji w Polsce i budowa krajowych zdolności wytwarzania komponentów. PGZ złożyła wymagany wniosek do PFR/KPRM już 8 maja 2023 roku. Nowe decyzje rządu – ustawa z 27 listopada 2024 r. o finansowaniu działań zmierzających do zwiększenia zdolności produkcji amunicji, przeznaczająca 3 mld zł (czyli tyle samo co NRA) na budowę potencjału – do chwili obecnej nie zaowocowały przekazaniem środków inwestycyjnych. Dopiero 28 marca 2025 roku, jak wynika z komunikatu MAP, PGZ złożyła kolejny wniosek. Od pierwszego dokumentu w sprawie pozyskania środków na rozwój produkcji amunicji mija więc niemal dwa lata – a proces, niefrasobliwie wstrzymywany, wciąż czeka na szczęśliwy finał.

Doświadczenie wojny na Ukrainie stawia w centrum pytanie, jak dziś jesteśmy przygotowani produkcyjnie do potencjalnego konfliktu – i czy wygląda to lepiej niż w innych krajach UE. Ewolucja jest oczywiście widoczna, ale jak wszędzie, diabeł tkwi w szczegółach. Trzeba też uświadomić sobie skalę zmiany otoczenia. Jeszcze dekadę temu Polska wydawała na obronność niespełna 40 mld zł rocznie. W 2024 roku kwota ta sięgnęła już 158 mld zł, przekraczając 4% PKB, a w 2026 roku mówi się nawet o 200 mld zł – to jeden z najwyższych wskaźników w całym NATO.

Same dostępne środki i podpisane umowy nie są jeszcze sukcesem – mają jednak dać podstawę, by do 2035 roku ulokować Polskę wśród kluczowych graczy europejskiego rynku zbrojeniowego. Już dziś zarówno podmioty państwowe, jak i prywatne inwestują w transfer technologii, budując kompetencje w obszarach cyberbezpieczeństwa i sztucznej inteligencji. Zdecydowanie ważniejszym elementem systemu jest jednak zasób ludzki – talenty to być może ostatni nasz skarb. Pilnie trzeba wspierać rozwój talentów, akumulować ich dorobek, materializować go we własności intelektualnej i skalować z Polski na świat. Według danych ARP w polskim sektorze zbrojeniowym pracuje ponad 50 tys. osób, a wraz z podwykonawcami i podmiotami powiązanymi – nawet 100 tys., i jest to bardzo szerokie spektrum zawodów. Przemysł poszukuje wysoko wykwalifikowanych specjalistów: inżynierów materiałowych, elektroników, mechaników precyzyjnych, konstruktorów lotniczych, projektantów systemów uzbrojenia, ekspertów od sztucznej inteligencji i uczenia

maszynowego, inżynierii danych, awioniki, cyberbezpieczeństwa oraz projektowania 3D. Większość dużych spółek państwowych szuka dziś setek nowych specjalistów, a na polskim rynku obecni są również światowi gracze rekrutujący lokalnie. W całej Europie widoczna jest spora rotacja kadr – wynikająca m.in. z negatywnego wizerunku sektora, czasem zbyt niskich wynagrodzeń, braku równowagi między pracą a życiem prywatnym oraz specyficznej kultury organizacyjnej. Mimo to branża radzi sobie, sięgając po różne metody pozyskiwania pracowników – od rekrutacji weteranów sił zbrojnych po sponsorowanie dedykowanych kierunków studiów i szkoleń dla przyszłych kadr. Lekcja jest jedna: uczymy się przez całe życie, a co ważniejsze – produkt doskonali się codziennie, i to na linii frontu. Liczą się szybkość, niezawodność i zwinność technologiczna, mierzona zdolnością do wytwarzania modułów zestawianych zgodnie z dynamicznie zmieniającymi się potrzebami.

3.

Najszybciej zmieniającym się elementem tego krajobrazu – i najsłabiej opisanym w oficjalnych przekazach – jest rola sektora prywatnego oraz technologii podwójnego zastosowania (dual-use). To właśnie tu, na styku cywilnej innowacji i potrzeb pola walki, rozgrywa się dziś znaczna część wyścigu technologicznego. Wojna na Ukrainie pokazała, że tani, masowo produkowany dron rozpoznawczy lub uderzeniowy potrafi zneutralizować sprzęt warty setki razy więcej, a cykl modernizacji liczony jest już nie w latach, lecz w tygodniach. W takim środowisku przewagę zyskują podmioty zwinne – startupy i prywatne firmy technologiczne – zdolne iterować szybciej niż wielkie, scentralizowane koncerny.

Zmiana ta jest doskonale widoczna w przepływach kapitału. Jeszcze kilka lat temu „obronność" była w europejskich rozmowach inwestycyjnych słowem niemal zakazanym; dziś to jeden z najdynamiczniejszych segmentów rynku. Według raportu Dealroom i NATO Innovation Fund europejskie startupy z obszaru obronności, bezpieczeństwa i odporności (DSR) pozyskały w 2025 roku rekordowe 8,7 mld dolarów kapitału wysokiego ryzyka – o 55% więcej rok do roku i niemal czterokrotnie więcej niż pięć lat wcześniej. Dla porównania szeroki europejski rynek VC urósł w tym czasie zaledwie o 16%. Sektor odpowiadał za 43% całego finansowania deep-techu i już za około 13% wszystkich inwestycji venture w Europie – udział ten potroił się w ciągu zaledwie trzech lat. Co istotne, finansowanie późnych faz

(late-stage) wzrosło trzykrotnie, do 4,7 mld dolarów, co świadczy o dojrzewaniu ekosystemu. Niekwestionowanym liderem tematycznym jest sztuczna inteligencja, która stała za 44% całego finansowania DSR – najwyższym udziałem od sześciu lat – napędzając rozwój systemów autonomicznych i obliczeń zoptymalizowanych pod zastosowania obronne.

Motorem tej zmiany stały się nowe instrumenty finansowe łączące kapitał publiczny z prywatnym. Powołany przez państwa Sojuszu fundusz NATO Innovation Fund o kapitalizacji 1 mld euro nie tylko inwestuje bezpośrednio w spółki technologiczne, lecz także zasila fundusze venture działające we wczesnych fazach i na rynkach wschodzących – wysyłając prywatnym inwestorom sygnał, że technologie dual-use to realna i atrakcyjna klasa aktywów. Równolegle Europejski Fundusz Inwestycyjny w ramach instrumentu InvestEU Defence Equity Facility angażuje dziesiątki milionów euro w wyspecjalizowane fundusze deep-techowe, pełniąc rolę inwestora-kotwicy, który „dolewa" kapitał prywatny do projektów o podwyższonym ryzyku. To właśnie ta architektura – państwo jako pierwszy inwestor i gwarant popytu, prywatny kapitał jako akcelerator – wyznacza dziś tempo rozwoju zachodniej zbrojeniówki.

Polska ma w tym wyścigu mocną kartę. Duży prywatny podmiotem krajowego sektora jest Grupa WB, producent bezzałogowców oraz amunicji krążącej, systemów łączności i dowodzenia. To przykład firmy dual-use: ten sam know-how z zakresu autonomii, łączności i przetwarzania danych obsługuje zarówno zastosowania wojskowe, jak i cywilne. Resort obrony zakupy dronów dla nowo utworzonego Inspektoratu Wojsk Dronowych realizuje właśnie u prywatnego producenta.

Coraz wyraźniejszym trendem są też spółki joint venture łączące kapitał prywatny z zagranicznym partnerem technologicznym.

Trzeba jednak zachować trzeźwość. Mimo dynamicznego wzrostu europejskiego finansowania, to Stany Zjednoczone wciąż dominują w globalnych inwestycjach defense-tech, zwłaszcza w późnych fazach i megarundach. Dla Polski oznacza to zarazem wyzwanie i szansę: skoordynowane ścieżki zakupowe, przewidywalny popyt ze strony państwa oraz strategiczne wehikuły inwestycyjne mogą pozwolić przechwycić większą część tego strumienia – szczególnie w obszarach autonomii opartej na AI, systemów antydronowych (counter-UAS), odpornej łączności i bezpiecznych łańcuchów dostaw. Kluczem nie jest wybór między przemysłem państwowym a prywatnym, lecz ich mądre połączenie: stabilność i skala wielkich koncernów oraz tempo i kreatywność prywatnych innowatorów. To w tej synergii – a nie w samych miliardach zapisanych w umowach – kryje się prawdziwa zdolność zbrojeniówki.

4.

Uruchomienie nowego modelu finansowania w ramach programu SAFE już dziś uwidacznia kolejne problemy, z którymi zmagać się będzie krajowy przemysł zbrojeniowy. Z jednej strony pojawiają się zwiększone zamówienia i nowe warunki finansowania produkcji; z drugiej – ograniczony okres dostaw i groźba wysokich kar w bliżej nieokreślonej procedurze odbiorczej wytworzonego sprzętu. Już dziś wiadomo, że będzie to ogromne wyzwanie zarówno dla spółek Grupy PGZ, jak i dla sektora prywatnego, i nie wszyscy wyjdą z tej batalii zwycięsko. Choć szumne zapowiedzi nowych wielkich kontraktów okazały się jedynie aneksową zmianą źródła finansowania, to otoczka nowych warunków wprowadzonych do umów może stać się raczej przekleństwem niż sukcesem zawierających je podmiotów. W połączeniu z mglistymi warunkami udzielenia całej pożyczki SAFE rysuje się dość smutna rzeczywistość, z którą branża i cała Polska zmierzą się w najbliższych latach. Ogromny kredyt obwarowany niejasnymi warunkami może – zdaniem wielu ekspertów i obserwatorów – stać się przysłowiowym gwoździem do trumny polskiego sektora zbrojeniowego. Czy będzie to szansa, czy przekleństwo i efekt politycznych gierek w ramach UE – przekonamy się dość szybko.

Nie to jednak powinno dziś zaprzątać głowy uczestnikom tego procesu. W obecnej sytuacji geopolitycznej wszystkie siły powinny zostać rzucone na odcinek budowy bezpieczeństwa Ojczyzny. Tyle założenia i optymizm – realia pokazują zgoła inny obraz. Wielomiesięczne opóźnienia przy najważniejszych inwestycjach w rozbudowę potencjału produkcyjnego PGZ, niezrozumiałe zmiany lokalizacji rozpoczętych procesów oraz bezmyślna i nieskoordynowana wymiana kadry menedżerskiej mogą zakończyć się jedynie kolejnymi problemami. Liczba niemerytorycznych i oderwanych od realiów decyzji – w połączeniu z propagandowym przypisywaniem cudzych sukcesów obecnym decydentom – świadczy o braku kompleksowego spojrzenia i planu na przyszłość.

Obyśmy obudzili się rano i przekonali, że to wszystko było tylko złym snem – a polska zbrojeniówka rozwijała się wzorcowo, na przekór krytykom i konkurencji.

Bezpieczeństwo finansowe państwa: między stabilnością makroekonomiczną a erozją bazy podatkowej

dr hab. Ireneusz Dąbrowski, prof. SGH

Abstrakt:
Artykuł analizuje bezpieczeństwo finansowe państwa jako fundament jego zdolności do działania. Autor identyfikuje trzy filary: stabilność monetarną, zdolność fiskalną i odporność sektora finansowego. Na przykładzie szarej strefy wyrobów akcyzowych (tytoń, alkohol) pokazuje, jak erozja bazy podatkowej zagraża nie tylko budżetowi, ale i bezpieczeństwu narodowemu – otwierając kanały dla zorganizowanej przestępczości o powiązaniach geopolitycznych. Wskazuje na pilną potrzebę przewidywalnej polityki fiskalnej jako warunku strategicznej podmiotowości państwa.
Słowa kluczowe: bezpieczeństwo finansowe, stabilność makroekonomiczna, szara strefa, akcyza, polityka fiskalna, dochody podatkowe, bezpieczeństwo państwa

Fundamenty bezpieczeństwa finansowego

Bezpieczeństwo państwa jest najczęściej omawiane w języku geopolityki: siły zbrojne, zdolności odstraszania, architektura sojuszy, odporność infrastruktury krytycznej czy pozycja w łańcuchach dostaw. Jest to perspektywa ważna, ale niepełna. U podstaw każdego z tych wymiarów leży bowiem bardziej elementarna kwestia: zdolność państwa do trwałego mobilizowania zasobów. Państwo, które nie potrafi stabilnie finansować swoich podstawowych funkcji, nie jest w stanie długo

utrzymywać zdolności obronnych, prowadzić polityki rozwojowej ani reagować na wstrząsy zewnętrzne. Bezpieczeństwo nie jest wyłącznie kategorią militarną czy strategiczną, lecz przede wszystkim kategorią instytucjonalno-ekonomiczną.

Tak rozumiane bezpieczeństwo finansowe państwa opiera się na trzech filarach. Pierwszym jest stabilność pieniądza, a więc wiarygodność waluty i zdolność banku centralnego do utrzymania ładu nominalnego. Drugim jest zdolność fiskalna państwa, czyli trwała możliwość pozyskiwania dochodów bez niszczenia bazy podatkowej. Trzecim jest odporność systemu finansowego i realnej gospodarki na zjawiska, które tę zdolność osłabiają: inflację, niestabilność regulacyjną, ucieczkę kapitału, wzrost szarej strefy i działalność struktur przestępczych. Relacja między tymi trzema elementami przesądza o realnej sile państwa.

W debacie poświęconej finansom publicznym, stabilności waluty i szarej strefie należy zwrócić uwagę, że kluczowe pytanie nie brzmi: „czy finansować bezpieczeństwo i rozwój?", ale „jak finansować je tak, aby nie podważyć zaufania do całego systemu?": do waluty, długu publicznego, sektora bankowego oraz samych reguł polityki gospodarczej. Utrata tego zaufania może bowiem uruchamiać procesy o charakterze samowzmacniającym: wzrost kosztów długu, wzrost inflacji, spadek bazy podatkowej i ograniczenie zdolności inwestycyjnych państwa. Taki właśnie sens ma teza, że finansowanie strategicznych ambicji państwa musi być podporządkowane stabilności makroekonomicznej.

Rola rządu i banku centralnego w tym układzie jest komplementarna, ale zarazem napięta. Rząd odpowiada za politykę fiskalną: strukturę wydatków, system podatkowy, zadłużenie publiczne oraz redystrybucję. Bank centralny odpowiada za politykę pieniężną: stabilność cen, zakotwiczenie oczekiwań inflacyjnych oraz płynność systemu finansowego. W warunkach dojrzałych instytucji obie polityki wzajemnie się wzmacniają: przewidywalna polityka fiskalna ogranicza presję inflacyjną, a wiarygodna polityka pieniężna obniża koszt finansowania długu. Problem zaczyna się wtedy, gdy cele krótkookresowe dominują nad długookresową spójnością. Jeżeli rząd próbuje szybko zwiększyć dochody bez uwzględnienia reakcji podmiotów gospodarczych, a bank centralny musi kompensować skutki destabilizacji, system przechodzi od równowagi do napięcia.

W ekonomii zjawisko to opisuje się często jako ryzyko dominacji fiskalnej. Oznacza ono sytuację, w której polityka pieniężna przestaje być autonomicznym narzędziem stabilizacji, a zaczyna reagować na presję wynikającą z potrzeb budżetowych. Taka konfiguracja jest szczególnie niebezpieczna dla państw, które chcą jednocześnie finansować wysokie potrzeby obronne i rozwojowe. W tych okolicznościach utrata

wiarygodności waluty lub długu publicznego nie jest już jedynie problemem księgowym, lecz realnym ograniczeniem strategicznej sprawczości. Wzrost rentowności długu, osłabienie kursu walutowego czy trwałe podwyższenie oczekiwań inflacyjnych oznaczają mniej środków na cele rozwojowe i mniejszą zdolność reagowania w sytuacji kryzysowej.

Własna waluta ma tu znaczenie zasadnicze. Jest ona nie tylko technicznym środkiem płatniczym, lecz instytucjonalnym nośnikiem zaufania. Państwo emitujące wiarygodny pieniądz dysponuje większą swobodą antycykliczną, może elastyczniej reagować na wstrząsy i jest mniej podatne na zewnętrzny szantaż finansowy. Taka przewaga znika jednak wtedy, gdy stabilność waluty zostaje podważona. Waluta traci wówczas funkcję bezpiecznego punktu odniesienia dla kalkulacji gospodarczej, a jej osłabienie przenosi się na ceny importu, oczekiwania inflacyjne, koszty finansowania i skłonność do ucieczki w aktywa poza systemem oficjalnym. Z punktu widzenia bezpieczeństwa państwa nie chodzi więc wyłącznie o „posiadanie własnej waluty", ale o utrzymanie jej wiarygodności.

Podobnie należy patrzeć na dług publiczny. Sam poziom zadłużenia nie przesądza jeszcze o kryzysie. O bezpieczeństwie nie decyduje bowiem dług nominalny, lecz relacja między zadłużeniem, tempem wzrostu, kosztem finansowania i zaufaniem inwestorów. Państwo o wysokiej wiarygodności może finansować znaczne potrzeby rozwojowe bez gwałtownego wzrostu ryzyka. Jednak gdy zaufanie słabnie, nawet umiarkowane zadłużenie może stać się źródłem destabilizacji, ponieważ rosną koszty rolowania długu i zawęża się przestrzeń fiskalna. W efekcie polityka publiczna staje się zakładnikiem własnych wcześniejszych decyzji, a budżet coraz większą część zasobów przeznacza nie na rozwój, lecz na obsługę niepewności.

Nie można przy tym abstrahować od sektora bankowego. To on jest kanałem transmisji polityki pieniężnej, podstawowym pośrednikiem w finansowaniu gospodarki oraz kluczowym filarem bezpieczeństwa płynnościowego. Jeżeli rośnie niepewność dotycząca waluty, inflacji lub zdolności państwa do kontrolowania procesów fiskalnych, sektor bankowy działa w warunkach większego ryzyka. Przekłada się to na warunki kredytowania, skłonność do inwestowania i wycenę aktywów. Stabilność sektora bankowego nie jest osobnym zagadnieniem, lecz elementem szerszej całości: bezpieczne państwo to państwo, którego pieniądz, finanse publiczne i kanały finansowania realnej gospodarki tworzą spójny system.

Należy także odnotować rolę gotówki i pieniądza cyfrowego. Gotówka pełni funkcję nie tylko transakcyjną, ale także ustrojową i bezpieczeństwa: jest awaryjnym

nośnikiem płynności w sytuacjach kryzysowych, ogranicza uzależnienie obywateli od infrastruktury cyfrowej i zapewnia minimalny poziom autonomii wobec zakłóceń systemowych. Rozwój pieniądza cyfrowego oraz dalsza cyfryzacja płatności zwiększają przejrzystość obrotu i ułatwiają ograniczanie części nadużyć, ale jednocześnie wzmacniają znaczenie zaufania do instytucji. Im bardziej system staje się ucyfrowiony tym bardziej destabilizujące mogą być zakłócenia formalne, regulacyjne lub technologiczne. Bezpieczeństwo finansowe wymaga nie likwidacji gotówki, lecz racjonalnej równowagi między efektywnością cyfrową a odpornością systemową.

Na tym tle inflacja jawi się jako zjawisko szczególnie niebezpieczne. Nie jest ona wyłącznie „wzrostem cen", lecz procesem destabilizacji ładu nominalnego całej gospodarki. Inflacja działa jak ukryty podatek, ponieważ obniża realną siłę nabywczą dochodów i oszczędności, ale jej skutki sięgają dalej. Podważa ona wiarygodność kontraktów, utrudnia kalkulację inwestycyjną, skraca horyzont decyzyjny przedsiębiorstw i gospodarstw domowych oraz wzmacnia bodźce do zachowań defensywnych. W gospodarce o utrwalonej inflacji podmioty coraz mniej energii przeznaczają na produktywność, a coraz więcej na zabezpieczanie się przed ryzykiem nominalnym.

Z perspektywy teorii ekonomii inflacja zaburza funkcję informacyjną cen. Ceny przestają przekazywać jednoznaczne sygnały o relatywnej rzadkości dóbr, ponieważ coraz większa część zmian cen wynika nie z procesów realnych, lecz z niestabilności nominalnej. To obniża jakość alokacji zasobów, a więc w długim okresie uderza w tempo wzrostu gospodarczego. W konsekwencji państwo traci część podstaw własnej siły: niższy wzrost to niższe dochody podatkowe, niższa inwestycja prywatna i wyższe napięcia społeczne. Stabilność cen nie jest technicznym parametrem polityki banku centralnego, lecz jednym z warunków bezpieczeństwa narodowego.

Erozja bazy podatkowej

Jeżeli inflacja jest jednym z mechanizmów erozji zaufania, to jej fiskalnym odpowiednikiem jest erozja bazy podatkowej. To proces, w którym formalna zdolność państwa do nakładania podatków nie przekłada się na realną zdolność poboru dochodów, ponieważ część aktywności gospodarczej przechodzi do strefy nieformalnej lub nielegalnej. W państwie o słabych bodźcach instytucjonalnych wzrost stawek nie musi zwiększać wpływów, a może wręcz uruchamiać ucieczkę od legalnego obrotu, zmianę struktury konsumpcji, spadek rejestrowanej sprzedaży oraz rozwój przemytu

i podróbek. Taka właśnie logika leży u podstaw zjawiska, które można określić jako „ucieczkę dochodów z budżetu do szarej strefy".

To zjawisko bywa upraszczane do ilustracji krzywej Laffera, ale w praktyce ma ono znacznie bardziej złożony charakter. Nie chodzi wyłącznie o poziom samej stawki podatkowej. Równie ważne są: przewidywalność zmian, czas ich wprowadzania, struktura rynku, skala substytucji między legalnym i nielegalnym kanałem dostaw, siła egzekucji państwa oraz percepcja społecznej legitymizacji podatku. Jeżeli system podatkowy jest przewidywalny, konsultowany i stopniowy, przedsiębiorcy oraz konsumenci mogą dostosowywać się bez gwałtownego wyjścia poza legalny obieg. Jeżeli natomiast jest skokowy, nieprzewidywalny i oderwany od realiów rynku, wówczas uruchamia mechanizmy obronne, których efektem staje się kurczenie bazy podatkowej.

Dane pokazują, że problem ten ma w Polsce wymiar strukturalny. Według szacunków IPAG wartość szarej strefy w Polsce w 2025 r. odpowiadała 18,1 proc. PKB, czyli około 780 mld zł. Dla porównania średnia unijna miała wynosić około 11,8 proc. PKB. Oznacza to, że skala aktywności gospodarczej pozostającej poza pełną kontrolą państwa jest nie tylko znaczna, ale i znacznie wyższa niż w wielu krajach porównywalnych. To nie jest wyłącznie problem fiskalny, ale także informacja o jakości instytucji, skuteczności egzekucji i sile bodźców wypychających część rynku poza oficjalny obieg.

Szczególnie wyraźnie widać to w sektorach objętych wysoką akcyzą, gdzie cena legalnego produktu zawiera już bardzo duży komponent fiskalny. W takich warunkach niewielka nawet zmiana relacji cenowych może wygenerować silny bodziec do przechodzenia do kanałów nielegalnych. Dotyczy to zwłaszcza rynku wyrobów tytoniowych i alkoholu, czyli obszarów, w których występuje wysoka elastyczność względem różnic cenowych, a zarazem rozbudowane sieci przemytu i fałszerstw. Nadmierne i skokowe podwyżki akcyzy nie zwiększają dochodów budżetowych, lecz przesuwają konsumpcję poza legalny rynek, kurcząc bazę podatkową.

Na tym tle polityka akcyzowa ostatnich lat stanowi bardzo dobry przykład mechanizmu, w którym prawidłowość ekonomiczna i diagnoza bezpieczeństwa nakładają się na siebie. W latach 2022–2024 funkcjonowała przewidywalna ścieżka podwyżek podatków akcyzowych, określana jako mapa akcyzowa. Rozwiązanie to zostało wypracowane w formule dialogu pomiędzy administracją, branżą, plantatorami i przedsiębiorcami. Miało ono dwa cele: po pierwsze zapewnić stabilny wzrost wpływów budżetowych, po drugie nie doprowadzić do takiego wzrostu cen legalnych produktów, który wypchnąłby konsumentów do szarej strefy. Mapa ta przyniosła

realne efekty: wpływy budżetowe z akcyzy zaczęły rosnąć w tempie 10–13 proc. rocznie, a skala szarej strefy na rynku tytoniowym malała.

To właśnie ten okres można traktować jako model względnie racjonalnej polityki fiskalnej w obszarze akcyzy. W latach 2022–2024 wpływy z akcyzy tytoniowej były wyższe niż zakładała ocena skutków regulacji, a raport IPAG z 2024 r. odnotowywał „odwrotną tendencję na rynku tytoniowym": wzrost wpływów budżetowych przy malejącej szarej strefie, która osiągnęła historycznie niski poziom około 4,7 proc. W sensie ekonomicznym oznaczało to, że państwo zwiększało dochody nie poprzez fiskalny szok, lecz poprzez przewidywalne dostosowanie rynku, które utrzymywało legalny obrót. W sensie instytucjonalnym było to potwierdzenie tezy, że trwałe dochody budżetowe wymagają stabilności reguł.

Załamanie tego modelu nastąpiło wraz z rewizją mapy akcyzowej w 2024 r. Wprowadzono wtedy wyraźnie wyższe podwyżki akcyzy: na papierosy o 25 proc. zamiast planowanych 10 proc., na tytoń do palenia o 38 proc., a na wyroby nowatorskie jeszcze wyższe. W 2025 r. skutki tej zmiany stały się już wyraźnie widoczne: nastąpił spadek legalnej sprzedaży papierosów o 13 proc., tytoniu do palenia o 15 proc. i wyrobów nowatorskich o 6 proc., przy jednoczesnym wzroście udziału szarej strefy z 4,7 proc. do 7,5 proc. To skok o 59 proc. w relacji do wcześniejszego poziomu. Mechanizm zadziałał więc zgodnie z ekonomiczną intuicją: formalny wzrost stawki nie przełożył się na proporcjonalny wzrost dochodów, ale na wyjście części popytu poza legalny obieg.

Skutki tej zmiany dają się uchwycić nie tylko przez wskaźniki udziału szarej strefy, ale także przez jej wartość nominalną. Szara strefa tytoniowa wzrosła z 2,1 mld zł w 2023 r. do 2,4 mld zł w 2024 r. i 3,3 mld zł w 2025 r. Jednocześnie sam ubytek dochodów budżetowych z tego tytułu w 2025 r. wyniósł niemal 2,8 mld zł. Dane te pokazują, że nie chodzi wyłącznie o abstrakcyjny „procent rynku", lecz o konkretny transfer środków z legalnego kanału podatkowego do obiegu nieoficjalnego. Część pieniędzy, które mogły zasilać budżet państwa, przeszła do podmiotów działających poza systemem.

Potwierdzeniem rozminięcia się prognoz z rzeczywistością są również dane o wykonaniu budżetu. Rząd zakładał w ustawie budżetowej wpływy z akcyzy w 2025 r. na poziomie 95,8 mld zł, podczas gdy rzeczywiste wpływy miały wynieść ok. 90,54 mld zł, a więc o ponad 5,3 mld zł mniej. Największa rozbieżność dotyczyła właśnie wyrobów tytoniowych: zamiast prognozowanych 37,14 mld zł budżet uzyskał ok. 33,61 mld zł, czyli o 3,53 mld zł mniej. Była to pierwsza od lat tak duża rozbieżność

pomiędzy prognozą a wykonaniem w tym obszarze, a wcześniejsze lata raczej przynosiły wpływy wyższe od założeń.

Z ekonomicznego punktu widzenia jest to sytuacja modelowa. Państwo podniosło stawki, oczekując większych wpływów, ale nie uwzględniło w pełni reakcji rynku: spadku legalnej sprzedaży, wzrostu skłonności do zakupów w szarej strefie, wzrostu skali podróbek i przemytu oraz zmiany struktury konsumpcji. Proces fiskalny nie powinien być analizowany wyłącznie po stronie stawek, lecz po stronie iloczynu stawki i legalnej podstawy opodatkowania. Gdy drugi element maleje szybciej niż rośnie pierwszy, dochody netto spadają.

Podobne zjawisko dostrzeżono również w branży spirytusowej. W latach 2023–2025 budżet państwa mógł stracić około 4,4 mld zł z tytułu nielegalnego obrotu alkoholem, z czego najwyższa strata – 1,8 mld zł – miała przypadać na 2025 r. Jednocześnie wpływy z akcyzy na alkohol etylowy w 2024 r. nie wykazały istotnego wzrostu mimo wcześniejszych podwyżek, co sugeruje podobną logikę erozji podstawy opodatkowania. Także tutaj budżet nie uzyskuje automatycznie większych dochodów tylko dlatego, że nominalna stawka rośnie.

Mechanizm ten ma wymiar historyczny. W latach 2011–2014, gdy po drastycznych podwyżkach akcyzy szara strefa tytoniowa w Polsce miała osiągnąć blisko 20 proc. rynku jej ograniczenie zajęło ponad dekadę. Obecne załamanie trendu nie jest anomalią, lecz powrotem do znanego z przeszłości schematu: fiskalny szok wywołuje wzrost nielegalnego obrotu, a jego późniejsze ograniczanie wymaga wielu lat kosztownego uszczelniania. Oznacza to, że błędna polityka może pozostawiać długotrwałe konsekwencje, które dalece wykraczają poza rok budżetowy, w którym popełniono błąd.

Konsekwencje dla bezpieczeństwa państwa i wnioski

Najważniejszą konsekwencją opisanych procesów jest to, że problem szarej strefy nie kończy się na fiskusie. Utrata dochodów budżetowych to tylko pierwszy poziom skutków. Drugi poziom to zmiana struktury realnych przepływów finansowych w gospodarce. Kiedy legalny rynek kurczy się, a część obrotu przenosi się do kanałów nieformalnych, państwo traci nie tylko pieniądze, ale też informację, kontrolę i możliwość egzekwowania standardów. W rezultacie obok oficjalnej gospodarki rozwija się równoległy system wymiany: mniej przejrzysty, mniej opodatkowany i trudniejszy

do monitorowania. To już nie jest wyłącznie kwestia poziomu wpływów, lecz kwestia jakości państwowości.

Nielegalny rynek wyrobów akcyzowych jest udokumentowanym obszarem działalności zorganizowanych grup przestępczych, powiązanym z praniem pieniędzy i finansowaniem podmiotów zewnętrznych. Istnieją działania międzynarodowych grup przemytniczych rozbijanych przez organy ścigania, a także produkcja dziesiątek milionów nielegalnych papierosów z uszczupleniami publicznoprawnymi rzędu dziesiątek milionów złotych. Nie chodzi więc o rozproszoną „drobnicę bazarową", ale o profesjonalne struktury uzyskujące zyski z systemowego obchodzenia państwa. To stawia problem szarej strefy w jednym szeregu z innymi zagrożeniami dla bezpieczeństwa wewnętrznego.

Istnieje także wymiar geopolityczny. Ważnym źródłem nieopodatkowanego towaru na polskim rynku pozostaje Białoruś, a każda złotówka nieodprowadzonej akcyzy może pośrednio zasilać struktury działające poza polskim systemem prawno-fiskalnym. Część nielegalnego towaru pochodzi z obszarów powiązanych z państwami prowadzącymi politykę destabilizacyjną wobec regionu. Ostatecznie problem szarej strefy nie jest już wyłącznie problemem budżetu i ochrony zdrowia, lecz staje się zagadnieniem bezpieczeństwa państwa. Pieniądz, który nie trafia do polskiego budżetu, może wzmacniać podmioty sprzeczne z polską racją stanu.

Realny koszt utraconych dochodów jest znacznie większy niż sama wartość luki fiskalnej. Każdy miliard złotych niewpłacony do budżetu oznacza mniej środków na finansowanie infrastruktury, energetyki, obronności, ochrony granic, cyfryzacji administracji czy modernizacji usług publicznych. Szara strefa to nie abstrakcyjna statystyka, ale konkretne megawaty niewybudowanych farm wiatrowych, kilometry niezmodernizowanej sieci energetycznej, nieuruchomione programy wsparcia. Koszt szarej strefy trzeba mierzyć nie tylko w utraconych wpływach, lecz także w utraconej zdolności państwa do inwestowania w własne bezpieczeństwo.

Szczególnego znaczenia nabiera problem przewidywalności polityki publicznej. W nowoczesnej gospodarce nie wystarcza już formalna zdolność państwa do stanowienia prawa. Równie ważna jest jakość bodźców, jakie to prawo tworzy. Stabilne, transparentne i konsultowane reguły podatkowe zwiększają skłonność do działania w legalnym obiegu, ponieważ ograniczają niepewność i pozwalają planować działalność gospodarczą. Reguły gwałtowne, skokowe i niestabilne wywołują natomiast reakcje obronne: ograniczają zaufanie, zachęcają do unikania opodatkowania i obniżają skuteczność samego państwa. Przykład akcyzy pokazuje, że przewidywalność nie jest luksusem administracyjnym, lecz warunkiem bezpieczeństwa fiskalnego.

Z tego powodu polityka gospodarcza państwa aspirującego do strategicznej podmiotowości musi opierać się na kilku zasadach. Po pierwsze, wydatki rozwojowe i na bezpieczeństwo powinny być planowane w zgodzie z długookresową stabilnością pieniądza i długu. Po drugie, polityka podatkowa, zwłaszcza w sektorach wrażliwych na przemyt i nielegalny obrót, musi uwzględniać reakcje podaży i popytu, a nie tylko arytmetykę stawek. Po trzecie, uszczelnianie systemu nie powinno polegać na szoku fiskalnym, lecz na połączeniu przewidywalności regulacyjnej, skutecznej egzekucji i wysokiej jakości danych. Po czwarte, szara strefa musi być traktowana nie jako margines życia gospodarczego, lecz jako zjawisko strategiczne, które osłabia finanse publiczne, wzmacnia zorganizowaną przestępczość i ogranicza suwerenność ekonomiczną.

W takim sensie bezpieczeństwo finansowe państwa można zdefiniować jako zdolność do prowadzenia ambitnej polityki rozwojowej i bezpieczeństwa bez naruszania wiarygodności waluty, długu i bazy podatkowej. Jest to definicja wymagająca, ponieważ zakłada jednoczesne utrzymanie trzech rodzajów równowagi: nominalnej, fiskalnej i instytucjonalnej. Państwo nie przegrywa wtedy, gdy wydaje dużo na bezpieczeństwo. Przegrywa wtedy, gdy wydaje tak, że podważa podstawy własnej zdolności finansowania. Jeśli wzrost wydatków prowadzi do destabilizacji pieniądza lub erozji legalnego rynku, bezpieczeństwo staje się pozorne, ponieważ osłabia własne źródła finansowania.

Stabilna waluta, wiarygodny bank centralny, przewidywalna polityka fiskalna, odporny sektor bankowy, utrzymanie roli gotówki jako bufora bezpieczeństwa i zdecydowane ograniczanie szarej strefy nie są odrębnymi agendami. To elementy jednego systemu bezpieczeństwa państwa. Naruszenie któregokolwiek z tych elementów uruchamia mechanizmy sprzężeń zwrotnych: wyższa inflacja osłabia zaufanie, niższe zaufanie zwiększa koszt długu, wyższy koszt długu zachęca do fiskalnych skrótów, a fiskalne skróty mogą przyspieszać ucieczkę dochodów do szarej strefy. Granica między polityką gospodarczą a bezpieczeństwem narodowym jest znacznie bardziej płynna, niż zwykle się zakłada.

Państwo nowoczesne musi więc myśleć o bezpieczeństwie nie tylko w kategoriach wojska i dyplomacji, ale także w kategoriach jakości własnych instytucji monetarnych i fiskalnych. To tam rozstrzyga się, czy będzie ono zdolne finansować swój rozwój, obronność i odporność. W świecie rosnącej niepewności strategicznej nie wystarczy mieć ambitne cele. Trzeba jeszcze mieć zdolność, by finansować je w sposób, który nie wzmacnia przeciwników państwa, nie osłabia jego waluty i nie wypycha legalnej gospodarki poza system. Dopiero wtedy bezpieczeństwo finansowe staje się rzeczywistym fundamentem bezpieczeństwa państwa.

Odporne państwo – strategiczne wyzwania dla bezpieczeństwa Polski

Zbigniew Hoffmann

Abstrakt

Artykuł analizuje koncepcję odporności państwa jako fundament polskiego bezpieczeństwa narodowego. Autor wyróżnia trzy główne komponenty odporności – instytucjonalną, społeczną i infrastrukturalną, wskazując na Krajowy System Ratowniczo-Gaśniczy jako element integrujący cały system. Na przykładzie powodzi z 2024 roku diagnozuje słabości: rozproszenie kompetencji, opóźnione reagowanie i brak jednolitych podstaw prawnych zarządzania kryzysowego. Formułuje rekomendacje dotyczące centralizacji koordynacji kryzysowej na szczeblu rządowym, reformy edukacji obywatelskiej w zakresie bezpieczeństwa oraz dalszego rozwoju infrastruktury strategicznej.

Słowa kluczowe: odporność państwa, zarządzanie kryzysowe, ochrona ludności, KSRG, infrastruktura krytyczna, bezpieczeństwo narodowe, powódź, edukacja dla bezpieczeństwa

Poczucie bezpieczeństwa Polaków jako ważny element skutecznego budowania odporności państwa

Budowanie poczucia bezpieczeństwa Polaków stanowi społeczny fundament wzmacniania odporności państwa na zagrożenia. Obywatele, którzy ufają instytucjom publicznym i mają poczucie stabilności, są skłonni do angażowania się w działania na rzecz wspólnego bezpieczeństwa.

Według badań Centrum Badania Opinii Społecznej (CBOS) przeprowadzonych w 2023 roku, 88% Polaków deklarowało, że czuje się bezpiecznie, żyjąc w Polsce.

Poczucie bezpieczeństwa w latach 2015–2023 systematycznie wzrastało. Niewielkie zachwianie tego trendu nastąpiło w latach 2020–2022, było to związane z wybuchem pandemii COVID-19, a następnie zbrojną napaścią Rosji na Ukrainę. Mimo tych wydarzeń od 2022 roku poczucie bezpieczeństwa ponownie zaczęło rosnąć.

Niestety obecnie analiza wyników badań wskazuje na spadek poczucia bezpieczeństwa wśród Polaków. Trudno jednak jednoznacznie stwierdzić jak szybko ta tendencja będzie się pogłębiać. Dlatego konieczne jest podejmowanie działań odbudowujących zaufanie społeczne do państwa oraz zwiększających poczucie bezpieczeństwa obywateli wobec współczesnych zagrożeń co w ujęciu ogólnym prowadzi do wzmacniania odporności państwa.

Należy podkreślić, że odporność państwa jest nierozerwalnie związana z dobrze funkcjonującym społeczeństwem, charakteryzującym się wysokim współczynnikiem zaufania do instytucji publicznych.

To właśnie zdolność państwa i społeczeństwa do przeciwstawiania się zagrożeniom, ograniczania ich skutków oraz szybkiego powrotu do normalnego funkcjonowania po wystąpieniu sytuacji kryzysowej stanowi ramy definicji, w których poruszamy się przywołując zagadnienie odporności państwa.

Potrzebne jest zatem dobrze wyposażone państwo w narzędzia zapewniające ochronę obywatelom, ale także stwarzające warunki, aby obywatele w ramach wspólnoty mogli się organizować i skutecznie współtworzyć odporność państwa.

Komponenty odporności państwa

Wzmacnianie odporności wymaga identyfikacji zagrożeń, przeprowadzenia oceny ryzyka i przygotowania odpowiednich procedur reagowania. Bardzo ważne jest również podtrzymywanie ciągłości doskonalenia zdolności instytucji państwowych i społeczeństwa.

Dlatego można wyróżnić trzy główne komponenty, na których opiera się odporność państwa: odporność instytucjonalną, odporność społeczną oraz odporność infrastrukturalną.

- Odporność instytucjonalna, czyli sprawne funkcjonowanie administracji publicznej w tym systemów zarządzania kryzysowego. Dzięki wysokiej odporności instytucjonalnej możliwe jest szybkie podejmowanie decyzji, efektywne wykorzystanie zasobów oraz ograniczanie skutków kryzysów.

- Odporność społeczna to przygotowanie obywateli do właściwego reagowania na różnego rodzaju zagrożenia. Dzięki niej społeczeństwo potrafi skuteczniej radzić sobie w sytuacjach kryzysowych: naturalnych, technologicznych/środowiskowych, społeczno-politycznych oraz osobistych.
- Odporność infrastrukturalna, czyli zdolność ochrony infrastruktury krytycznej w sytuacjach zagrożeń. Obejmuje między innymi systemy energetyczne, telekomunikacyjne, transportowe, wodociągowe czy ochrony zdrowia, które są niezbędne do funkcjonowania państwa i społeczeństwa.

Należy również wspomnieć, że jednym z najważniejszych elementów odporności państwa jest system ochrony ludności, który jest elementem łączącym wszystkie komponenty. W Polsce kluczową rolę odgrywa Krajowy System Ratowniczo-Gaśniczy (KSRG), który obejmuje swoim działaniem całe państwo. Do zadań KSRG należy między innymi: walka z pożarami, usuwanie skutków klęsk żywiołowych, ratownictwo techniczne, chemiczne, ekologiczne oraz medyczne.

Trzonem systemu jest Państwowa Straż Pożarna, a jego działanie wspierają Państwowe Ratownictwo Medyczne oraz jednostki Ochotniczych Straży Pożarnych. Dzięki rozbudowanej sieci jednostek możliwe jest szybkie reagowanie na zagrożenia i koordynowanie działań ratowniczych na poziomie lokalnym i krajowym.

Czy system odporności państwa pozbawiony jest słabości?

Pomimo wielu osiągnięć system odporności państwa nie jest pozbawiony słabości. Niewydolność systemu odporności państwa można było zaobserwować podczas np. powodzi w 2024 roku. Konsekwencje braku wdrożenia odpowiednich działań ze strony administracji rządowej i samorządowej ponoszą mieszkańcy terenów popowodziowych do dzisiaj.

Zdarzenie ujawniło problemy z koordynacją działań oraz przepływem informacji. W wielu regionach reakcja była spóźniona, a ostrzeżenia nie docierały na czas do mieszkańców. Wpłynęło to na ograniczenie skuteczności ewakuacji czy zabezpieczania mienia. Powódź uwidoczniła również potrzebę lepszego planowania przestrzennego i inwestycji w zabezpieczenia przeciwpowodziowe. Brak odpowiednich

rozwiązań technicznych zwiększył skalę strat i wydłużył proces powrotu do normalnego funkcjonowania.

Podczas powodzi w 2024 roku system odporności państwa zawiódł w kluczowych obszarach.

Luki w systemie odporności.

Problemem wciąż pozostaje rozproszenie kompetencji pomiędzy różnymi instytucjami odpowiedzialnymi za bezpieczeństwo oraz brak jednolitych podstaw prawnych regulujących zagadnienie odporności państwa.

Wciąż niewystarczający jest także poziom przygotowania społeczeństwa do reagowania na sytuacje kryzysowe. Wiedza dotycząca pierwszej pomocy, zasad postępowania podczas sytuacji kryzysowych, nadzwyczajnych, czy zagrożeń hybrydowych nadal nie jest powszechna.

Ważnym wyzwaniem pozostaje także dalsze wzmacnianie odporności infrastruktury krytycznej. Coraz częstsze awarie techniczne, powodzie, susze, huragany czy cyberzagrożenia pokazują, że bezpieczeństwo kluczowych systemów państwa wymaga stałego doskonalenia.

Wzmacnianie społecznej odporności poprzez edukację, skuteczną komunikację i rozwój zdolności reagowania kryzysowego zwiększa możliwości państwa do radzenia sobie z sytuacjami nadzwyczajnymi.

Rekomendacje

W warunkach państwa polskiego skuteczne zarządzanie systemem odporności państwa wymaga silnej koordynacji na poziomie centralnym oraz zachowania decydującej roli administracji rządowej nad działaniami podejmowanymi przez jednostki samorządu terytorialnego. Współczesne zagrożenia, takie jak konflikty zbrojne, cyberataki, dezinformacja, kryzysy energetyczne czy klęski żywiołowe, mają charakter ponadregionalny i często wykraczają poza możliwości reagowania pojedynczych jednostek samorządu terytorialnego. Z tego względu niezbędne jest zapewnienie jednolitego systemu planowania, podejmowania decyzji oraz koordynacji działań na szczeblu krajowym.

Centralizacja w obszarze bezpieczeństwa pozwala na efektywne wykorzystanie zasobów państwa, uniknięcie rozproszenia kompetencji oraz ograniczenie ryzyka występowania niespójnych działań pomiędzy poszczególnymi regionami. W sytuacjach kryzysowych kluczowe znaczenie ma szybkość podejmowania decyzji i możliwość ich natychmiastowego wdrażania na terenie całego kraju.

Silna pozycja administracji rządowej umożliwia stworzenie jednolitych standardów ochrony ludności, zarządzania kryzysowego oraz ochrony infrastruktury krytycznej.

Rola samorządów pozostaje istotnym elementem systemu bezpieczeństwa ze względu na znajomość lokalnych uwarunkowań i bezpośredni kontakt z mieszkańcami. Działania samorządów powinny być jednak realizowane w ramach spójnej strategii państwowej i podlegać koordynacji ze strony administracji rządowej.

Doświadczenie w zakresie sytuacji kryzysowych, z którymi mierzyło się polskie państwo w ostatnich latach, a także realia geopolityczne, w których żyjemy pokazują, że budowanie silnego systemu bezpieczeństwa w oparciu o administrację rządową pozwoli na skuteczne budowanie odporności państwa.

Doświadczenia te pokazały, że rozproszenie kompetencji i brak jednolitego kierownictwa mogą prowadzić do opóźnień w podejmowaniu decyzji oraz utrudniać efektywne wykorzystanie dostępnych środków.

Silne państwo powinno dysponować zdolnością do szybkiego przejmowania inicjatywy i koordynowania działań wszystkich podmiotów odpowiedzialnych za bezpieczeństwo. Wnioski płynące z ostatnich doświadczeń wskazują, że brak silnego centrum decyzyjnego zmniejsza skuteczność reagowania w obliczu sytuacji kryzysowych.

Kolejnym istotnym elementem budowania odporności państwa są również zmiany w systemie oświaty i edukacji, których celem powinno być zwiększanie świadomości obywateli w zakresie bezpieczeństwa, zarządzania kryzysowego oraz odpowiedzialności społecznej. Odporne państwo wymaga nie tylko sprawnych instytucji, ale także odpowiednio przygotowanego społeczeństwa, zdolnego do przeciwdziałania dezinformacji oraz do racjonalnego reagowania na sytuacje kryzysowe.

Edukacja powinna obejmować zagadnienia związane z ochroną ludności, pierwszą pomocą, bezpieczeństwem cyfrowym oraz funkcjonowaniem państwa w warunkach zagrożenia.

Następnym istotnym elementem wzmacniania odporności państwa jest rozwój infrastruktury strategicznej, obejmującej sieci transportowe, energetyczne, telekomunikacyjne oraz infrastrukturę służącą bezpieczeństwu i ochronie ludności.

W okresie rządów Prawa i Sprawiedliwości podejmowaliśmy szereg działań mających na celu zwiększenie odporności państwa, w szczególności w obszarze infrastruktury krytycznej. Dotyczyło to między innymi sektora energetycznego, transportowego, a także teleinformatycznego, które odgrywają kluczową rolę w zapewnieniu ciągłości funkcjonowania państwa w sytuacjach kryzysowych.

Kontynuacja tego rodzaju działań będzie stanowić ważny element budowania długoterminowej odporności państwa na zagrożenia.

Automatyzacja produkcji amunicji z wykorzystaniem systemów opartych o sztuczną inteligencję

dr inż. Przemysław Kowalczuk

Abstrakt

Artykuł omawia automatyzację produkcji amunicji wielkokalibrowej w ujęciu Industry 4.0, z naciskiem na projektowanie nowej generacji linii produkcyjnych, integrację danych procesowych oraz zastosowanie AI w utrzymaniu wysokiej dostępności technicznej. Punktem odniesienia jest referencyjna liniowo-gniazdowa infrastruktura do produkcji pocisków artyleryjskich kalibru 155mm. Referencyjny proces produkcyjny obejmuje przepływ materiału poprzez magazyn ogólny, skanowanie laserowe, stację elaboracji pocisku, kontrolę X-Ray, linię malarską i magazyn produktów gotowych. Główna teza artykułu brzmi: największą wartością biznesową AI w takim środowisku nie jest autonomiczne sterowanie procesem technologicznym, lecz ***predictive*** i ***preventive maintenance*** – ograniczanie nieplanowanych postoi, stabilizacja OEE oraz ochrona kosztu jednostkowego przy wysokich wolumenach produkcji.

Słowa kluczowe: automatyzacja, amunicja wielkokalibrowa, AI, Industry 4.0, OEE (Overall Equipment Effectiveness), MTBF, MTTR, preventive maintenance, predictive maintenance, KUKA, X-Ray, MES, ERP, SCADA

Wprowadzenie

Produkcja amunicji należy do obszarów, w których presja na wolumen spotyka się z bardzo wysokimi wymaganiami jakości, bezpieczeństwa i powtarzalności. Ostatnie

programy publiczne i branżowe, w tym europejska inicjatywa ASAP, działania NATO oraz analizy dotyczące odbudowy zdolności przemysłowych, pokazują, że problemem nie jest wyłącznie dostępność pojedynczych maszyn. Kluczowe staje się zaprojektowanie stabilnego systemu produkcyjnego zdolnego do pracy w wysokim obciążeniu, z kontrolą jakości typu „inline" i z pełną identyfikowalnością produktu.

Największą wartość biznesową sztucznej inteligencji w nowoczesnej produkcji amunicji stanowi nie autonomiczne sterowanie procesem technologicznym, lecz zapewnienie wysokiej dostępności linii produkcyjnej poprzez wdrożenie technik predictive i preventive maintenance. W praktyce oznacza to wcześniejsze wykrywanie zużycia robotów, napędów transportu, skanerów, urządzeń X-Ray, układów wentylacji i suszenia oraz innych elementów infrastruktury, zanim ich degradacja zamieni się w przestój linii.

Automatyzacja nie oznacza więc wyłącznie zastąpienia operatora robotem. Jest systemem obejmującym robotyzację, transport wewnętrzny, kontrolę inline, NDT (Non-Destructive Testing), traceability, integrację MES (Manufacturing Execution System), ERP (Enterprise Resource Planning), SCADA (Supervisory Control and Data Acquisition), CMMS (Computerized Maintenance Management System) oraz cyberbezpieczeństwo. AI powinna wzmacniać ten system przede wszystkim przez analizę danych, przewidywanie awarii i stabilizację dostępności technicznej.

Po co automatyzować produkcję amunicji

Bezpieczeństwo i redukcja ekspozycji operatora

Pierwszym uzasadnieniem automatyzacji jest bezpieczeństwo. W procesach związanych z amunicją część operacji posiada podwyższone ryzyko dla operatora. Technologie ograniczające ręczną manipulację, ekspozycję człowieka i pracę w warunkach obciążających ergonomicznie mają wartość większą niż sama oszczędność roboczogodzin. Roboty, linie transportowe i skanowanie automatyczne powinny być rozpatrywane jako element architektury bezpieczeństwa procesu.

Jakość, powtarzalność i traceability

Drugim uzasadnieniem jest jakość. W produkcji wielkoseryjnej niewielka zmienność wejściowa może szybko przełożyć się na koszt braków, przeróbek, blokad partii

i dodatkowych kontroli. Szczególnie wartościowe są technologie umożliwiające kontrolę w toku produkcji: skanowanie geometryczne, laserowe potwierdzenie pozycji, X-Ray/CT, rejestr parametrów operacji i cyfrowy paszport produktu. Koszt badań poligonowych każdej z wyprodukowanej serii pocisków to co najmniej kilka milionów złotych. Eliminacja choćby jednego nadmiarowego badania w obrębie danego kontraktu to realna oszczędność dla przedsiębiorstwa.

Przepustowość i odporność operacyjna

Trzecim uzasadnieniem jest przepustowość. Automatyzacja staje się ekonomicznie atrakcyjna, gdy popyt jest stabilny, linia pracuje wielozmianowo, mix wyrobów jest ograniczony, a koszt przestoju lub braku jakości jest wysoki. Przy krótkich seriach bardziej racjonalna może być automatyzacja modułowa; przy wysokich wolumenach uzasadnienie przesuwa się w stronę zintegrowanej linii, kontroli inline, preventive maintenance i digital twin.

Efekt skali a automatyzacja

Skalę zagadnienia najlepiej odzwierciedlają roczne wolumeny produkcji przypisywane w analizach poszczególnym producentom i programom amunicji wielkokalibrowej. Wartości przedstawione poniżej zostały wykorzystane jako dane referencyjne do oceny potencjału automatyzacji procesów produkcyjnych. Ze względu na dynamiczny charakter rynku, przed ich wykorzystaniem w materiałach komercyjnych zaleca się potwierdzenie danych w aktualnych źródłach.

Tab 1. Przewidywane roczne zdolności produkcyjne amunicji 155mm wybranych producentów w Europie

Producent	Przewidywany wolumen roczny
Polska Grupa Zbrojeniowa	150 tys.
AMC Global	160 tys.
Niewiadów	180 tys.
KNDS	250-300 tys.
CSG	300-400 tys.
Rheinmetall	350-450 tys.

Poniżej około 100 tys. sztuk rocznie dominują argumenty jakościowe i bezpieczeństwa. Powyżej tego wolumenu zaczynają pojawiać się przesłanki ekonomiczne dla szerokiej automatyzacji. Przy wolumenach przekraczających 120 tys. sztuk rocznie dostępność linii staje się jednym z głównych czynników wpływających na koszt jednostkowy. W tej skali każda godzina nieplanowanego postoju obniża nie tylko bieżącą produkcję, ale również zdolność zakładu do utrzymania harmonogramu dostaw. Próg 120 tys. sztuk wynika z wydajności dwóch typowych linii do elaboracji pocisków wynoszący ok. 60 tys. sztuk / rok.

2. Referencyjna linia produkcyjna nowej generacji

Referencyjny model zakładu nowej generacji oparto na architekturze liniowo-gniazdowej obejmującej co najmniej dwa równoległe ciągi produkcyjne. Model ten nie opisuje technologii wytwarzania ani parametrów procesowych, lecz przedstawia docelową organizację przepływu materiałów, produktów i danych. Jego celem jest zobrazowanie struktury zakładu zaprojektowanego pod kątem wysokiej przepustowości, odporności operacyjnej, bezpieczeństwa procesowego oraz pełnej identyfikowalności wyrobów na każdym etapie produkcji.

Założenia projektowe

Układ referecyjny zakłada dwie równoległe linie produkcyjne pracujące w logice jednokierunkowego przepływu. Taki podział zwiększa odporność operacyjną: awaria jednej nitki nie musi zatrzymywać całego zakładu, a równoległa architektura ułatwia balansowanie wolumenu, serwisowanie i wdrażanie zmian procesowych.

- Dwie równoległe linie produkcyjne, pozwalające na separację przepływów i ograniczenie skutków awarii jednej nitki;
- Przepływ jednokierunkowy, ograniczający cofanie produktu i ryzyko pomyłek partii;
- Transport rolkowy między gniazdami, redukujący ręczną manipulację i stabilizujący takt transferu;
- Roboty typu KUKA do pobierania, pozycjonowania i przenoszenia korpusów lub półwyrobów między strefami;

- Pełna identyfikowalność produktu od przyjęcia partii do magazynu wyrobu gotowego;
- Kontrola jakości inline, obejmująca skanowanie laserowe, rejestr operacji i kontrolę X-Ray;
- Integracja MES/ERP/SCADA jako warunek wykorzystania AI w utrzymaniu ruchu i jakości.

Przepływ materiału

Przepływ materiału powinien być projektowany jako prosty i czytelny strumień: Magazyn Główny → Skaner Laserowy → Stacja Elaboracji → Kontrola X-Ray → Linia Malarska → Magazyn Produktowy. Każdy etap ma własną funkcję procesową i własny punkt danych. W takim modelu fizyczny przepływ produktu i cyfrowy przepływ informacji powinny być zsynchronizowane.

Tab 2. Zestawienie funkcji procesu oraz danych pomiarowych względem etapów procesu ryftuyjnego

Etap	Funkcja w przepływie	Dane / kontrola
Magazyn Główny	przygotowanie materiałów, komponentów i partii	identyfikacja dostaw, status jakościowy, kompletność partii
Skaner Laserowy	kontrola geometrii i identyfikacja produktu przed operacją główną	wynik skanu, ID partii, cyfrowy paszport produktu
Robot przeładunkowy	automatyczne pobranie, pozycjonowanie i transfer	liczba cykli, przeciążenia, status osi, alarmy
Stacja Elaboracji	operacja główna procesu w stacji referencyjnej	status operacji, czas cyklu, zapis parametrów dopuszczonych przez procedury
Kontrola X-Ray	kontrola wewnętrzna po operacji głównej	wynik NDT, klasyfikacja OK/NOK/HOLD, zapis obrazu lub decyzji
Linia Malarska	operacja powierzchniowa i oznaczeniowa	status transportu, suszenia, wentylacji i kontroli wizualnej
Magazyn Produktowy	odłożenie wyrobu po zwolnieniu jakościowym	lokalizacja, etykieta, status zwolnienia i traceability

Rola robotów

Roboty typu KUKA pełnią rolę kręgosłupa automatyzacji stanowiskowej. Ich zadaniem nie jest tylko przyspieszenie operacji, lecz także stabilizacja pozycji produktu, ograniczenie ręcznych transferów i zmniejszenie zmienności między operatorami. Robot może pobierać korpus lub półwyrób z transportu rolkowego, pozycjonować go względem oprzyrządowania, przenosić między gniazdami oraz odkładać na kolejnym odcinku przepływu.

Z punktu widzenia bezpieczeństwa robotyzacja ma szczególne znaczenie tam, gdzie ręczna manipulacja jest niepożądana z uwagi na masę elementu, wymagania ergonomiczne, bliskość stref niebezpiecznych lub konieczność zachowania powtarzalnej trajektorii. Wartość biznesowa robotów wzrasta jednak dopiero wtedy, gdy ich dane eksploatacyjne są wykorzystywane przez UR i systemy AI: liczba cykli, przeciążenia osi, alarmy serwonapędów i czasy postoju powinny zasilać model preventive maintenance.

Rola skanowania laserowego

Skanowanie laserowe powinno być traktowane jako bramka danych przed operacją główną. Jego funkcją jest nie tylko kontrola geometrii, lecz również potwierdzenie tożsamości produktu, zgodności partii i gotowości do dalszego przetwarzania. W modelu cyfrowym wynik skanowania staje się jednym z pierwszych wpisów w cyfrowym paszporcie produktu.

Cyfrowy paszport produktu powinien łączyć ID partii, historię materiałową, wyniki skanowania, status operacji, wynik X-Ray, status malowania i lokalizację magazynową. Dzięki temu jakość nie jest odtwarzana dopiero po reklamacji lub blokadzie partii, lecz powstaje jako bieżący zapis procesu.

Kontrola X-Ray

Kontrola X-Ray jest krytyczną bramką jakości między operacją główną czyli napełnianiem pocisku w materiał wybuchowy a dalszą obróbką powierzchniową. W modelu nowoczesnej fabryki nie powinna być traktowana jako osobna inspekcja końcowa, lecz jako element sterowania jakością w toku produkcji. Jej zadaniem jest potwierdzenie, że wyrób może przejść do kolejnego etapu bez ryzyka przeniesienia poważnej (i kosztownej) wady na dalsze operacje.

AI może wspierać analizę obrazów X-Ray przez priorytetyzację przypadków, wykrywanie wzorców niezgodności i porównanie wyników z historią partii. W klasach krytycznych decyzja powinna jednak pozostać objęta zatwierdzonym planem kontroli i nadzorem jakości. Największą wartością AI w X-Ray jest skrócenie czasu przeglądu, stabilizacja kryteriów oraz ograniczenie ryzyka „defect escape".

3. Ocena efektywności produkcji

Ocena automatyzacji nie powinna opierać się wyłącznie na OEE. Wskaźnik ten jest użyteczny, bo rozdziela dostępność, wydajność i jakość, ale nie pokazuje pełnego obrazu. Linia może mieć wysokie OEE, a jednocześnie generować nadmierny WIP, zbyt wiele interwencji utrzymania ruchu albo zbyt długi czas reakcji na niezgodność.

Tab 3. Wskaźniki oceny wpływu automatyzacji dla poszczególnych obszarów

Obszar	Przykładowe KPI	Wpływ automatyzacji/AI
Wydajność	throughput, takt, czas cyklu	stabilniejszy przepływ i mniej wąskich gardeł
Jakość	FPY, scrap, defect escape	wcześniejsze wykrywanie wad i separacja partii
Dostępność	OEE, MTBF, MTTR, awarie nieplanowane	preventive maintenance i lepsze planowanie UR
Bezpieczeństwo	ekspozycja, near miss, operacje ręczne	separacja operatora i mniej manipulacji ręcznej
Koszt	koszt jednostkowy, koszt jakości, koszt przestoju	spadek kosztu przy wysokim wykorzystaniu linii

W przyjętym modelu szczególną wagę należy przypisać dostępności urządzeń krytycznych: robotów, transportu rolkowego, stacji elaboracji, X-Ray i linii malarskiej. Wysoki wolumen powoduje, że przestój jednego urządzenia nie jest lokalnym problemem technicznym, lecz zdarzeniem wpływającym na koszt jednostkowy i zdolność realizacji dostaw.

4. Warstwa AI: funkcje, koszty i dojrzałość

Warstwa AI w fabryce amunicji to nie pojedynczy model, lecz system danych. Obejmuje sensory, kamery, X-Ray/CT, SCADA, MES, ERP, CMMS, infrastrukturę ryf lub serwerową, walidację modeli, monitoring ryftu, cyberbezpieczeństwo i procedury reakcji. Bez tej warstwy AI pozostaje prezentacją analityczną, a nie narzędziem poprawy dostępności, jakości i kosztu.

Preventive maintenance jako główne zastosowanie AI

Najdłuższy i najbardziej biznesowo uzasadniony fragment zastosowań AI w fabryce referencyjnej dotyczy preventive i predictive maintenance. W nowoczesnej linii amunicji awaria robota, transportu, X-Ray lub linii malarskiej może zatrzymać przepływ całej partii. AI powinna więc monitorować nie tylko jakość produktu, ale również stan techniczny infrastruktury, która tę jakość i przepustowość umożliwia.

Tab 4. Obszary i zakresy monitorowania infrastruktury przez system AI

Obiekt monitorowania	Sygnały dla AI	Cel utrzymaniowy
Roboty	serwonapędy, przekładnie, liczba cykli, przeciążenia, alarmy osi	wcześniejsze planowanie przeglądów, ograniczenie awarii robota i stabilizacja taktów transferu
Transport rolkowy	napędy, czujniki, prądy silników, zacięcia, czasy zatrzymania	redukcja mikroprzestojów i szybsza reakcja na narastające opory lub błędy detekcji
Skaner Laserowy	stabilność pomiaru, błędy kalibracji, odchylenia wyników, liczba powtórzeń skanu	utrzymanie wiarygodnej bramki wejściowej i ograniczenie fałszywych odrzuceń
X-Ray	dostępność urządzenia, cykle pracy, alarmy, harmonogram przeglądów, czas analizy	ochrona krytycznej bramki jakości i ograniczenie kolejek WIP przed kontrolą
Linia malarska	układy transportowe, suszenie, wentylacja, temperatury, alarmy filtracji	stabilność operacji powierzchniowej i redukcja braków estetycznych lub oznaczeniowych

Tak rozumiane preventive maintenance ma bezpośredni wpływ na OEE, MTBF i MTTR. Zamiast reagować na awarię po zatrzymaniu linii, zakład buduje harmonogram interwencji oparty na trendach zużycia, liczbie cykli, alarmach i odchyleniach procesu. To właśnie ten obszar jest najbardziej przekonujący dla czytelnika przemysłowego, ponieważ łączy AI z konkretnym kosztem: nieplanowanym postojem.

AI kontra KPI

Tab 5. Zestawienie funkcji AI względem przyjętych wskaźników KPI

Funkcja AI	KPI
Preventive Maintenance	OEE, MTBF, MTTR
Computer Vision	FPY, Scrap
X-Ray AI	Defect Escape
Scheduling AI	Throughput, WIP
Digital Twin	Cost per Unit

Kontrola jakości, harmonogramowanie i digital twin

Computer vision czyli techniki komputerowego przetwarzania i rozpoznawania obrazu mogą wspierać wykrywanie wad powierzchniowych, analizę zgodności oznaczeń i porównywanie geometrii. AI dla X-Ray może wspierać klasyfikację obrazów i ograniczenie defect escape, ale wymaga rygorystycznej walidacji oraz nadzoru jakości. Scheduling AI może ograniczać WIP i stabilizować przepływ między równoległymi liniami, natomiast budowa cyfrowego modelu fabryki czyli „cyfrowego bliźniaka" (digital twin) pozwala symulować wpływ awarii, przezbrojeń, zmian wolumenu i ograniczeń magazynowych na koszt jednostkowy.

Koszt AI obejmuje nie tylko licencje i serwery. Należy uwzględnić sensory, integrację IT/OT, czyszczenie danych, walidację, utrzymanie modeli, szkolenia, cyberbezpieczeństwo i czas inżynierów procesu, jakości oraz UR. Najbezpieczniejsza ścieżka wdrożenia jest etapowa: najpierw dane, traceability i pomiar stabilności, następnie modele predykcyjne dla UR, a dopiero później zaawansowane rekomendacje decyzyjne.

5. Dojrzałość cyfrowa wdrożeń

Do porównywania publikacji i wdrożeń potrzebna jest prosta skala dojrzałości cyfrowej. Bez niej obok siebie pojawiają się pełna kontrola inline, pojedynczy patent AI, linia automatyczna bez integracji danych i ogólna zapowiedź inwestycji. W artykule warto odróżnić automatyzację fizyczną, integrację danych, analitykę, rekomendacje decyzyjne i adaptacyjne sterowanie.

Tab 6. Poziomy dojrzałości cyfrowej oparte na założeniach Fundacji Digital Poland

Poziom	Charakterystyka	Ocena
D0	proces ręczny lub wyspowa mechanizacja bez danych	poza Industry 4.0
D1	automatyzacja stanowiskowa z lokalnym zapisem	wdrożenie punktowe
D2	integracja MES/SCADA i traceability partii	fundament cyfryzacji
D3	analityka jakości i preventive maintenance	dojrzałe użycie danych
D4	digital twin i rekomendacje decyzyjne	wdrożenie zaawansowane
D5	adaptacyjne sterowanie z nadzorem	kierunek przyszłości

Większość jawnie opisywanych rozwiązań w obszarze amunicji mieści się między D1 a D3. Oznacza to, że realne są wdrożenia automatyzacji, kontroli jakości i preventive maintenance, natomiast pełna fabryka adaptacyjna pozostaje raczej modelem docelowym. Takie rozróżnienie pozwala pokazać potencjał AI bez tworzenia wrażenia, że krytyczny proces technologiczny powinien być autonomicznie sterowany przez algorytm.

Wnioski

Automatyzacja produkcji amunicji jest najbardziej uzasadniona tam, gdzie łączą się: stabilny lub strategicznie gwarantowany popyt, wysokie wykorzystanie linii, wysoki

koszt niezgodności oraz istotne ryzyko BHP. Efekt skali pojawia się wtedy, gdy automatyzacja zwiększa przepustowość, redukuje koszt jakości i ogranicza nieplanowane postoje. W modelu referencyjnym szczególnie ważne są roboty, transport rolkowy, skanowanie laserowe, X-Ray, linia malarska oraz integracja MES/ERP/SCADA.

Najbardziej wiarygodna teza brzmi: AI powinna wzmacniać fabrykę amunicji przede wszystkim przez preventive i predictive maintenance, kontrolę jakości oraz planowanie przepływu, a nie przez autonomiczne sterowanie krytycznym procesem technologicznym. Dodatni ROI zależy od wolumenu, wykorzystania linii, kosztu braków, kosztu przestoju i dojrzałości danych.

O ile fabryki amunicji budowane przed 2023 rokiem były projektowane głównie pod minimalizację kosztów inwestycyjnych i umiarkowane wolumeny produkcji, o tyle nowa generacja zakładów budowanych obecnie w Europie jest projektowana pod wysoką przepustowość, odporność operacyjną oraz zdolność do szybkiego zwiększania produkcji. W takim środowisku automatyzacja, robotyzacja i systemy AI przestają być dodatkiem technologicznym, a stają się jednym z podstawowych elementów modelu biznesowego zakładu.

Wybrane źródła

European Commission, Act in Support of Ammunition Production (ASAP), 2023.
OSW, ASAP: EU support for ammunition production in member states, 2023.
NATO, NATO's role in defence industry production, 2024.
GAO, Army Modernization; GAO, NNSA Explosives Program, 2025.
RAND, Implications of Russia's War on Ukraine for Defense Industrial Bases, 2024.
MESKO/PGZ, komunikaty dotyczące zdolności produkcyjnych amunicji 155 mm, 2025.
STV Group, Launch of a new line for filling artillery shells, 2023.
General Inspection, Metrology News, materiały o automatycznej kontroli amunicji, 2019-2024.
North Star Imaging / Vcxray, CT/X-Ray dla uzbrojenia I amunicji, 2024-2025.
MDPI, Industry 4.0 Technologies on Underground Ammunition Storage, 2021.
Frontiers in AI, Generative and Predictive AI for digital twin systems in manufacturing, 2025.
Intel, Smart Manufacturing Using Computer Vision and AI for Inline Inspection, 2023.
McKinsey, The robotics revolution: Scaling beyond the pilot phase, 2025.
PIE, Robotyzacja w Polsce w 2023 roku, 2024.

Suwerenność gospodarcza – fundament bezpieczeństwa i rozwoju Polski

Jacek Sasin

ABSTRAKT:

Tekst analizuje koncepcję suwerenności gospodarczej w kontekście kryzysu globalizacji. Autor wskazuje na doświadczenia pandemii COVID-19, blokady Kanału Sueskiego i kryzysu energetycznego jako punkty zwrotne ujawniające kruchość modelu uzależnienia od zagranicznych dostaw. Formułuje tezę, że w XXI wieku bezpieczeństwo narodowe zaczyna się w elektrowni, hucie i zakładzie produkcyjnym. Za kluczowe priorytety uznaje reindustrializację, niezależność energetyczną i odbudowę krajowych łańcuchów wartości.

Słowa kluczowe: suwerenność gospodarcza, reindustrializacja, bezpieczeństwo energetyczne, globalizacja, łańcuchy dostaw, polityka przemysłowa

Jeszcze kilka lat temu wielu polityków, ekspertów i komentatorów przekonywało, że tzw. „koniec historii" zaprowadził ludzkość do demokracji liberalnej – ostatecznej, lepszej formy ustrojowej, a towarzysząca temu globalizacja miała sprawić, że państwa staną się od siebie tak zależne gospodarczo, iż konflikty przestaną się „opłacać". Dzięki temu produkcja mogła być lokowana na drugim końcu świata, a kluczowe technologie rozwijane poza Europą. W zamian mieliśmy otrzymać niższe koszty, większą efektywność i trwały dobrobyt.

Rzeczywistość okazała się znacznie bardziej brutalna. Pandemia COVID-19, blokada Kanału Sueskiego, kryzys energetyczny wywołany przez Rosję, wojna na Ukrainie, kryzys półprzewodników czy chińskie ograniczenia eksportowe pokazały, że suwerenność gospodarcza nie jest dodatkiem do bezpieczeństwa państwa. Jest jego podstawowym warunkiem.

Obecny upadek globalizacji nie został rozpoczęty przez jej przeciwników. Idea została obalona przez własne sprzeczności. Na globalizacji wygrali przede wszystkim ci, którzy nigdy nie uwierzyli w opowieść o świecie pozbawionym narodowych interesów. Wygrali ci, którzy przez cały czas prowadzili twardą transakcyjną politykę.

Chiny, wchodząc w 2001 roku do WTO, zaczęły na niespotykaną skalę korzystać z otwartych rynków Zachodu, jednocześnie konsekwentnie chroniąc własne strategiczne sektory. Stany Zjednoczone głosiły wolny handel, ale nigdy nie zrezygnowały z aktywnej polityki przemysłowej w obszarach kluczowych dla bezpieczeństwa narodowego. Państwa Zatoki Perskiej budowały narodowe fundusze majątkowe i przejmowały aktywa na całym świecie budując swój potencjał i wpływy w państwach rozwiniętych.

Problem „starej" Europy polegał na tym, że część jej elit uwierzyła, bądź chciała wierzyć, iż reguły geopolityki przestały obowiązywać. Tymczasem inni gracze nadal prowadzili politykę w kategoriach sprawczego wpływu na rzeczywistość. Stąd ostatnie lata to seria tak bolesnych lekcji.

Pandemia pokazała między innymi, że Europa ekstremalnie uzależniła się od azjatyckiej produkcji leków i substancji czynnych. Kiedy zerwane zostały łańcuchy dostaw, okazało się, że nawet podstawowe produkty medyczne nie są czymś, co możemy brać za pewnik.

Blokada Kanału Sueskiego przypomniała, jak kruche są globalne szlaki handlowe. Jeden statek wystarczył, aby sparaliżować znaczącą część światowego handlu. Następnie wspierani przez Iran rebelianci Huti pokazali, że podobne zakłócenia mogą trwać miesiącami.

Kryzys energetyczny udowodnił natomiast, że uzależnienie się np. Niemiec od rosyjskich surowców nie było przejawem realizmu, lecz strategicznej naiwności. Rosja wykorzystała energię jako broń polityczną. Państwa, które oddały kontrolę nad własnym bezpieczeństwem energetycznym, bardzo szybko znalazły się pod presją.

Wojna na Ukrainie obnażyła kolejną słabość Zachodu. Unia Europejska dysponuje gospodarką wielokrotnie większą od rosyjskiej. Mimo to nie jest zdolna do zapewnienia Ukrainie odpowiedniej ilości uzbrojenia i amunicji bez wsparcia Stanów Zjednoczonych. Okazało się, że potencjał gospodarczy nie wystarcza, jeśli przez dekady zaniedbuje się własny przemysł.

Te wydarzenia nie są przypadkiem. Są skutkiem wieloletniej polityki, w której ideologia bierze górę nad przemyślaną strategią ekonomiczną i bezpieczeństwem. Dziś rachunek za tę politykę płacą europejskie gospodarki, europejski przemysł i – przede wszystkim – europejskie społeczeństwa.

To wszystko nie oznacza – oczywiście – końca współpracy międzynarodowej. Nie oznacza zamknięcia granic ani gospodarczej autarkii – to nierealne, tym bardziej w XXI wieku. Oznacza coś znacznie bardziej fundamentalnego. Oznacza zrozumienie, że państwo musi zachować sterowalność nad tymi obszarami, od których zależy jego bezpieczeństwo i rozwój.

W XXI wieku bezpieczeństwo narodowe nie zaczyna się na granicy państwa. Zaczyna się w elektrowni. Zaczyna się w hucie. Zaczyna się w laboratorium farmaceutycznym. Zaczyna się w centrum danych. Zaczyna się tam, gdzie powstają zdolności pozwalające państwu funkcjonować niezależnie od zewnętrznych nacisków.

Szczególne znaczenie ma tutaj energetyka. Bez stabilnej i konkurencyjnej cenowo energii nie ma nowoczesnego przemysłu. Bez przemysłu nie ma trwałego wzrostu gospodarczego. Bez wzrostu nie ma środków na obronność, infrastrukturę czy politykę społeczną.

Tymczasem Unia Europejska prowadzi politykę energetyczną w oderwaniu od realiów gospodarczych. Rosnące koszty energii stają się jednym z głównych powodów utraty konkurencyjności europejskiego przemysłu. Coraz więcej przedsiębiorstw przegrywa rywalizację z konkurentami działającymi poza UE, którzy nie ponoszą porównywalnych kosztów regulacyjnych.

Polska nie może zaakceptować sytuacji, w której polityka energetyczna prowadzi do likwidacji własnego potencjału. Transformacja energetyczna musi być podporządkowana interesowi narodowemu, a nie odwrotnie. Potrzebujemy nowych technologii, energetyki jądrowej, magazynów energii i nowoczesnych sieci. Potrzebujemy polskiej drogi w transformacji naszej energetyki.

Przez lata słyszeliśmy, że miejsce produkcji nie ma większego znaczenia. Liczy się wyłącznie cena i efektywność. Dzisiaj widzimy konsekwencje takiego myślenia. To nie są teoretyczne rozważania. To są zależności, które w ostatnich latach obserwowaliśmy na własne oczy. Przykład hutnictwa jest szczególnie wymowny. Polska przez dekady ograniczała własne zdolności produkcyjne, podczas gdy konkurenci spoza Unii Europejskiej korzystali z tańszej energii i znacznie mniej restrykcyjnych regulacji. Efekt jest łatwy do przewidzenia. Rośnie uzależnienie od importu stali, a wraz z tym maleje odporność państwa na kryzysy. Nie chodzi przy tym o sentymentalny powrót do przemysłu XIX wieku. Chodzi o budowę nowoczesnej bazy produkcyjnej wykorzystującej automatyzację, robotyzację, sztuczną inteligencję i zaawansowane technologie. Reindustrializacja nie jest powrotem do przeszłości. Jest warunkiem przyszłego rozwoju.

Coraz większego znaczenia nabiera również suwerenność technologiczna. W świecie sztucznej inteligencji, cyberwojny i cyfrowej gospodarki państwa

konkurują nie tylko kapitałem i zasobami naturalnymi. Konkurują zdolnością do tworzenia własnych technologii. Kto kontroluje dane, algorytmy i infrastrukturę cyfrową, ten w coraz większym stopniu kontroluje przyszłość. Polska nie może być wyłącznie odbiorcą cudzych rozwiązań. Musimy rozwijać własne kompetencje, wspierać polskich inżynierów, naukowców i przedsiębiorców oraz tworzyć warunki do powstawania przełomowych technologii. To samo dotyczy kapitału.

Nie zbudujemy trwałej podmiotowości gospodarczej, jeśli strategiczne decyzje inwestycyjne będą zapadały wyłącznie poza granicami kraju. Kapitał ma narodowość. Potrzebujemy silnego, rodzimego – polskiego kapitału, zdolnego finansować rozwój, ekspansję zagraniczną i budowę narodowych czempionów. Dlatego tak istotne jest stworzenie instrumentów pozwalających wspierać polski biznes, mobilizować krajowe oszczędności i kierować je do sektorów strategicznych. Państwo nie powinno zastępować przedsiębiorców. Powinno jednak tworzyć komfortowe warunki, które umożliwią polskim firmom skuteczną konkurencję na globalnych rynkach.

Polska znajduje się dziś w szczególnym momencie historycznym. Procesy nearshoringu i friendshoringu powodują, że coraz więcej inwestorów poszukuje bezpiecznych lokalizacji bliżej europejskich rynków. To ogromna szansa dla naszego kraju. Możemy stać się jednym z głównych operatorów przebudowy światowej gospodarki. Nie stanie się to jednak automatycznie. Potrzebujemy państwa aktywnego, sprawczego i świadomego własnych interesów. Państwa, które rozumie znaczenie energii, przemysłu, technologii i kapitału. Państwa zdolnego do prowadzenia długofalowej polityki rozwojowej.

Największym błędem byłoby dziś przekonanie, że wystarczy przeczekać obecne turbulencje, a świat wróci do ułudy globalizacyjnej bajki. Wchodzimy w epokę trwałej rywalizacji gospodarczej, technologicznej i geopolitycznej. W takiej rzeczywistości zwyciężają państwa, które potrafią skutecznie bronić własnych interesów. Suwerenność gospodarcza nie jest hasłem wyborczym. Jest praktyczną odpowiedzią na świat, który stał się bardzo niebezpieczny.

Polska potrzebuje nowej doktryny rozwoju. Doktryny opartej na silnym systemie, silnej gospodarce i silnym polskim kapitale. Doktryny, która łączy strategiczne interesy narodowe z zachowaniem zdolności do samodzielnego działania. Silne państwa są podmiotami ładu gospodarczego. Pozostałe stają się przedmiotem decyzji podejmowanych przez innych.

Od tego, do której grupy będzie należeć Polska, zależy nie tylko tempo naszego rozwoju. W największym stopniu zależy od tego bezpieczeństwo i spokój życia przyszłych pokoleń Polek i Polaków.

Bezpieczeństwo polskich portów morskich – od ochrony przed zagrożeniami hybrydowymi do zabezpieczenia strategicznych interesów państwa

Michał Śmigielski

Abstrakt:
Artykuł analizuje bezpieczeństwo polskich portów morskich wobec narastających zagrożeń hybrydowych. Autor omawia zagrożenia dla infrastruktury portowej: sabotaż, cyberataki, działalność wywiadowczą i drony. Na przykładach konkretnych podmiotów wskazuje na strategiczne wymiary własności infrastruktury portowej. Podkreśla, że porty morskie stają się elementami systemu bezpieczeństwa i odporności państwa, nie tylko węzłami logistycznymi.
Słowa kluczowe: porty morskie, bezpieczeństwo morskie, zagrożenia hybrydowe, infrastruktura krytyczna, cyberbezpieczeństwo, Bałtyk

Wstęp

Porty morskie odgrywają kluczową rolę w funkcjonowaniu współczesnych państw. W przypadku Polski ich znaczenie wykracza daleko poza tradycyjnie rozumianą funkcję transportową. Porty w Gdańsku, Gdyni, Szczecinie i Świnoujściu są obecnie

elementem infrastruktury krytycznej państwa, mającym wpływ na bezpieczeństwo gospodarcze, energetyczne, żywnościowe i militarne. Wojna w Ukrainie oraz zmiana sytuacji geopolitycznej na Morzu Bałtyckim uwidoczniły strategiczne znaczenie infrastruktury portowej oraz potrzebę jej kompleksowej ochrony.

Współczesne bezpieczeństwo portów nie może być postrzegane wyłącznie przez pryzmat ochrony fizycznej. Coraz większego znaczenia nabierają zagrożenia hybrydowe, cyberbezpieczeństwo, bezpieczeństwo energetyczne, kontrola strategicznych łańcuchów dostaw oraz struktura właścicielska operatorów terminalowych.

Współczesne zagrożenia dla polskich portów

Do najważniejszych zagrożeń należą działania hybrydowe, sabotaż infrastruktury krytycznej, cyberataki, działalność wywiadowcza, operacje dezinformacyjne oraz wykorzystanie podmiotów gospodarczych do realizacji celów politycznych. Przykłady uszkodzeń infrastruktury podmorskiej na Bałtyku pokazały, że współczesne konflikty mogą być prowadzone poniżej progu otwartej wojny.

Coraz większym wyzwaniem są również bezzałogowe systemy powietrzne i nawodne. Rozwój technologii powoduje, że infrastruktura portowa, energetyczna i logistyczna wymaga coraz bardziej zaawansowanych systemów ochrony i monitorowania.

System ochrony polskich portów

Za bezpieczeństwo portów odpowiadają przede wszystkim Morski Oddział Straży Granicznej, Marynarka Wojenna RP, administracja morska oraz służby odpowiedzialne za ochronę infrastruktury krytycznej. Straż Graniczna realizuje zadania związane z ochroną granicy morskiej, kontrolą ruchu jednostek pływających oraz przeciwdziałaniem zagrożeniom terrorystycznym.

Marynarka Wojenna RP odpowiada za bezpieczeństwo żeglugi oraz ochronęstrategicznej infrastruktury na Morzu Bałtyckim, w tym Baltic Pipe, infrastruktury LNG, kabli podmorskich i torów podejściowych do portów.

Wraz z rozwojem sektora offshore wind zakres odpowiedzialności tych służb rozszerza się o ochronę morskich farm wiatrowych, stacji transformatorowych, podmorskich kabli energetycznych oraz portów instalacyjnych i serwisowych.

Strategiczna infrastruktura energetyczna

Polska zachowała pełną kontrolę nad najważniejszą infrastrukturą energetyczną zlokalizowaną w portach. Naftoport w Gdańsku pozostaje pod kontrolą PERN i jest jednym z filarów bezpieczeństwa energetycznego państwa. Po odejściu od importu rosyjskiej ropy jego znaczenie jeszcze wzrosło.

Podobnie Terminal LNG im. Prezydenta Lecha Kaczyńskiego w Świnoujściu zarządzany jest przez GAZ-SYSTEM i umożliwia dywersyfikację dostaw gazu ziemnego. Oba obiekty stanowią przykład świadomego utrzymania kontroli państwa nad najbardziej strategicznymi aktywami energetycznymi.

Należy również odnotować działania zmierzające do zwiększania krajowej kontroli nad wybranymi elementami infrastruktury portowej o znaczeniu strategicznym. Przykładem jest przejęcie przez państwowy Węglokoks spółki Port Północny od belgijskiej grupy Sea-Invest.

Port Północny w Gdańsku należy do najważniejszych terminali masowych w Polsce i odgrywa istotną rolę w przeładunkach surowców strategicznych, w szczególności węgla oraz rud żelaza. Znaczenie terminalu wzrosło szczególnie po 2022 roku, kiedy Polska zwiększyła import surowców energetycznych drogą morską w związku ze zmianą kierunków dostaw.

Przejęcie terminalu przez Węglokoks było postrzegane jako element wzmacniania kontroli państwa nad infrastrukturą mającą znaczenie dla bezpieczeństwa energetycznego i gospodarczego kraju. Przypadek Portu Północnego pokazuje, że polityka państwa wobec infrastruktury portowej może obejmować również działania właścicielskie ukierunkowane na zabezpieczenie strategicznych interesów gospodarczych państwa.

Operatorzy terminalowi i kontrola operacyjna

Znacznie bardziej złożona jest sytuacja w przypadku terminali logistycznych, kontenerowych i masowych. W Gdańsku działa Baltic Hub, największy terminal kontenerowy na Bałtyku, którego udziałowcami są PSA International, Polski FunduszRozwoju oraz IFM Investors.

W Porcie Gdynia funkcjonują dwa główne terminale kontenerowe. GCT zarządzany jest przez Hutchison Ports Holdings, natomiast BCT należy do filipińskiej

grupy ICTSI. Warto zauważyć, że PSA International posiada około 20% udziałów w Hutchison Ports Holdings, co pokazuje skalę globalnych powiązań kapitałowych w sektorze portowym.

W Szczecinie większościowym udziałowcem Bulk Cargo Szczecin został niemiecki operator logistyczny Rhenus Logistics. Działają tam również podmioty związane z obsługą rynku rolnego i przeładunków masowych.

Baltic Hub jest obecnie jedynym terminalem głębokowodnym na Morzu Bałtyckim zdolnym do regularnej obsługi największych oceanicznych kontenerowców zawijających bezpośrednio z Dalekiego Wschodu. Podkreśla to jego strategiczne znaczenie nie tylko dla Polski, ale również dla całego regionu Europy ŚrodkowoWschodniej.

OT Logistics, GBT i SBT

Ważnym elementem polskiego sektora portowego pozostaje grupa OT Logistics, która przez wiele lat była największym krajowym operatorem portowo-logistycznym. Wejście kapitału zagranicznego (Czechy) do grupy było przez część ekspertów postrzegane jako utrata szansy na budowę silnego narodowego operatora logistycznego.

Warto również zwrócić uwagę na GBT Terminal w Gdańsku oraz SBT Terminal w Szczecinie, które związane są z działalnością Copenhagen Merchants i odgrywają istotną rolę w obsłudze rynku produktów rolnych i paszowych.

Viterra, Copenhagen Merchants i bezpieczeństwo żywnościowe

Viterra należy do największych światowych traderów zbożowych i działa w obszarach skupu, magazynowania, eksportu oraz logistyki produktów rolnych. Copenhagen Merchants jest jednym z najważniejszych podmiotów handlujących produktami rolnymi w regionie Morza Bałtyckiego.

Obie grupy od lat współpracują biznesowo, co powoduje, że ich obecność w polskich portach ma znaczenie nie tylko gospodarcze, ale również strategiczne. Kontrola nad infrastrukturą eksportową produktów rolnych może mieć wpływ na bezpieczeństwo żywnościowe państwa oraz konkurencyjność polskiego sektora rolnego.

Bałtycki Terminal Zbożowy w Gdyni

Sprawa Bałtyckiego Terminalu Zbożowego w Gdyni stała się jednym z najciekawszych przykładów zmiany podejścia państwa do infrastruktury strategicznej. W dwóch kolejnych postępowaniach przetargowych zwyciężyło konsorcjum związane ze SzczecinBulk Terminal, Copenhagen Merchants oraz Viterrą.

Pomimo wygrania przetargów terminal nie został dotychczas ostatecznie przekazany operatorowi. Przypadek ten pokazuje, że współczesna ocena inwestycji infrastrukturalnych coraz częściej uwzględnia nie tylko efektywność ekonomiczną, ale również kwestie bezpieczeństwa państwa.

Offshore wind, Baltic Pipe i nowy wymiar bezpieczeństwa energetycznego

Nowym filarem bezpieczeństwa energetycznego Polski ma stać się morska energetyka wiatrowa. Projekt Orlenu i Northland Power – Baltic Power jest już na ukończeniu budowy, Projekt Baltica 2 realizowany jest przez PGE i Ørsted, natomiast projektyBałtyk II i Bałtyk III przez Polenergię i Equinor.

Szczególne znaczenie ma Equinor, który jest jednocześnie jednym z głównych dostawców gazu ziemnego do Polski poprzez Baltic Pipe. Choć sam gazociąg pozostaje pod kontrolą operatorów państwowych – GAZ-SYSTEM i Energinet – rola dużych międzynarodowych koncernów energetycznych w systemie bezpieczeństwa energetycznego Polski stale rośnie.

Z jednej strony współpraca z Equinor i Ørsted wzmacnia niezależność energetyczną Polski. Z drugiej strony pokazuje, że bezpieczeństwo energetyczne państwa coraz silniej zależy od relacji z globalnymi partnerami uczestniczącymi w dostawach gazu, rozwoju offshore wind i funkcjonowaniu infrastruktury energetycznej na Bałtyku.

Powstająca infrastruktura offshore wind wymaga również rozwoju portów instalacyjnych i serwisowych, które w przyszłości staną się elementem infrastruktury krytycznej państwa porównywalnym pod względem znaczenia do terminali energetycznych.

Ochrona tej infrastruktury będzie jednym z kluczowych zadań administracji morskiej, Straży Granicznej oraz Marynarki Wojennej RP.

Gdzie kończy się biznes, a zaczyna bezpieczeństwo państwa

Analiza struktury właścicielskiej i operatorskiej polskich portów prowadzi do interesującego wniosku. Polska zachowała kontrolę nad strategiczną infrastrukturą energetyczną, ale znacząca część terminali kontenerowych, masowych i agro znajduje się pod operacyjną kontrolą międzynarodowych operatorów.Nie musi to oznaczać zagrożenia dla państwa, wymaga jednak skutecznych mechanizmów nadzoru oraz zdolności do reagowania w sytuacjach kryzysowych.

Współczesne bezpieczeństwo portów obejmuje bowiem nie tylko ochronę fizyczną, ale również kontrolę przepływów logistycznych, bezpieczeństwo danych, odporność łańcuchów dostaw oraz bezpieczeństwo energetyczne i żywnościowe.

Perspektywy rozwoju – zespół portowy Gdańsk–Gdynia

Analizując przyszłość polskiej gospodarki morskiej warto rozważyć doświadczenia największych portów europejskich. Szczególnie interesującym przykładem jest utworzenie Port of Antwerp-Bruges, powstałego w wyniku integracji dwóch belgijskich portów.

W polskich warunkach podobna dyskusja mogłaby dotyczyć utworzenia silnego zespołu portowego Gdańsk–Gdynia. Oba porty funkcjonują w bezpośrednim sąsiedztwie, obsługują podobne segmenty rynku i stanowią najważniejszy ośrodek gospodarki morskiej w Polsce.

Prowadzenie wspólnej polityki strategicznej, inwestycyjnej i logistycznej mogłoby zwiększyć konkurencyjność polskich portów wobec Hamburga oraz innych największych portów Europy. Tego rodzaju rozwiązanie wymagałoby jednak szczegółowych analiz ekonomicznych, organizacyjnych i prawnych.

Wnioski

Bezpieczeństwo polskich portów morskich należy dziś postrzegać jako zdolność państwa do ochrony infrastruktury przed zagrożeniami hybrydowymi oraz do zabezpieczenia strategicznych interesów narodowych poprzez utrzymanie odpowiedniej kontroli nad kluczowymi procesami logistycznymi, energetycznymi i żywnościowymi.

Porty przestały być wyłącznie miejscem przeładunku towarów. Stały się elementem systemu bezpieczeństwa państwa, obejmującego energetykę, żywność, logistykę, infrastrukturę offshore oraz współpracę międzynarodową. W świecie narastającej rywalizacji geopolitycznej przyszłość polskich portów będzie zależała nie tylko od skuteczności ich ochrony, lecz również od umiejętności budowania silnych i konkurencyjnych struktur zdolnych do rywalizacji z największymi portami Europy.

W tym kontekście bezpieczeństwo polskich portów morskich należy rozumieć nie tylko jako zdolność do ochrony infrastruktury przed zagrożeniami hybrydowymi, lecz również jako umiejętność zachowania kontroli nad procesami logistycznymi, energetycznymi i żywnościowymi, które w coraz większym stopniu decydują o suwerenności gospodarczej państwa.

Suwerenność albo zależność. Jak zbudować polską gospodarkę bezpieczeństwa i system odstraszania?

Dariusz Wroński

ABSTRAKT:

Artykuł analizuje strategiczne wyzwania stojące przed Polską w zakresie budowy przemysłu obronnego zdolnego do funkcjonowania zarówno w warunkach pokoju, jak i konfliktu wysokiej intensywności. Autor stawia tezę, że doświadczenia wojny rosyjsko-ukraińskiej obaliły mit „małej zawodowej armii" i przywróciły znaczenie przemysłowej skali produkcji jako czynnika odstraszania. Wskazuje filary zdolności bojowych niezbędnych Polsce: masową produkcję amunicji, warstwową obronę przeciwlotniczą, zdolności dronowe oraz integrację systemów sieciocentrycznych. Artykuł omawia rolę śmigłowców bojowych AH-64E Apache jako platformy wielodomenowej oraz analizuje koncepcję dual-use, w myśl której inwestycje obronne stanowią zarazem koło zamachowe nowoczesnej gospodarki. W konkluzji autor formułuje pięć rekomendacji strategicznych dotyczących przebudowy polskiej „fabryki bezpieczeństwa".

Słowa kluczowe: gospodarka bezpieczeństwa, przemysł obronny, odstraszanie, suwerenność, mobilizacja przemysłowa, , systemy dronowe, Apache AH-64E, dual-use, Ukraina

Polska jako państwo frontowe – nowe zobowiązania strategiczne

Jeszcze kilka lat temu w wielu państwach dominowało myślenie wyłącznie o konfliktach ekspedycyjnych, ograniczonych operacjach stabilizacyjnych oraz profesjonalnych

armiach wyposażonych w niewielką liczbę zaawansowanych technologicznie platform bojowych. Liczyła się precyzja, przewaga informacyjna i szybkość projekcji siły. Wojna rosyjsko-ukraińska brutalnie zweryfikowała ten sposób myślenia: okazała się nie tylko konfliktem o terytorium Ukrainy, lecz przede wszystkim wielkim eksperymentem strategicznym XXI wieku, pokazującym, jak wygląda wojna nowej generacji prowadzona jednocześnie metodami przemysłowymi i technologicznymi. Każdego dnia testowane są w niej nowe technologie, modele dowodzenia, sposoby wykorzystania dronów, amunicji precyzyjnej, systemów walki radioelektronicznej oraz zdolności przemysłowych państw.

Jedna z najważniejszych lekcji tej wojny brzmi – nie wygrywa wyłącznie ten, kto ma najlepszy sprzęt, wygrywa ten, kto potrafi szybciej produkować, odtwarzać straty, adaptować technologię i utrzymać odporność państwa przez wiele miesięcy lub lat konfliktu. Jest to fundamentalna zmiana logiki bezpieczeństwa. W świecie niestabilnym nie wystarczy posiadać silnej armii – trzeba posiadać silne państwo przemysłowe zdolne do długotrwałego prowadzenia działań zbrojnych przy równoczesnym utrzymaniu funkcjonowania gospodarki. Innymi słowy, niezbędna jest nowoczesna „fabryka bezpieczeństwa".

Polska znajduje się dziś w szczególnym położeniu geopolitycznym. Nie jest państwem odległym od potencjalnego zagrożenia ani państwem zaplecza – jest państwem frontowym NATO, kluczowym węzłem logistycznym i strategiczną przestrzenią operacyjną Sojuszu. Ta geograficzna rzeczywistość nakłada na Polskę obowiązki, których nie sposób delegować na innych partnerów sojuszniczych. Rosja, nawet po zakończeniu konfliktu zbrojnego na Ukrainie, pozostanie państwem zmilitaryzowanym z ogromnym potencjałem adaptacyjnym, przemysłem wojennym oraz zdolnością do prowadzenia konfliktu długotrwałego. Doświadczenie pokazuje, że sankcje gospodarcze i straty wojskowe nie wyczerpały szybko jej zdolności do prowadzenia działań – Federacja Rosyjska przeszła bowiem częściową transformację w gospodarkę wojenną. Wniosek jest zatem prosty – Polska nie może budować armii wyłącznie na czas pokoju, lecz musi tworzyć system bezpieczeństwa zdolny do funkcjonowania w warunkach wojny wysokiej intensywności, co wymaga gruntownej zmiany filozofii myślenia o przemyśle obronnym.

Koniec iluzji „małej zawodowej armii"

Doświadczenia ukraińskiego i rosyjskiego pola walki obaliły kilka wojskowych mitów ostatnich dekad. Okazało się, że po pierwsze: współczesna wojna nie jest krótka;

po drugie: nowoczesna technologia nie eliminuje znaczenia masy; po trzecie: zapasy amunicji liczone na kilka dni walki stanowią fikcję strategiczną. Europa Zachodnia przez lata redukowała magazyny amunicji, moce produkcyjne i potencjał mobilizacyjny, uznając, że intensywny konflikt zbrojny na kontynencie jest mało prawdopodobny. Dziś okazuje się, że intensywność zużycia amunicji artyleryjskiej na Ukrainie wielokrotnie przekraczała możliwości produkcyjne wielu państw NATO.

Oznacza to, że przemysł obronny staje się integralną częścią systemu odstraszania. W XXI wieku nie odstrasza już wyłącznie liczba czołgów czy samolotów, lecz również zdolność państwa do szybkiego odtworzenia strat, masowej produkcji efektorów i utrzymania ciągłości działań bojowych. Przeciwnik musi mieć świadomość, że nawet po pierwszym uderzeniu państwo nie zostanie sparaliżowane przemysłowo ani logistycznie. To nowe rozumienie odstraszania wymaga zasadniczej zmiany podejścia do planowania obronnego.

Cztery filary zdolności bojowych

Wbrew logice efektownych zakupów platformowych, Polska potrzebuje dziś przemyślanej struktury czterech wzajemnie powiązanych zdolności bojowych. Błędem byłoby budowanie sił zbrojnych według kryterium prestiżu pozyskiwanego sprzętu – doświadczenia ukraińskiego pola walki pokazują bowiem wyraźnie, że nawet najdroższe platformy bez odpowiedniego ekosystemu wsparcia szybko tracą wartość operacyjną.

Pierwszym i najważniejszym „systemem uzbrojenia" współczesnej wojny pozostaje amunicja. Polska musi osiągnąć zdolność produkcji liczonej nie w tysiącach, lecz w setkach tysięcy sztuk rocznie – amunicji 155 mm, rakietowej, precyzyjnej, efektorów przeciwlotniczych oraz inteligentnych systemów minowania. Państwo, które nie produkuje amunicji na wystarczającą skalę, w praktyce oddaje kontrolę nad własnym bezpieczeństwem.

Drugi filar to warstwowa obrona przeciwlotnicza. Doświadczenia ukraińskie jednoznacznie pokazują, że państwo pozbawione tej zdolności szybko traci możliwość funkcjonowania jako całość. Rosja uderza nie tylko w siły zbrojne, lecz w system energetyczny, logistykę, centra dowodzenia, lotniska, kolej i przemysł. Polska musi budować pełny ekosystem obrony obejmujący systemy Patriot dla celów wysokiego pułapu, Narew dla średniego zasięgu, Pilica+, Poprad i Piorun dla bardzo krótkiego zasięgu, a także systemy C-UAS do zwalczania dronów, wspartą szeroką warstwą

radarową i pasywnymi sensorami. Ochrona musi objąć nie tylko stolicę, lecz porty, rafinerie, terminale LNG, mosty, centra logistyczne, zakłady przemysłowe i infrastrukturę energetyczną.

Trzecim filarem są systemy bezzałogowe – nowa artyleria XXI wieku, która w wielu sektorach pola walki zastępuje dziś klasyczne systemy bojowe, artylerię, a nawet lotnictwo załogowe. Polska powinna rozwijać jednocześnie kilka kategorii: tanie i masowe mikro-drony i drony FPV, drony rozpoznawcze na poziomie batalionu i brygady zapewniające pełną świadomość sytuacyjną, tanią amunicję krążącą jako alternatywę dla kosztownych systemów rakietowych, drony logistyczne zdolne do dostarczania zaopatrzenia na pierwszą linię oraz platformy klasy MALE do głębokiego rozpoznania i uderzeń. Przyszły konflikt nie będzie pojedynkiem platform – będzie starciem sensorów, algorytmów, autonomii i zaplecza przemysłowego.

Czwartym filarem jest integracja sieciocentryczna. Żaden z wymienionych komponentów nie osiągnie pełnej wartości operacyjnej w izolacji – decydujące znaczenie ma architektura połączeń między sensorami, systemami dowodzenia, środkami rażenia i zapleczem logistycznym.

AH-64E Apache: platforma wielodomenowa, nie „latający czołg"

W debacie publicznej regularnie powraca pytanie o zasadność utrzymywania śmigłowców bojowych Apache AH-64E w dobie dominacji dronów na współczesnym polu walki. Odpowiedź jest twierdząca – pod jednym zasadniczym warunkiem. Apache nie może być traktowany jak „latający czołg" w rozumieniu doktrynalnym z Iraku czy Afganistanu. Środowisko walki nasycone przenośnymi przeciwlotniczymi zestawami rakietowymi (MANPADS), radarami, dronami i środkami walki radioelektronicznej radykalnie zmieniło sposób użycia śmigłowców bojowych i wymogi wobec ich integracji systemowej.

AH-64E Apache pozostaje jednym z najpotężniejszych systemów pola walki pod warunkiem, że staje się elementem sieciocentrycznego systemu rażenia. Jego niezmienne przewagi operacyjne obejmują zdolność do działania nocnego, wysoką świadomość sytuacyjną, integrację danych w czasie rzeczywistym, skuteczne niszczenie wojsk pancernych, dynamiczne zwalczanie celów wysokiej wartości oraz szybkie reagowanie operacyjne. Jednak Apache XXI wieku musi współdziałać z rojami dronów

rozpoznawczych, systemami walki radioelektronicznej, samolotami F-35, zasobami satelitarnymi i rozpoznaniem klasy ISR oraz artylerią dalekiego zasięgu. Apache pozbawiony tej integracji staje się podatny na zagrożenia; Apache współpracujący z dronami staje się myśliwym o zasadniczo zwiększonej skuteczności. Z perspektywy Wojsk Aeromobilnych śmigłowiec bojowy zachowuje niezastąpioną wartość jako narzędzie manewru – zwłaszcza w działaniach nocnych, rozproszonych i dynamicznych – jednak jego użycie wymaga dziś znacznie wyższej niż dotychczas świadomości zagrożeń oraz pełnej integracji systemowej.

Dual-use: przemysł obronny jako koło zamachowe gospodarki

Fundamentalnym błędem w myśleniu o przemyśle obronnym jest traktowanie go wyłącznie w kategorii kosztu. Nowoczesny przemysł bezpieczeństwa jest kołem zamachowym całej gospodarki. Technologie wojskowe przechodzą do sektora cywilnego w dziedzinach sztucznej inteligencji, robotyki, cyberbezpieczeństwa, sensoryki, technologii kosmicznych, energetyki rozproszonej i komunikacji. Mechanizm ten, dobrze znany w Izraelu, Korei Południowej i Finlandii, sprawia, że inwestycje obronne wzmacniają jednocześnie konkurencyjność całej gospodarki – to właśnie istota koncepcji dual-use.

Polska posiada dziś wyjątkową szansę połączenia potencjału dużych spółek obronnych z dynamiką sektora prywatnego, startupów technologicznych, uczelni i centrów badawczo-rozwojowych. Warunkiem koniecznym jest jednak rezygnacja z modelu opartego wyłącznie na montowniach zagranicznych systemów na rzecz budowy własnych kompetencji: własnych algorytmów, elektroniki, amunicji i autonomii technologicznej.

Podsumowanie: pięć rekomendacji dla polskiej polityki bezpieczeństwa

Ryzyko przegrania wojny zwielokrotnia się, gdy brakuje zdolności do produkowania bezpieczeństwa szybciej, niż przeciwnik produkuje zagrożenie. Doświadczenie ukraińskie potwierdziło, że za żołnierzem stoją fabryki, energetyka, logistyka, algorytmy,

przemysł i odporność społeczna – to tam rozstrzygają się wyniki współczesnych konfliktów zbrojnych. Polska nie może być wyłącznie konsumentem bezpieczeństwa w ramach NATO, musi stać się jego współproducentem.

W tym celu należy przyjąć pięć rekomendacji strategicznych. Po pierwsze, model konfliktu długotrwałego powinien stać się centralnym punktem odniesienia w planowaniu obronnym, zastępując dominującą dotychczas optykę krótkich kampanii. Po drugie, przemysł obronny musi zostać uznany za infrastrukturę strategiczną państwa na równi z energetyką i transportem. Po trzecie, Polska powinna podjąć konsekwentne działania zmierzające do uzyskania pozycji europejskiego lidera w obszarze technologii dronowych i systemów antydronowych, inwestując zarówno w krajowe zdolności produkcyjne, jak i w certyfikację i eksport. Po czwarte, niezbędne jest radykalne zwiększenie zdolności wytwarzania amunicji i efektorów, ze szczególnym uwzględnieniem produkcji amunicji 155 mm oraz systemów precyzyjnych. Po piąte, konieczne jest stworzenie i instytucjonalne utrwalenie narodowego ekosystemu dual-use łączącego wojsko, przemysł, środowisko naukowe i sektor prywatny. Realizacja tych rekomendacji – w formule „fabryki bezpieczeństwa" – nie oznacza militaryzacji państwa, lecz budowę państwa zdolnego do przetrwania kryzysu, odstraszenia przeciwnika i równoczesnego rozwijania nowoczesnej gospodarki.

Cyberbezpieczeństwo jako warunek odporności państwa i akcelerator rozwoju gospodarczego

Tomasz Zdzikot

Abstrakt:

Artykuł argumentuje za postrzeganiem cyberbezpieczeństwa jako nowej infrastruktury rozwoju – nie kosztu, lecz inwestycji. Autor omawia specyficzne uwarunkowania Polski jako państwa frontowego NATO i trzy wymiary wartości cyberbezpieczeństwa: kompetencje, rynek i zaufanie. Analizuje nadchodzącą rewolucję kwantową i wyzwania kryptografii postkwantowej. Identyfikuje lukę wykonawczą – nie zasobową – jako główną przeszkodę.

Słowa kluczowe: cyberbezpieczeństwo, odporność państwa, NIS2, kryptografia postkwantowa, luka wykonawcza, inwestycja, bezpieczeństwo cyfrowe

Wprowadzenie: cyberbezpieczeństwo w logice odpornego państwa

Odporności państwa nie uda się osiągnąć, traktując bezpieczeństwo jako sumę oddzielnych polityk sektorowych. Współczesny kryzys rzadko ma charakter homogeniczny, a kluczem jest zbudowanie zdolności do utrzymania ciągłości działania pod presją, wtedy, gdy ryzyka materializują się równocześnie w wielu obszarach i wzajemnie wzmacniają. Akty sabotażu, dezinformacja, ataki na łańcuchy dostaw i infrastrukturę krytyczną mogą być elementami tej samej operacji. Państwo zdolne

do działania to takie, które w warunkach skumulowanego napięcia nie traci sterowności, utrzymuje funkcjonowanie instytucji, ciągłość usług publicznych, systemy dowodzenia, łączności i komunikowania się z obywatelami.

Cyberprzestrzeń jest w tym kontekście obszarem, w którym splatają się różne wymiary aktywności ludzi, organizacji i państw, które mogą być i są atrakcyjnym celem ataku. To w cyfrowej domenie zapadają decyzje, przepływają płatności, sterowane są sieci energetyczne i wodociągowe, koordynowane działania zbrojne i prowadzone kampanie wpływu. Dlatego cyberbezpieczeństwo należy traktować jako warunek brzegowy suwerennego działania państwa – warstwę, bez której pozostałe aspekty odporności tracą fundament.

Z tego punktu widzenia warto odwrócić utarty tok myślenia. Cyberbezpieczeństwo bywa wciąż jeszcze bowiem traktowane jako koszt, pozycja w budżecie, którą minimalizuje się do poziomu „akceptowalnego ryzyka". Tymczasem dla państwa położonego w trudnym otoczeniu geostrategicznym jest ono oczywiście warunkiem odporności, ale powinno być też traktowane jako akcelerator rozwoju gospodarczego. Te same inwestycje, które chronią systemy, budują zarazem kompetencje, rynek technologii, cyfrowy przemysł i zdolność innowacyjną. Nie powinniśmy więc pytać, ile musimy wydać na cyberbezpieczeństwo, lecz jak wykorzystać presję strategiczną i niezbędne wydatki, jako dźwignię budowy państwa zdolnego do działania i konkurowania.

Polska perspektywa: ciągłość państwa pod stałą presją

Polska prowadzi tę debatę w warunkach, których większość państw zachodnich nie doświadcza w tak bezpośredni sposób. Za naszą wschodnią granicą trwa wojna, a kraj jest celem nieprzerwanej presji poniżej progu konwencjonalnego konfliktu. W tym środowisku bezpieczeństwo cyberprzestrzeni nie jest abstrakcją, lecz jednym z podstawowych wymiarów bezpieczeństwa narodowego, a stawką jest codziennie ciągłość działania państwa. Administracja publiczna, system finansowy, sieci energetyczne, wodociągi, transport, ochrona zdrowia i systemy łączności opierają się dziś na cyfrowych technologiach, których awaria -przypadkowa lub wywołana przez przeciwnika – natychmiast przekłada się na świat fizyczny. Infrastruktura krytyczna jest przy tym coraz silniej zintegrowana, a pojedynczy udany atak na dostawcę usług współdzielonych może kaskadowo dotknąć tysiące podmiotów.

Podkreślenia wymaga, iż silna presja pod jaką funkcjonuje nasz kraj nie ma charakteru czasowego, a wrogie działania to nie pojedyncze incydenty, lecz nieprzerwane tło funkcjonowania państwa – sondowanie słabości, testowanie procedur reagowania i przyzwyczajanie opinii publicznej do stałego napięcia. W takim środowisku odporność nie jest stanem, który raz się osiąga, lecz procesem, który wymaga nieustannego, rosnącego zaangażowania. To z kolei musi zmieniać logikę inwestycji, w których nie chodzi o jednorazowy zakup systemów zabezpieczeń, lecz o trwałe utrzymanie kadr, procesów i technologii zdolnych działać również wtedy, gdy część systemu zawiedzie. Państwo odporne to państwo, które zakłada, że incydent nastąpi i projektuje swoją architekturę tak, aby mimo tego zachować zdolność do działania i zaufanie obywateli. Ważnych jest w tym kontekście wiele czynników, od redundantnej łączności, przez plany ciągłości działania, po zdolność szybkiego odtwarzania usług krytycznych.

Warto jednak przy tym pamiętać, że cyberprzestrzeń nie jest wyłącznie przestrzenią zagrożeń. Jest również środowiskiem innowacyjności, kreatywności i intensywnej komercjalizacji osiągnięć naukowych. W tym sensie bezpieczeństwo, rozwój i suwerenność technologiczna są ze sobą nierozerwalnie splecione, a państwo, które potrafi rozpoznać zagrożenia, zorganizować odpowiedź instytucjonalną i uruchomić potencjał nauki oraz biznesu, może przekuć presję strategiczną w przewagę rozwojową. To właśnie ten dwoisty charakter cyberprzestrzeni, jako domeny ryzyka i szansy sprawia, że jej bezpieczeństwo powinno się traktować jako jedną z horyzontalnych polityk państwowych.

Unijne ramy prawne wyznaczają tu kierunek, który może stać się swoista pułapką. Dyrektywa NIS2 podnosi wymagania wobec podmiotów kluczowych i ważnych w kilkunastu sektorach, nakłada obowiązki w zakresie zarządzania ryzykiem i zgłaszania incydentów oraz wprost wiąże odpowiedzialność za cyberbezpieczeństwo z kierownictwem organizacji. To istotne minimum, lecz minimum właśnie. Realna odporność i rozwojowa dźwignia może powstać wtedy, gdy państwo nie zatrzymuje się na regulacyjnej zgodności, ale sięga dalej ku samodzielnemu budowaniu odporności, także wówczas, gdy dostęp do zewnętrznych technologii lub usług zostanie ograniczony. Zgodność to punkt wyjścia, celem jest w tym przypadku mierzalne spektrum zdolności.

Cyberbezpieczeństwo jako inwestycja rozwojowa

Jeśli przyjąć, że odporność wymaga krajowej zdolności, to wydatki na cyberbezpieczeństwo przestają być wyłącznie kosztem ochrony, a stają się inwestycją

o wymiernym zwrocie rozwojowym. Każda złotówka skierowana na zabezpieczenie systemów może jednocześnie finansować kompetencje, popyt na rozwiązania, rozwój firm i działalność badawczo-rozwojową, ale pod warunkiem, że jest wydawana świadomie. Analizy Banku Światowego wskazują, że gotowość w obszarze cyberbezpieczeństwa przynosi korzyści wykraczające poza samą redukcję strat. Sprzyja bowiem zaufaniu, inwestycjom i rozwojowi rynku usług cyfrowych. Cyberbezpieczeństwo ma więc charakter czynnika rozwojowego, a nie tylko swoistego ubezpieczenia.

Pierwszym i najcenniejszym aktywem są kompetencje. Specjaliści szkoleni do obrony kluczowych systemów to ten sam kapitał ludzki, który tworzy oprogramowanie, projektuje bezpieczną architekturę rozwiązań i zakłada innowacyjne firmy technologiczne. Polska ma tu wyróżniający się w skali świata potencjał – polskie zespoły regularnie plasują się w czołówce międzynarodowych ćwiczeń i zawodów z zakresu cyberobrony, a krajowe talenty inżynierskie współtworzą globalne firmy technologiczne. Problem nie leży w braku talentu, lecz w tym, że zbyt często wartość zbudowana na polskich kompetencjach materializuje się poza Polską. Inwestycje państwa w cyberbezpieczeństwo muszą być zatem przede wszystkim tak profilowane, aby zapewnić, że ten kapitał ludzki będzie budował wartość w kraju.

Drugim wymiarem jest rynek. Popyt państwa i sektora publicznego na rozwiązania bezpieczeństwa może uruchomić cały łańcuch wartości – od oprogramowania, przez sprzęt i usługi, po badania i certyfikację. Wiele z tych technologii ma charakter podwójnego zastosowania, jak kryptografia, bezpieczna łączność czy systemy wykrywania zagrożeń. Świadomie prowadzona polityka pozwala, by wydatki na bezpieczeństwo narodowe stawały się zarazem akceleratorem cyfrowego przemysłu. Doświadczenia partnerów pokazują, że jest to realne, a wiele krajów sojuszniczych konsekwentnie wiąże wzmacnianie bezpieczeństwa cyberprzestrzeni z rozwojem własnego sektora cyberbezpieczeństwa, traktując go jako rosnącą gałąź gospodarki, a nie wyłącznie obciążenie budżetu.

Trzecim wymiarem jest zaufanie, a więc zasób, który trudno wycenić, lecz bez którego gospodarka cyfrowa nie urośnie. Bezpieczeństwo systemów przekłada się wprost na skłonność obywateli do korzystania z e-usług, na gotowość firm do cyfryzacji procesów i na decyzje inwestorów o lokowaniu kapitału. Tam, gdzie zaufanie do przestrzeni cyfrowej jest wysokie, taniej i szybciej powstają nowe usługi i modele biznesowe, zaś tam, gdzie jest niskie, każda innowacja napotyka opory i koszty. W tym sensie cyberbezpieczeństwo działa jak infrastruktura zaufania – niewidoczna, gdy

funkcjonuje, lecz nieodzowna dla całej nadbudowy gospodarczej. Inwestycja w ten obszar to zatem wzmocnienie dla przepustowości całej cyfrowej gospodarki.

Państwo jako inteligentny zamawiający i organizator rynku

Aby cyberbezpieczeństwo stało się akceleratorem rozwoju, państwo musi przyjąć rolę inteligentnego zamawiającego, czyli nie biernego nabywcy gotowych produktów „z półki", lecz świadomego organizatora rynku, który potrafi formułować wymagania, dzielić ryzyko i nagradzać rozwój krajowych zdolności. Zamówienia z szeroko rozumianego sektora publicznego są tu najpotężniejszym dostępnym narzędziem polityki przemysłowej. Sposób, w jaki państwo kupuje, decyduje o tym, czy w kraju powstaje rynek dla rodzimych rozwiązań, czy też strumień publicznych środków zasila wyłącznie dostawców zewnętrznych.

Praktyczne instrumenty są znane, kluczowe jest w tych procesach jedno – umiejętne łączenie świata zamawiających z dostawcami. Przede wszystkim sektor obronny, dysponujący zarówno finansowaniem plasującym Polskę na pierwszym miejscu w NATO pod względem wydatków obronnych liczonych jako procent PKB, a także mierzący się z realnymi wyzwaniami bezpieczeństwa, musi nauczyć się wreszcie komunikować rynkowi swoje rzeczywiste potrzeby, zamiast ukrywać je za tajemnicą i zamkniętymi procedurami. Tam bowiem, gdzie ta komunikacja zawodzi, rynek nie potrafi odpowiedzieć, nawet jeśli dysponuje kompetencjami. Doświadczenie państw, które zbudowały silny przemysł cyberbezpieczeństwa, pokazuje, że decydujące jest sprzężenie trzech środowisk: wojska jako wymagającego i wiarygodnego odbiorcy, biznesu jako wykonawcy zdolnego skalować rozwiązania oraz nauki jako źródła przewag technologicznych. Tam, gdzie te trzy światy współpracują, kompetencje wypracowane na potrzeby obronności zasilają rynek komercyjny, a rozwiązania komercyjne wracają do sektora bezpieczeństwa już sprawdzone w boju. To mechanizm, którego Polsce wciąż brakuje, mimo że dysponuje wszystkimi jego składnikami z osobna.

Rola inteligentnego zamawiającego wymaga jednak od państwa kompetencji, których biurokracja domyślnie nie posiada. Trzeba umieć ocenić ryzyko technologiczne, zaprojektować pilotaż, który nie kończy się efektowną demonstracją bez wdrożenia oraz utrzymać zdolność do dialogu z rynkiem. Trzeba także zaakceptować, że część

projektów rozwojowych zakończy się niepowodzeniem i że jest to wkalkulowane w koszt budowy zdolności, a nie dowód marnotrawstwa. Państwa, które skutecznie stymulują postęp technologiczny, działają w tym systemie jak aktywny gracz, a nie wyłącznie sponsor. Wykorzystują zamówienia, zlecenia i funkcje regulacyjne do kształtowania rynków i nadawania kierunku rozwojowi. Bez takiej postawy nawet hojne finansowanie zamienia się w serię odrębnych grantów, po których nie zostaje trwała zdolność.

Technologie następnej generacji – Polska wobec rewolucji kwantowej

Po rewolucji sztucznej inteligencji na horyzoncie rysuje się kolejna zasadnicza fala zmiany technologicznej – technologie kwantowe. Nie należy traktować ich jako odległej ciekawostki naukowej ani tematu zarezerwowanego dla kilku mocarstw. To obszar, w którym w najbliższych latach będą rozstrzygały się kwestie bezpieczeństwa komunikacji i systemów finansowych, przewagi przemysłowej i pozycji w najbardziej zaawansowanych łańcuchach wartości. Polska, ze względu na swoje kompetencje nie powinna jedynie uczestniczyć w tej zmianie. Powinniśmy stawiać sobie cel ambitniejszy – znaleźć się w gronie państw współtworzących jej standardy, zastosowania i praktyczne wdrożenia.

Doświadczenie sztucznej inteligencji pokazuje, jak istotne znaczenie w cyfrowym wyścigu ma nie tylko zasób intelektualny, ale też twarda siła, mierzona mocą infrastruktury obliczeniowej i dostępem do źródeł energii. W tym obszarze cała Europa znajduje się dziś w trudniejszej pozycji niż Stany Zjednoczone i Azja. Kontynent ma ograniczoną podaż taniej i stabilnej energii, a jego pozycję dodatkowo osłabia dogmatyczna polityka klimatyczna, która utrudnia budowę energochłonnej infrastruktury nowej generacji. Nie oznacza to rezygnacji z ambicji w AI. Przeciwnie, szanse nadal istnieją i powinny być wykorzystywane, nad czym pracujemy w ramach szeroko rozumianego środowiska technologicznego. Jednak właśnie dlatego, że w AI punkt startu Europy, a co za tym idzie także Polski jest trudny, obszar technologii kwantowych powinien zostać potraktowany jako strategiczna lekcja – nie wolno wejść w kolejną rewolucję z opóźnieniem.

W cyberbezpieczeństwie najpilniejszym wymiarem tej nadchodzącej rewolucji jest z pewnością kryptografia. Rozwój komputerów kwantowych zagraża podstawom

współczesnego szyfrowania, na którym opiera się poufność łączności, podpisy cyfrowe, systemy bankowe i identyfikacyjne. Zagrożenie ma przy tym charakter wyprzedzający – dane przechwycone i przechowywane dziś mogą zostać odszyfrowane w przyszłości („zbieraj teraz, odszyfruj później"). Dlatego migracja kryptograficzna jest zadaniem na teraz, a nie dopiero na czas upowszechnienia się intensywnie wypracowywanej technologii.

Pierwszą odpowiedzią jest kryptografia postkwantowa (PQC), czyli algorytmy odporne na atak kwantowy, działające na istniejącym sprzęcie i możliwe do wdrażania w administracji, infrastrukturze krytycznej i gospodarce. W 2024 r. amerykański NIST sfinalizował pierwsze trzy standardy szyfrowania postkwantowego i zachęcił administratorów systemów do możliwie szybkiej migracji. Taki harmonogram instytucji publicznych określono już w USA. Dla Polski powinno to oznaczać konkretne zadanie polegające na inwentaryzacji systemów wykorzystujących wrażliwą kryptografię i przygotowanie planu migracji kluczowych sektorów do standardów odpornych kwantowo.

Drugim obszarem jest kwantowa dystrybucja klucza (QKD), wykorzystująca prawa fizyki do ustalania kluczy szyfrujących. Nie jest to cudowna recepta ani uniwersalny zamiennik klasycznej kryptografii. Amerykańska NSA wskazuje jej ograniczenia: wysokie koszty, konieczność zapewnienia dedykowanej infrastruktury, trudności z uwierzytelnianiem, ryzyko związane z węzłami pośredniczącymi i zależność bezpieczeństwa od jakości implementacji. Jednocześnie NATO prowadzi i opisuje projekty dotyczące zarówno kryptografii postkwantowej, jak i kwantowej dystrybucji klucza, traktując technologie kwantowe jako obszar przyszłej odporności komunikacyjnej Sojuszu. Na dziś, praktycznie wnioskować można byłoby więc, iż PQC powinna stać się priorytetem migracyjnym, a QKD obszarem pilotaży, prac rozwojowych i wybranych zastosowań wysokiego zaufania.

Szczególnie ważne jest to, że technologie kwantowe mogą połączyć potrzeby różnych sektorów państwa i gospodarki. Bezpieczna komunikacja, kryptografia, zarządzanie kluczami, odporność centrów danych, ochrona transakcji i długoterminowa poufność danych są przedmiotem wspólnego zainteresowania wojska, administracji, sektora finansowego, operatorów infrastruktury krytycznej i przemysłu technologicznego. To naturalny obszar synergii, w którym rozwiązania rozwijane dla obronności mogą wzmacniać bankowość i rynek kapitałowy, a standardy oraz kompetencje budowane w sektorze finansowym mogą podnosić odporność państwa. Polska powinna dążyć do tego, aby programy kwantowego cyberbezpieczeństwa nie były rozproszone między instytucjami, lecz projektowane jako wspólna agenda bezpieczeństwa i rozwoju.

Realistyczne podejście do technologii kwantowych nie oznacza więc ostrożności rozumianej jako bierność. Oznacza koncentrację na zdolnościach, które mogą tworzyć krajowy rynek technologii wysokiego zaufania zwłaszcza w dziedzinach podwójnego zastosowania. Jeśli Polska chce traktować cyberbezpieczeństwo jako akcelerator rozwoju, powinna uznać technologie kwantowe za jeden z tych obszarów, w których ambicją nie jest nadążanie za liderami, lecz wejście do ich grona.

Polska luka wykonawcza

Polska dysponuje zasobami, talentami i położeniem, które wprost wymuszają ambicję. Jest jedną z największych gospodarek świata i jak już wspomniano – liderem NATO pod względem wydatków obronnych w relacji do PKB, ma rozbudowany ekosystem cyberbezpieczeństwa w resorcie obrony, wyróżniające się w skali globalnej kadry eksperckie oraz liczną populację studentów kierunków technicznych. Krótko mówiąc – ma wszystkie składniki sukcesu z osobna. Brakuje natomiast tego, co łączy je w działającą całość.

Lukę najlepiej opisać jako wykonawczą, nie zasobową. Po pierwsze, brakuje spójnego mechanizmu koordynacji, a zatem instytucji i procesów zdolnych tworzyć strategie, a następnie przekładać je na trwałe zdolności w wieloletniej perspektywie. Po drugie, brakuje rynku dla krajowych rozwiązań, niestety popyt strategiczny państwa na polskie technologie jest zbyt słaby, by uruchomić skalę, a dominującym modelem kooperacji z rynkiem technologicznym jest zakup gotowych rozwiązań od globalnych korporacji, zamiast kreowania nowych wspólnie z polskimi przedsiębiorcami. Po trzecie, brakuje kapitału zdolnego skalować rozwój i zapewniać finansowanie wzrostu, które utrzymałoby krajowych liderów w Polsce, zamiast wypychać ich do zagranicznych jurysdykcji i funduszy. Po czwarte, system badawczo-rozwojowy jest rozproszony i słabo powiązany z rynkiem. I wreszcie – brakuje rutynowej współpracy na linii wojsko–biznes–nauka, bez której kompetencje obronne nie zasilają gospodarki, a innowacje cywilne nie wzmacniają obronności.

Konsekwencje tej luki widać w powtarzalnym wzorcu polskiej historii technologicznej, w której realne przewagi – od pionierskiego oprogramowania, przez sprzęt komputerowy, po zaawansowane materiały – nie zostały przekute w trwały sukces gospodarczy, najczęściej z powodu braku długofalowej polityki, kapitału i poprawnego ładu korporacyjnego, a nie ze względu na brak pomysłu. Dziś polskie talenty

budują firmy o globalnej skali, lecz robią to w innych ekosystemach. Bariera leży więc w jakości ekosystemu i polityce państwa, jest więc możliwy do naprawienia.

Konkluzja: cyberbezpieczeństwo jako nowa infrastruktura rozwoju

O cyberbezpieczeństwie warto myśleć jak o infrastrukturze, analogicznie do dróg, sieci energetycznych czy kolei, którą buduje się obligatoryjnie, gdyż bez niej gospodarka nie działa, a z nią rośnie. Tak samo cyberbezpieczeństwo jest w dzisiejszym coraz bardziej cyfrowym świecie warunkiem koniecznym ciągłości działania państwa pod presją oraz zdolności gospodarki do innowacji i konkurowania. To nowa infrastruktura rozwoju, a nie pozycja kosztowa do ograniczenia.

Trudne otoczenie geostrategiczne, które bywa traktowane jak obciążenie, jest zarazem najsilniejszym bodźcem do budowy zdolności. Wymaga to świadomego zamawiania, rynku dla krajowych rozwiązań, kapitału skalującego, sprawnego systemu B+R oraz rutynowej współpracy wojska, biznesu i nauki. Wymaga też selektywności i skupienia na technologiach o znaczeniu strategicznym, w tym np. na kryptografii postkwantowej.

Cyberbezpieczeństwo jest jednocześnie warunkiem odporności i akceleratorem rozwoju gospodarczego. Potraktowane jako inwestycja, a nie koszt, może stać się jednym z fundamentów ambicji, o której mówi tegoroczny Kongres SET – Polski silnej i sprawczej w niestabilnym świecie.

ROZDZIAŁ II.
ENERGIA

Energetyka jądrowa jako fundament bezpieczeństwa i reindustrializacji Polski

Wojciech Dąbrowski

Abstrakt:

Artykuł przedstawia energetykę jądrową jako strategiczny fundament bezpieczeństwa energetycznego i reindustrializacji Polski. Autor analizuje wyzwania polskiego systemu elektroenergetycznego: rosnący udział OZE, potrzebę mocy dyspozycyjnych i konieczność uniezależnienia się od paliw importowanych. Wskazuje na atom jako rozwiązanie zdolne zagwarantować stabilność dostaw, niskie koszty operacyjne w długim horyzoncie i niezależność od geopolitycznych wahań cen surowców. Podkreśla znaczenie energetyki jądrowej dla reindustrializacji i budowy polskich kompetencji technologicznych.

Słowa kluczowe: energetyka jądrowa, bezpieczeństwo energetyczne, OZE, reindustrializacja, system elektroenergetyczny, niezależność energetyczna

Energetyka jądrowa nie powinna być w Polsce postrzegana wyłącznie jako jedna z wielu technologii wytwarzania energii elektrycznej. W debacie publicznej zbyt często sprowadza się ją do prostego porównania kosztów produkcji jednej megawatogodziny albo do pytania, czy atom ma zastąpić energetykę węglową w procesie dekarbonizacji ? Takie ujęcie jest zbyt wąskie. W rzeczywistości energetyka jądrowa jest jednocześnie narzędziem bezpieczeństwa, instrumentem polityki gospodarczej, elementem odporności państwa na kryzysy oraz jednym z najważniejszych projektów modernizacyjnych, jakie Polska może podjąć w najbliższych dekadach. Energia nie jest bowiem zwykłym towarem, który można zastąpić dowolnym innym produktem kupionym na rynku. Jest warunkiem operacyjnym funkcjonowania

państwa, przemysłu, administracji, transportu, rolnictwa, obronności i codziennego życia obywateli.

Z perspektywy Polski kluczowe jest utrzymanie działalności gospodarki w sposób ciągły, przewidywalny i odporny na szoki zewnętrzne. Dyskusja o miksie energetycznym jest ważna, ale nie może przesłaniać celu nadrzędnego: państwo musi mieć dostęp do stabilnej, dostępnej cenowo i niezależnej od pogody energii. To nie jest wyłącznie kwestia środowiskowa . To fundament konkurencyjności gospodarki. Jeżeli energia jest droga, niestabilna albo zależna od czynników, których państwo nie kontroluje, osłabia to przemysł, zniechęca inwestorów, podnosi koszty życia i ogranicza zdolność do prowadzenia samodzielnej polityki rozwojowej. Dlatego energetyka musi być traktowana jako obszar strategiczny, a nie wyłącznie sektor rynkowy.

Polski system elektroenergetyczny przez dekady opierał się na dużych elektrowniach konwencjonalnych, które zapewniały stabilną produkcję energii w sposób ciągły. Ich znaczenie nie polegało jedynie na samej mocy wytwórczej. Duże jednostki systemowe dawały także bezwładność, przewidywalność pracy sieci i odporność na nagłe wahania częstotliwości. Z punktu widzenia bezpieczeństwa systemu elektroenergetycznego ma to znaczenie zasadnicze, ponieważ ryzyko blackoutu nie wynika wyłącznie z braku energii w ujęciu rocznym. Może pojawić się wtedy, gdy system w konkretnym momencie nie jest w stanie zbilansować podaży i popytu, utrzymać parametrów pracy sieci oraz szybko zareagować na nagłe zakłócenia.

W ostatnich latach w Polsce znacząco wzrósł udział odnawialnych źródeł energii. OZE dostarczają energię bezemisyjną na etapie produkcji i są ważnym elementem dla modernizacji energetyki . Nie można jednak prowadzić odpowiedzialnej polityki energetycznej, opierając się wyłącznie na prostym haśle ich dalszego rozwoju. Rzeczywiste koszty budowy i funkcjonowania systemu opartego na dużym udziale źródeł zależnych od pogody są znacznie wyższe niż jednostkowy koszt wytworzenia megawatogodziny, często przywoływany w mediach jako dowód na stawianą tezę, że energia z OZE jest najtańsza . Do tego rachunku trzeba doliczyć koszty rozbudowy sieci, przyłączeń, magazynowania, usług systemowych oraz przede wszystkim bilansowania produkcji w źródłach dyspozycyjnych. Jeżeli te koszty są pomijane, debata staje się niepełna i prowadzi do błędnych wniosków i jest wręcz nieprawdziwa.

System elektroenergetyczny musi dziś radzić sobie z dwoma przeciwstawnymi ryzykami. Z jednej strony występują okresy nadprodukcji energii z OZE, kiedy energia jest dostępna, lecz system nie zawsze jest w stanie ją w pełni wykorzystać. Z drugiej

strony pojawiają się okresy, gdy nie wieje wiatr i nie świeci słońce, a zapotrzebowanie gospodarki pozostaje niezmienne. Wtedy konieczne są źródła stabilne, które mogą dostarczyć energię niezależnie od warunków atmosferycznych. Oznacza to, że sama rozbudowa OZE nie rozwiązuje problemu bezpieczeństwa energetycznego a nawet zwiększa koszty systemowe, jeżeli nie towarzyszy jej równoległy rozwój mocy dyspozycyjnych, infrastruktury sieciowej oraz mechanizmów stabilizacji w tym magazynów energii, które też są kosztochłonne.

Dlatego najważniejsze pytanie nie brzmi dzisiaj wyłącznie: jak rozwijać odnawialne źródła energii? To zadanie pozostaje w dużej mierze domeną bieżącej polityki państwa i regulacji europejskich. Pytanie strategiczne jest inne: jak zabezpieczyć system przed ryzykiem niedoboru energii, wysokimi kosztami back-upowania OZE oraz utratą konkurencyjności gospodarki? Polska potrzebuje cen energii, które będą akceptowalne społecznie i konkurencyjne dla przemysłu. Bez tego nie będzie reindustrializacji, nie będzie nowych inwestycji, nie będzie silnego sektora prywatnego i nie będzie realnej suwerenności gospodarczej. Państwo, które nie zapewnia własnych potrzeb energetycznych, staje się zależne od zewnętrznych dostawców, zewnętrznych regulacji i zewnętrznych kryzysów.

W Europie rolę stabilizatora transformacji energetycznej często przypisuje się elektrowniom gazowym. Gaz według aktualnych założeń energetycznej polityki Unii Europejskiej ma być paliwem przejściowym, które uzupełnia produkcję ze źródeł odnawialnych wtedy, gdy OZE nie dostarczają wystarczającej ilości energii. Jednak doświadczenia ostatnich lat pokazują, że oparcie bezpieczeństwa energetycznego na paliwie importowanym wiąże się z poważnym ryzykiem. Kryzysy geopolityczne, konflikty w rejonach kluczowych szlaków transportowych, napięcia wokół cieśnin ostatnio Ormuz i infrastruktury przesyłowej oraz gwałtowne zmiany cen paliw pokazują, że dostępność gazu i jego cena nie są dane raz na zawsze. Kierunek gazowy może więc pełnić funkcję uzupełniającą, ale nie rozwiązuje problemu strategicznego: ciągłości dostaw i przewidywalności kosztów w długim horyzoncie.

Zasadniczym problemem Polski nie jest wyłącznie dostępność paliw i energii w sensie technicznym. Równie ważna jest ciągłość dostaw oraz przewidywalność cen. Gospodarka nie może funkcjonować w warunkach ciągłej niepewności co do kosztów energii. Przedsiębiorca podejmujący decyzję o inwestycji musi wiedzieć, że przez kolejne lata będzie miał dostęp do energii w cenie pozwalającej konkurować z firmami z innych państw. Przemysł energochłonny, sektor chemiczny, hutnictwo, produkcja materiałów budowlanych, centra danych, transport i nowoczesne

technologie wymagają stabilnych warunków. Bez nich inwestycje odpływają, a państwo traci zdolność budowania własnego potencjału przemysłowego.

W tym kontekście energetyka jądrowa staje się dla Polski rozwiązaniem kluczowym. Jej rola nie sprowadza się wyłącznie do zastąpienia wysokoemisyjnych bloków węglowych w przyszłości, choć taki efekt również jest istotny. Najważniejsze jest to, że atom dostarcza moc ciągłą, niezależną od pogody i odporną na krótkoterminowe wahania cen paliw. Elektrownia jądrowa pracuje w podstawie systemu, zapewniając stabilny fundament dla pozostałych technologii. Może współistnieć z OZE, ale jednocześnie zmniejsza skalę ryzyka związanego z ich zmiennością. Daje systemowi elektroenergetycznemu kręgosłup, którego nie można zbudować wyłącznie na źródłach zależnych od pogody.

Szczególne znaczenie ma także charakter paliwa jądrowego. W przeciwieństwie do gazu czy węgla, paliwo jądrowe stanowi maksymalnie do 15% części całkowitego kosztu inwestycji, a jego zapasy można planować z dużym wyprzedzeniem. Oznacza to większą odporność na gwałtowne szoki cenowe na rynkach paliw. Zakup paliwa i jego wykorzystanie w długim cyklu pracy elektrowni daje stabilność kosztową, której nie zapewniają paliwa kopalne importowane w dużych wolumenach. Energetyka jądrowa nie eliminuje wszystkich ryzyk, ale znacząco zmniejsza zależność od bieżących wahań rynkowych i politycznych.

Atom ma również ogromne znaczenie gospodarcze. Budowa elektrowni jądrowych to projekt infrastrukturalny, technologiczny i przemysłowy o skali wykraczającej poza sektor energetyczny. Daje długoterminowe gwarancje systemowe dla inwestorów, wzmacnia bezpieczeństwo dostaw energii i tworzy warunki do rozwoju nowoczesnego przemysłu. Może stać się impulsem dla polskich firm, uczelni, instytutów badawczych i ośrodków szkoleniowych. Program jądrowy wymaga kadr technicznych, inżynierów, specjalistów od materiałów, automatyki, cyberbezpieczeństwa, logistyki, prawa, finansów i zarządzania wielkimi projektami. Właśnie dlatego powinien być traktowany jako strategiczny projekt narodowy, a nie wyłącznie inwestycja energetyczna.

Energetyka jądrowa jest również narzędziem polityki międzynarodowej. Ze względu na kosztochłonność programu, wysoki poziom technologiczny i ograniczony krąg państw oraz firm posiadających kompetencje w tym obszarze, wybór partnera do budowy elektrowni jądrowej oznacza wejście w relację strategiczną na dziesięciolecia. Nie jest to zwykły zakup technologii. To partnerstwo obejmujące finansowanie, serwis, szkolenie kadr, dostawy paliwa, standardy bezpieczeństwa, współpracę regulacyjną i często szersze relacje polityczne. Dlatego decyzje w tym

obszarze muszą być podejmowane nie tylko na podstawie ceny, lecz także z perspektywy suwerenności, bezpieczeństwa i długofalowych interesów państwa.

Skuteczna realizacja programu jądrowego wymaga odwagi, determinacji oraz sprawnego państwa. Polska nie może być wyłącznie biernym odbiorcą technologii. Powinna przejść do roli aktywnego, sprawczego inwestora, który jasno definiuje swoje interesy, wymaga udziału krajowych firm, buduje kompetencje i dba o transfer wiedzy. Potrzebna jest szybka i stabilna legislacja, przewidywalny model finansowania, silny nadzór właścicielski, profesjonalne zarządzanie projektem oraz konsekwencja niezależna od cyklu wyborczego. Program jądrowy trwa dłużej niż jedna kadencja parlamentu, dlatego musi być chroniony przed doraźnością polityczną.

W tym miejscu warto zwrócić uwagę na szerszy kontekst europejski. Unia Europejska stała się w wielu obszarach fabryką dyrektyw, regulacji i obowiązków, które często miały przyspieszać transformację, lecz w praktyce doprowadziły do przeregulowania i utraty konkurencyjności. Systemy takie jak ETS, ETS 2, regulacje dotyczące efektywności energetycznej czy wymogi dyrektywy budynkowej EPBD wpływają na koszty funkcjonowania przedsiębiorstw i gospodarstw domowych. Jeżeli polityka klimatyczna jest prowadzona bez uwzględnienia realiów gospodarczych, to w konsekwencji stała się przeciw skuteczna.

Efektem jest droga energia, spadek konkurencyjności europejskiej gospodarki oraz ucieczka emisji do państw, które nie podlegają restrykcyjnym wymogom polityki klimatycznej a przede wszystkim są poza systemem handlu emisjami ETS.

Polska potrzebuje reindustrializacji, czyli odbudowy i rozwoju własnych gałęzi przemysłu. Własny przemysł to fundament, na którym można budować bezpieczeństwo gospodarcze, energetyczne, militarne, technologiczne i żywnościowe. Państwo pozbawione silnej bazy przemysłowej staje się zależne od importu, zewnętrznych łańcuchów dostaw i decyzji podejmowanych poza jego granicami. Pandemia, wojna, kryzysy surowcowe i napięcia handlowe pokazały, że globalizacja bez zabezpieczeń może być źródłem słabości. Dlatego rozwój energetyki jądrowej powinien być powiązany z polityką przemysłową, innowacyjną i edukacyjną.

W procesie reindustrializacji doniosła jest rola sektora prywatnego on jest tkanką, która daje życie gospodarce. Państwo powinno tworzyć warunki, w których sektor publiczny i prywatny wzajemnie się uzupełniają, a nie konkurują w sposób niszczący. Spółki z udziałem Skarbu Państwa i narodowi czempioni nie mogą dławić prywatnej przedsiębiorczości ani pełnić wyłącznie funkcji „dojnych krów" dla budżetu. Muszą inwestować, rozwijać kompetencje, budować ekspansję zagraniczną, wspierać

innowacje i tworzyć przestrzeń dla mniejszych firm w łańcuchach dostaw. Program jądrowy daje tu wyjątkową szansę: może stać się platformą współpracy między dużymi podmiotami, polskimi przedsiębiorstwami, uczelniami i start-upami technologicznymi.

Warunkiem sukcesu jest jednak polonizacja kompetencji, a nie jedynie montaż importowanej technologii. Polska powinna szukać partnerów gotowych dzielić się know-how, tworzyć lokalne zaplecze serwisowe, rozwijać kształcenie specjalistów i budować krajową własność intelektualną. Nie chodzi o autarkię ani udawanie, że wszystko można wykonać samodzielnie. Chodzi o to, aby wielki projekt infrastrukturalny zostawił w Polsce trwałe kompetencje, nowe firmy, patenty, laboratoria, kierunki studiów i zdolność eksportu usług. Inwestycje powinny koncentrować się tam, gdzie powstaje wiedza, technologia oraz możliwość komercjalizacji.

Potrzebna jest także strategia rozwoju innowacji, która będzie realnie mierzona, a nie oparta wyłącznie na hasłach. Polska powinna wzmacniać ośrodki badawczo-rozwojowe, wspierać projekty o wysokiej szansie komercjalizacji i tworzyć mechanizmy finansowania dla technologii istotnych z punktu widzenia suwerenności państwa. Najważniejsze jest jednak, aby środki publiczne były wydawane transparentnie i prowadziły do powstawania realnych zdolności, a nie jedynie do finansowania kolejnych programów bez efektu rynkowego.

Energetyka jądrowa może być osią tak rozumianej modernizacji. Daje energię stabilną, bezemisyjną i przewidywalną kosztowo. Wzmacnia pozycję państwa w relacjach międzynarodowych. Tworzy podstawy dla rozwoju przemysłu, nauki i innowacji. Zwiększa odporność na kryzysy paliwowe, gospodarcze i geopolityczne. Pozwala również ograniczyć presję kosztową wynikającą z konieczności utrzymywania coraz bardziej skomplikowanego systemu bilansowania źródeł odnawialnych. Nie jest rozwiązaniem wszystkich problemów, ale jest jednym z niewielu narzędzi, które jednocześnie odpowiadają na problem bezpieczeństwa energetycznego, konkurencyjności gospodarki i suwerenności strategicznej.

Dlatego Polska powinna traktować program jądrowy jako projekt państwowy najwyższej rangi. Nie wystarczy deklarować poparcia dla atomu. Potrzebne są decyzje, harmonogramy, odpowiedzialność, stabilne finansowanie i konsekwencja. Państwo musi działać szybko, ambitnie i profesjonalnie z otwarciem na partnerów zagranicznych, ale z jasno określonym interesem narodowym. Energetyka jądrowa to nie tylko elektrownie. To wybór modelu rozwoju państwa: czy Polska chce być gospodarką zależną od importowanych technologii, drogich paliw i zewnętrznych regulacji, czy też państwem budującym własną odporność, własne kompetencje i własną przewagę konkurencyjną.

Podsumowując, energia jest warunkiem funkcjonowania państwa, a nie zwykłym produktem rynkowym. W świecie niestabilnych cen, napięć geopolitycznych, rosnących kosztów transformacji i ryzyka utraty konkurencyjności Polska potrzebuje stabilnego fundamentu energetycznego. Tym fundamentem powinna być energetyka jądrowa, uzupełniająca OZE i ograniczająca zależność od paliw importowanych. Atom daje bezpieczeństwo dostaw, przewidywalność, suwerenność gospodarczą, impuls technologiczny i narzędzie prowadzenia polityki międzynarodowej. Jego skuteczna realizacja wymaga odwagi, sprawczości i myślenia w kategoriach dekad, a nie kadencji parlamentu. Jeśli Polska chce zachować realną niezależność decyzyjną, program jądrowy powinien stać się jednym z centralnych projektów narodowych.

Polska hubem gazowym Europy. Gaz ziemny jako instrument niezależności energetycznej, stabilnej transformacji i regionalnego bezpieczeństwa

Paweł Majewski

Abstrakt:

Artykuł analizuje szansę Polski na rolę regionalnego hubu gazowego Europy Środkowo-Wschodniej. Autor przedstawia geopolityczny powrót gazu jako paliwa bezpieczeństwa, ocenia infrastrukturalne podstawy tej roli (Baltic Pipe, terminal LNG w Świnoujściu) i formułuje sześć warunków realizacji tej szansy. Wskazuje, że okno strategiczne jest wyjątkowo korzystne, lecz nietrwałe – wymaga szybkich decyzji i aktywnej dyplomacji energetycznej.

Słowa kluczowe: hub gazowy, gaz ziemny, bezpieczeństwo energetyczne, Baltic Pipe, LNG, Europa Środkowa, geopolityka energetyczna

Polska ma realną szansę stać się regionalnym hubem gazowym Europy Środkowo-Wschodniej, jeżeli wykorzysta równocześnie trzy przewagi: dywersyfikację dostaw, położenie geograficzne na osi północ-południe oraz rozwój instrumentów rynkowych, które pozwolą handlować gazem nie tylko fizycznie, lecz także finansowo i terminowo. Gaz ziemny nie powinien być postrzegany jako konkurencja dla energetyki jądrowej i OZE, ale jako paliwo zapewniające bezpieczeństwo, elastyczność i wsparcie dla transformacji energetyki w okresie co najmniej najbliższych dwóch dekad.

Polska polityka gazowa weszła w nową fazę. Jeszcze dekadę temu jej głównym celem było ograniczenie zależności od dostaw ze wschodu. Dziś, po uruchomieniu terminalu LNG w Świnoujściu, gazociągu Baltic Pipe, połączeń międzysystemowych z Litwą i Słowacją oraz po całkowitym odejściu od fizycznych przepływów rosyjskiego gazu przez polski system przesyłowy, punkt ciężkości przesuwa się z samej dywersyfikacji na aktywne zarządzanie regionalnym bezpieczeństwem dostaw. Polska może nie tylko zabezpieczać własne potrzeby, ale także uczestniczyć w wypełnianiu luki po gazie rosyjskim w państwach Europy Środkowo-Wschodniej.

Warunkiem powodzenia jest jednak odejście od myślenia wyłącznie infrastrukturalnego. Hub gazowy to nie tylko terminal, gazociąg, magazyn i fizyczny wolumen. To również płynny rynek hurtowy, giełda towarowa, kontrakty terminowe, transparentne reguły dostępu do przepustowości, przewidywalne taryfy, sprawne bilansowanie oraz zaufanie uczestników rynku. Bez tych elementów Polska pozostanie ważnym korytarzem przesyłowym, ale nie stanie się centrum wyceny i obrotu gazem dla regionu.

Obecne okno strategiczne jest wyjątkowo korzystne. Unia Europejska przyjęła rozporządzenie stopniowo wygaszające import rosyjskiego gazu; w najnowszym harmonogramie pełny zakaz dla LNG z Rosji ma obowiązywać od początku 2027 r., a dla gazu rurociągowego od jesieni 2027 r. [4]. Równolegle rozwija się amerykański potencjał eksportu LNG, a polskie projekty FSRU w rejonie Zatoki Gdańskiej mogą otworzyć dodatkowe wolumeny dla Czech, Słowacji, Ukrainy, Litwy i – pośrednio – Węgier. Czas jest jednak czynnikiem krytycznym: konkurencyjne terminale i korytarze dostaw, w tym południowy kierunek przez Adriatyk (chorwacki Krk), nie będą czekały na decyzje Polski.

Zasadniczy wniosek jest następujący: gaz ziemny powinien pełnić w Polsce funkcję paliwa bezpieczeństwa i elastyczności. Nie zastąpi energetyki jądrowej, nie wyprze odnawialnych źródeł energii i nie blokuje ich rozwoju, ale może stabilizować system elektroenergetyczny, przemysł i ciepłownictwo w okresie, w którym OZE są wobec niewystarczającej infrastruktury magazynowej źródłami w zasadzie w pełni zależnymi od pogody, a energetyka jądrowa pozostaje projektem przyszłości. Jednocześnie rozbudowa infrastruktury gazowej, zarówno przesyłowej jak i magazynowej, może zmienić Polskę w regionalną bramę importową LNG, co przełoży się na bezpieczeństwo, wpływy z usług przesyłowych, większą płynność rynku i utrzymanie marży handlowej w kraju.

1. Geopolityczny powrót gazu – od paliwa przejściowego do paliwa bezpieczeństwa

W europejskiej debacie energetycznej gaz ziemny przez wiele lat był opisywany przede wszystkim jako paliwo przejściowe. Miał ograniczać emisyjność energetyki opartej na węglu, ułatwiać integrację OZE i pełnić rolę pomostu do gospodarki niskoemisyjnej. Po 2022 r. ta definicja okazała się niewystarczająca. Wojna Rosji przeciwko Ukrainie pokazała, że gaz jest nie tylko surowcem energetycznym, ale także narzędziem presji politycznej, instrumentem zależności gospodarczej i elementem odporności państwa. Lokalne konflikty natychmiast generują skutki globalne: ceny gazu, ropy i LNG reagują nie tylko na realne ograniczenia podaży, lecz także na ryzyko zakłóceń szlaków morskich, napięcia na Bliskim Wschodzie, sankcje, embargo, akty sabotażu i cyberataki na infrastrukturę krytyczną.

Dla Polski wniosek jest jednoznaczny: system energetyczny nie może opierać się wyłącznie na założeniu, że surowiec będzie zawsze dostępny na rynku międzynarodowym po akceptowalnej cenie. Bezpieczeństwo wymaga fizycznego dostępu do zróżnicowanych kierunków dostaw, zapasów, własnej infrastruktury importowej, elastycznego przesyłu, magazynowania oraz zdolności do szybkiego reagowania w kryzysie. W polskich warunkach historycznie taką funkcję pełnił węgiel. W nadchodzących dwóch dekadach coraz większą rolę powinien przejmować gaz ziemny, zwłaszcza tam, gdzie potrzebna jest szybka regulacja mocy, rezerwa dla OZE i stabilne źródło dla przemysłu oraz ciepłownictwa.

Nie oznacza to prostego zastąpienia jednej zależności drugą. Sens strategii gazowej polega na połączeniu kilku elementów: po pierwsze, zdywersyfikowanego importu LNG i gazu rurociągowego spoza Rosji; po drugie, rozbudowy magazynów i sieci przesyłowej; po trzecie, utrzymywania wystarczającej elastyczności krajowych źródeł wytwórczych; po czwarte, stworzenia rynku, na którym cena gazu będzie wynikiem konkurencji i płynności. W takim modelu gaz staje się nie tylko paliwem, lecz także częścią architektury bezpieczeństwa państwa.

W tym kontekście nie należy przeciwstawiać gazu odnawialnym źródłom energii ani energetyce jądrowej. OZE są potrzebne w miksie energetycznym z punktu widzenia kosztów krańcowych, bezpieczeństwa regulacyjnego (nadal silna presja klimatyczna w UE), ale ich produkcja zależy od pogody. Energetyka jądrowa może stać się filarem stabilnych mocy podstawowych, lecz wymaga długiego horyzontu inwestycyjnego. Gaz wypełnia przestrzeń pomiędzy tymi modelami: jest elastyczny,

relatywnie szybki inwestycyjnie, możliwy do uruchamiania w okresach niedoboru generacji z wiatru i słońca, a w razie potrzeby może stabilizować system elektroenergetyczny w czasie szczytowego zapotrzebowania.

2. Gaz jako stabilizator polskiej transformacji energetycznej

Polska transformacja energetyczna jest procesem trudniejszym niż w wielu państwach Europy Zachodniej. Wynika to z historycznego znaczenia węgla w elektroenergetyce, skali zapotrzebowania przemysłu, opóźnienia inwestycji jądrowych oraz rosnącego udziału OZE, które wymagają mocy bilansujących. W takim systemie gaz może pełnić funkcję stabilizatora jako instrument bezpiecznego przejścia przez okres największej zmienności technologicznej, regulacyjnej i geopolitycznej.

Źródła gazowe mają trzy cechy szczególnie ważne z punktu widzenia systemu elektroenergetycznego. Po pierwsze, są elastyczne i mogą szybko reagować na zmiany produkcji z OZE. Po drugie, mogą ograniczać wykorzystanie najbardziej emisyjnych jednostek węglowych w okresach, gdy system wymaga stabilnej rezerwy. Po trzecie, umożliwiają budowę nowoczesnych bloków kogeneracyjnych dla ciepłownictwa, które w wielu miastach stoi przed koniecznością głębokiej modernizacji. Krajowy Dziesięcioletni Plan Rozwoju systemu przesyłowego zakłada, że popyt na usługi przesyłowe będzie rósł co najmniej do początku lat trzydziestych, przede wszystkim ze względu na zapotrzebowanie sektora elektroenergetycznego, a dopiero później może ulec stopniowemu obniżeniu wraz z rozwojem OZE i energetyki jądrowej [1].

To właśnie dlatego gaz powinien być w Polsce traktowany jako element komplementarny, a nie konkurencyjny wobec atomu i OZE. Elektrownie jądrowe zapewniają stabilną, przewidywalną produkcję, ale nie są narzędziem szybkiego bilansowania godzinowego. Farmy wiatrowe i fotowoltaika obniżają koszt energii w wielu godzinach roku, lecz wymagają magazynów energii, elastycznego popytu oraz źródeł dyspozycyjnych. Gaz może spinać te elementy, zmniejszając ryzyko przerw w dostawach i ograniczając konieczność utrzymywania starych jednostek węglowych wyłącznie z powodu bezpieczeństwa systemu.

W praktyce oznacza to potrzebę dalszych inwestycji w bloki gazowe dla energetyki zawodowej, ale także w gazowe źródła rozproszone i kogeneracyjne. Inwestycje te powinny być projektowane tak, aby były odporne na przyszłe zmiany regulacyjne:

z możliwością pracy w niższych współczynnikach wykorzystania, świadczenia usług systemowych, potencjalnego współspalania gazów zdekarbonizowanych w przyszłości oraz integracji z lokalnymi systemami ciepłowniczymi. Tylko wtedy gaz nie stanie się pułapką aktywów osieroconych, lecz narzędziem sprawnej transformacji.

3. Polska infrastruktura gazowa – od dywersyfikacji dostaw do potencjału hubowego

Największą przewagą Polski jest dziś rozbudowana infrastruktura gazowa, będąca konsekwencją trafnych decyzji strategicznych i ich konsekwentnej realizacji. Terminal LNG w Świnoujściu po rozbudowie osiągnął zdolność regazyfikacyjną do 8,3 mld m^3 rocznie, co oznacza istotny wzrost wobec początkowej przepustowości terminalu [2]. Baltic Pipe zapewnia techniczną możliwość importu gazu z kierunku norweskiego przez Danię do Polski na poziomie 10 mld m^3 rocznie [3]. Interkonektor Polska-Litwa, połączenie Polska-Słowacja oraz połączenia z systemami zachodnimi i ukraińskimi tworzą sieć, która przestaje być jednokierunkowym systemem importu, a zaczyna przypominać układ regionalnej dystrybucji i arbitrażu.

Planowany pływający terminal regazyfikacyjny FSRU w rejonie Gdańska ma zwiększyć tę przewagę. Według informacji GAZ-SYSTEM projekt FSRU obejmuje nie tylko jednostkę regazyfikacyjną, lecz także rozbudowę infrastruktury lądowej, w tym gazociągi umożliwiające wyprowadzenie paliwa w głąb kraju oraz dalej w kierunku regionu. Zakładana przepustowość pierwszej jednostki FSRU to 6,1 mld m^3 gazu po regazyfikacji rocznie, a planowany horyzont uruchomienia przypada na lata 2027/2028 [2]. Zbiega się to z momentem, w którym Europa będzie potrzebowała stabilnych alternatyw dla rosyjskiego gazu.

Dane techniczne pokazują, że Polska posiada już istotną nadwyżkę zdolności importowych względem krajowego zapotrzebowania, a jednocześnie dysponuje konkretnymi kierunkami eksportowymi. W materiałach GAZ-SYSTEM prezentowanych dla korytarzy Baltic Sea i Amber Gas Corridor wskazano m.in. importową przepustowość systemu, bez Ukrainy, na poziomie 37,3 mld m^3 rocznie oraz eksportową na poziomie 12,6 mld m^3 rocznie [3]. To nie oznacza, że każda z tych wielkości jest w każdej chwili w pełni dostępna handlowo i ekonomicznie, ale pokazuje skalę potencjału infrastrukturalnego.

Sama infrastruktura importowa jednak nie wystarczy. Hub wymaga także rozbudowanych magazynów gazu oraz gazociągów przesyłowych na osi północ-południe.

To właśnie magazyny decydują o zdolności państwa do przetrwania krótkoterminowych szoków cenowych i podażowych, a także zapewniają bezpieczeństwo na wypadek kryzysów skutkujących przerwami w dostawach. Z kolei korytarz północ-południe jest warunkiem, aby wolumeny sprowadzane przez Bałtyk nie zatrzymywały się na rynku krajowym, ale mogły realnie konkurować z dostawami z południa Europy, Adriatyku i zachodnich hubów gazowych.

4. Kierunek południowy i wschodni – Czechy, Słowacja, Ukraina, Litwa i Węgry

Największy potencjał eksportowy Polski znajduje się w kierunku południowym i wschodnim. Słowacja i Węgry przez lata były silnie związane z dostawami rosyjskimi, a ich geografia przesyłowa była dostosowana do importu ze wschodu. Dla tych państw polska infrastruktura LNG i Baltic Pipe mogą stać się alternatywną bramą dostępu do gazu spoza Rosji. Z punktu widzenia Polski oznacza to szansę na monetyzację nadwyżek infrastrukturalnych, zwiększenie wykorzystania systemu przesyłowego, wzmocnienie pozycji politycznej w regionie i utrzymanie części marży handlowej w kraju.

Połączenie Polska-Słowacja jest szczególnie ważne, ponieważ jego przepustowość w kierunku Słowacji wynosi około 4,7 mld m^3 rocznie, a w kierunku Polski około 5,7 mld m^3 rocznie [3]. W praktyce daje to Polsce możliwość oferowania gazu LNG po regazyfikacji albo gazu z kierunku norweskiego partnerom południowym. Dalej, poprzez słowacki system przesyłowy, możliwe jest pośrednie oddziaływanie na rynek węgierski. Oczywiście wymaga to konkurencyjnej ceny, odpowiednio niskich kosztów przesyłu, zdolności rezerwacji przepustowości oraz przewidywalnych regulacji.

Kierunek ukraiński ma z kolei znaczenie zarówno handlowe, jak i geopolityczne. Ukraina dysponuje dużym potencjałem magazynowym i pozostaje państwem istotnym z punktu widzenia bezpieczeństwa wschodniej flanki Europy. Zdolności przesyłowe z Polski w kierunku Ukrainy są mniejsze niż w przypadku Słowacji, ale mogą odgrywać istotną rolę w okresach kryzysowych, przy sezonowych niedoborach albo przy budowie regionalnych pakietów handlowych obejmujących LNG, przesył i magazynowanie [3]. W dłuższej perspektywie integracja ukraińskiego rynku z europejskim może dodatkowo zwiększyć znaczenie Polski jako bramy dostępu do północnego LNG.

Litwa i państwa bałtyckie tworzą osobny, ale istotny wymiar koncepcji hubowej. Interkonektor GIPL wzmacnia dwukierunkową wymianę między Polską a Litwą, a jednocześnie łączy polski system z rynkiem, który już wcześniej budował bezpieczeństwo w oparciu o terminal LNG w Kłajpedzie. W takim układzie Polska nie musi konkurować wyłącznie wolumenem. Może konkurować elastycznością, dostępem do wielu źródeł, płynnością giełdową i możliwością zawierania kontraktów o różnych profilach dostaw.

Czechy pozostają naturalnym partnerem ze względu na położenie, integrację gospodarczą i powiązanie z niemieckim oraz środkowoeuropejskim rynkiem gazu. Dla Pragi polskie terminale LNG mogą być jednym z kierunków dywersyfikacji, zwłaszcza jeżeli przepustowości z północy będą oferowane w sposób konkurencyjny wobec alternatyw zachodnich i południowych. Równocześnie trzeba pamiętać, że rynek czeski ma dostęp do infrastruktury niemieckiej, a więc Polska musi konkurować nie samą możliwością fizycznych dostaw, lecz ceną, płynnością i jakością produktu handlowego.

5. Hub to rynek, a nie tylko infrastruktura – rola TGE, taryf i regulacji

Najczęstszym błędem w debacie o hubie gazowym jest utożsamianie go wyłącznie z infrastrukturą fizyczną. Terminal LNG, FSRU, Baltic Pipe i interkonektory są warunkiem koniecznym, ale niewystarczającym. Hub powstaje dopiero wtedy, gdy uczestnicy rynku chcą zawierać transakcje w danym punkcie, gdy cena jest wiarygodna, gdy istnieje wystarczająca liczba sprzedających i kupujących, gdy kontrakty terminowe dają możliwość zabezpieczenia ryzyka, a regulacje ograniczają bariery wejścia. W tym sensie wzorem dla Europy jest holenderski TTF (Title Transfer Facility), który stał się nie tylko fizycznym punktem obrotu, lecz przede wszystkim benchmarkiem cenowym.

W Polsce naturalną instytucją dla takiej funkcji jest Towarowa Giełda Energii. Już dziś na TGE funkcjonują rynki spotowe i terminowe gazu, a dane URE za 2024 r. pokazują istotną skalę dostaw wynikających z kontraktów giełdowych [5]. Według danych TGE wolumen obrotu gazem na giełdzie w 2025 r. wzrósł do ponad 208,9 TWh, co oznaczało znaczący wzrost rok do roku [6]. To dobry punkt wyjścia, ale regionalny hub wymaga dalszego zwiększenia płynności, udziału podmiotów zagranicznych, produktów terminowych o odpowiedniej głębokości oraz zaufania, że cena z polskiego rynku może być referencyjna dla regionu.

Drugim warunkiem są taryfy przesyłowe. Jeżeli polski system ma być atrakcyjnym korytarzem importu i eksportu, koszty korzystania z infrastruktury muszą być konkurencyjne względem alternatywnych tras. Zwiększenie wykorzystania systemu przesyłowego może w dłuższym okresie działać na korzyść wszystkich odbiorców, ponieważ większy wolumen usług pozwala rozłożyć koszty stałe infrastruktury na większą liczbę jednostek energii. Nie jest to jednak mechanizm automatyczny. Wymaga ostrożnego projektowania taryf, tak aby z jednej strony zapewniały zwrot z inwestycji, a z drugiej nie zniechęcały zagranicznych partnerów handlowych do rezerwowania przepustowości przez Polskę.

Trzecim warunkiem jest rola regulatora i administracji. Ministerstwo odpowiedzialne za energię powinno wyznaczać kierunek strategiczny, URE zapewniać przewidywalność regulacyjną, GAZ-SYSTEM rozwijać i udostępniać infrastrukturę, Orlen wykorzystywać swoje kompetencje zakupowe i portfel kontraktów, a TGE tworzyć transparentną platformę obrotu. Jednocześnie dominująca pozycja Orlenu po połączeniu z PGNiG wymaga równowagi: z jednej strony duży podmiot może zabezpieczać wolumeny, kontrakty i ryzyko portfelowe, z drugiej – należy pamiętać, że ze względu na regulacje prawne UE hub potrzebuje konkurencji, dostępu dla niezależnych traderów i ograniczenia barier wejścia. Analizy rynkowe wskazywały, że udział Orlenu/PGNiG w polskim rynku pozostawał bardzo wysoki, sięgając około 85% w wybranych segmentach obrotu [7]. To siła negocjacyjna, ale także wyzwanie dla liberalizacji rynku.

Ostatecznie polski hub gazowy powinien być projektowany jako ekosystem. Składają się na niego: fizyczne przepustowości, magazyny, produkty giełdowe, przejrzyste taryfy, reguły bilansowania, rozliczenia finansowe, cyberbezpieczeństwo, standardy kontraktowe i aktywna dyplomacja energetyczna. Brak któregokolwiek z tych elementów nie przekreśla projektu, ale obniża jego wartość. Polska może mieć rury i terminale, a jednocześnie przegrać konkurencję o funkcję cenotwórczą, jeżeli handel będzie odbywał się gdzie indziej.

6. Okno regulacyjne UE i amerykański LNG

Unijne odejście od rosyjskiego gazu tworzy historyczne okno popytowe. Rozporządzenie przyjęte w 2026 r. przekształciło polityczną deklarację REPowerEU w wiążące prawo i wprowadziło stopniowy, trwały zakaz importu rosyjskiego gazu [4]. Co istotne, najnowszy harmonogram jest ostrzejszy niż wcześniejsze propozycje

dyskutowane publicznie: zakaz importu rosyjskiego LNG ma obowiązywać od początku 2027 r., a gazu rurociągowego od jesieni 2027 r. [4]. Dla Polski oznacza to, że moment uruchomienia FSRU i rozbudowy korytarzy południowych zbiega się z realną potrzebą zastąpienia rosyjskich wolumenów w regionie.

Stany Zjednoczone stały się w ostatnich latach jednym z największych eksporterów skroplonego gazu ziemnego na świecie. Gaz amerykański jest obecnie znacząco tańszy od cen europejskich benchmarków, choć charakteryzuje się pewną zmiennością cenową obserwowaną od kilku lat. W bazie danych administracji USA zarejestrowanych jest 18 zatwierdzonych projektów terminali eksportowych LNG, z czego 8 jest już w trakcie budowy – głównie w Teksasie i Luizjanie. Oznacza to, że podaż amerykańskiego LNG będzie w kolejnych latach systematycznie rosła.

Warto podkreślić, że warunki geopolityczne – w tym polityka handlowa administracji USA i jej nacisk na zwiększenie eksportu LNG do Europy jako substytut gazu rosyjskiego – działają na korzyść polskiej pozycji. Polska może być dla Waszyngtonu naturalnym partnerem w realizacji celu zastąpienia rosyjskich dostaw gazem zza Atlantyku.

Według danych amerykańskiego Departamentu Energii Stany Zjednoczone posiadały w marcu 2026 r. długoterminowe autoryzacje eksportowe LNG o łącznym potencjale ponad 56 Bcf dziennie, przy czym część tej zdolności była już operacyjna, a część w budowie [8]. Amerykańska EIA wskazywała ponadto, że zdolności eksportowe LNG w Ameryce Północnej mają wzrosnąć istotnie do 2029 r., a USA pozostają największym eksporterem LNG na świecie [9].

Dla Polski to istotna szansa, ale nie gwarancja sukcesu. Gaz amerykański jest wprawdzie o wiele tańszy od europejskiego w punkcie Henry Hub, lecz należy pamiętać, że o końcowej konkurencyjności decydują koszty skraplania, frachtu, regazyfikacji, przesyłu, zabezpieczenia finansowego i ryzyka kursowego. LNG jest rynkiem globalnym, a ładunki mogą płynąć tam, gdzie marża jest najwyższa. Dlatego Polska musi oferować nie tylko terminal, ale cały łańcuch wartości: portfel kontraktów, elastyczny odbiór, możliwość reeksportu, efektywną logistykę i płynny rynek giełdowy. Jeżeli te warunki zostaną spełnione, część marży handlowej rzeczywiście może pozostawać w Polsce, zamiast być przechwytywana przez zagraniczne huby i pośredników.

W tym miejscu szczególnego znaczenia nabiera projekt drugiej jednostki FSRU. GAZ-SYSTEM informował, że w ramach badania rynku (w ramach procedury tzw. open season) zainteresowanie przepustowością drugiej jednostki, projektowanej na 4,5 mld m^3 rocznie, z budową planowaną na lata 2031-2032, niemal czterokrotnie przekroczyło planowaną zdolność, a istotna część zgłoszonego popytu pochodziła

od podmiotów z Ukrainy, Słowacji, Czech i Litwy [10]. To potwierdza, że koncepcja polskiej bramy LNG nie jest wyłącznie postulatem publicystycznym, lecz odpowiada na realny popyt handlowy. Warunkiem jest jednak przejście od niewiążącego zainteresowania do wiążących rezerwacji, decyzji inwestycyjnych i umów długoterminowych.

7. Druga i trzecia jednostka FSRU – granice opłacalności inwestycji

Pierwsza jednostka FSRU o przepustowości 6,1 mld m^3 rocznie może zasadniczo zmienić pozycję Polski na rynku gazu. Druga jednostka, projektowana na 4,5 mld m^3 rocznie, byłaby krokiem od bezpieczeństwa krajowego do realnej funkcji regionalnej. W perspektywie dalszej można rozważać nawet trzecią jednostkę, jeżeli po zaspokojeniu potrzeb krajowych potwierdzi się trwały popyt eksportowy do Czech, Słowacji, Ukrainy i Litwy na poziomie 7-9 mld m^3 rocznie. Taki scenariusz wymaga jednak szczególnie ostrożnego podejścia do ryzyka inwestycyjnego.

Pierwszym ryzykiem jest horyzont czasowy. Infrastruktura gazowa ma długi cykl przygotowania, a rynek zmienia się szybko. Jeżeli Polska opóźni decyzje, część popytu regionalnego może zostać zagospodarowana przez inne korytarze: chorwacki terminal LNG na wyspie Krk, infrastrukturę niemiecką, kierunki włoskie, greckie lub tureckie. Wtedy nawet gotowy terminal w Polsce może mieć niższe wykorzystanie niż zakładano. Konkurencja nie polega wyłącznie na wolumenie, lecz na czasie wejścia na rynek.

Drugim ryzykiem jest trwałość popytu. Europa jednocześnie odchodzi od rosyjskiego gazu i ogranicza ogólne zużycie paliw kopalnych. W latach trzydziestych rozwój OZE, magazynów energii, efektywności energetycznej, biometanu, wodoru i energetyki jądrowej może stopniowo obniżać zapotrzebowanie na gaz. Dlatego inwestycje FSRU powinny być projektowane z myślą o elastyczności: jako aktywa częściowo eksportowe, zdolne do obsługi wielu kontrahentów, o możliwie ograniczonym ryzyku kosztów stałych przerzucanych na krajowych odbiorców.

Trzecim ryzykiem jest bezpieczeństwo Bałtyku. Terminale LNG, jednostki FSRU, podmorskie i lądowe gazociągi, systemy teleinformatyczne oraz infrastruktura portowa są elementami infrastruktury krytycznej. Po doświadczeniach ostatnich lat nie można zakładać, że ryzyko sabotażu, ataków hybrydowych, cyberataków lub presji militarnej jest hipotetyczne. Polska koncepcja hubu gazowego musi więc obejmować

nie tylko decyzje gospodarcze, ale także ochronę morską, monitoring infrastruktury, procedury awaryjne, zdolności naprawcze, współpracę wojskową i ubezpieczeniową oraz odporność kontraktową na zdarzenia nadzwyczajne.

Czwartym ryzykiem jest akceptacja polityczna, a ściślej "klimatyczna". Inwestycje gazowe mogą spotykać się z zarzutem utrwalania paliw kopalnych. Odpowiedzią nie powinno być ignorowanie tej krytyki, lecz jasne określenie funkcji gazu: bezpieczeństwo, elastyczność, zastępowanie bardziej emisyjnych źródeł, bilansowanie OZE i czasowy charakter części inwestycji. Im bardziej projekty gazowe będą wpisane w całościową strategię transformacji, tym łatwiej będzie uzasadnić ich racjonalność gospodarczo i klimatycznie.

8. Rekomendacje strategiczne

Po pierwsze, Polska powinna konsekwentnie rozwijać korytarz gazowy północ-południe. FSRU w Gdańsku, Baltic Pipe i terminal w Świnoujściu tworzą północną bramę dostaw. Aby stała się ona bramą regionalną, konieczne jest zwiększanie zdolności przesyłowych w kierunku Słowacji, Czech, Ukrainy i Litwy, a także usuwanie ograniczeń wewnętrznych w krajowym systemie przesyłowym. Infrastruktura powinna być projektowana z myślą o eksporcie, a nie tylko o zabezpieczeniu krajowego popytu.

Po drugie, trzeba rozbudować magazyny gazu. Hub bez magazynów jest podatny na sezonowość, krótkoterminowe szoki cenowe i ograniczoną elastyczność handlową. Magazyny są także narzędziem budowy produktów rynkowych: umożliwiają arbitraż sezonowy, kontrakty elastyczne i świadczenie usług bezpieczeństwa dla partnerów zewnętrznych. Polska może rozważać współpracę z Ukrainą w zakresie magazynowania, ale nie powinna w żadnym razie rezygnować z rozbudowy własnej bazy magazynowej, co najmniej do poziomu zabezpieczenia własnych potrzeb wewnętrznych.

Po trzecie, konieczne jest wzmocnienie TGE jako regionalnej platformy obrotu. TGE powinna rozwijać produkty terminowe, zwiększać udział podmiotów zagranicznych, pogłębiać płynność, wzmacniać transparentność i budować wiarygodność indeksów cenowych. Celem nie jest natychmiastowe zastąpienie TTF, lecz stworzenie środkowoeuropejskiego punktu odniesienia, który będzie naturalny dla kontraktów związanych z polską infrastrukturą LNG i przesyłem w regionie.

Po czwarte, taryfy przesyłowe powinny wspierać wykorzystanie infrastruktury. Regulator i operator powinni analizować, jak struktura opłat wpływa na decyzje

zagranicznych traderów. Jeżeli koszty przesyłu przez Polskę będą nadmierne, partnerzy wybiorą alternatywne szlaki, nawet jeżeli polska infrastruktura będzie technicznie dostępna. Jednocześnie taryfy muszą zapewniać finansowanie inwestycji i ochronę odbiorców krajowych przed nieuzasadnionym przerzucaniem kosztów projektów eksportowych.

Po piąte, administracja publiczna powinna prowadzić aktywną dyplomację energetyczną. Hub gazowy nie powstaje wyłącznie decyzją operatora. Wymaga porozumień międzyrządowych, stabilnych ram regulacyjnych, koordynacji z Komisją Europejską, współpracy z operatorami systemów przesyłowych w państwach sąsiednich oraz oferty skierowanej do konkretnych odbiorców: Czech, Słowacji, Ukrainy, Litwy i Węgier. Polska będąc członkiem UE powinna przedstawiać im swoje projekty nie tylko jako narodową infrastrukturę, lecz także jako europejskie narzędzie bezpieczeństwa dostaw.

Po szóste, konieczne jest zintegrowanie polityki gazowej z polityką bezpieczeństwa. Ochrona Bałtyku, portów, terminali LNG, gazociągów i systemów cybernetycznych powinna być traktowana jako część kosztu projektu hubowego. Nie ma hubu bez zaufania do ciągłości dostaw. Każdy poważny kontrahent zagraniczny będzie oceniał nie tylko cenę gazu, ale także ryzyko polityczne, militarne, infrastrukturalne i regulacyjne.

9. Wnioski – polska szansa, która wymaga decyzji

Polska ma obecnie wyjątkową szansę stać się hubem gazowym Europy Środkowo-Wschodniej. Nie jest to slogan polityczny, lecz konsekwencja kilku zbiegających się procesów: odejścia Europy od rosyjskiego gazu, rozbudowy polskiej infrastruktury LNG i przesyłowej, rosnącej podaży LNG z USA, potrzeby stabilizacji systemów energetycznych opartych coraz mocniej na OZE oraz położenia Polski pomiędzy Bałtykiem, Ukrainą, Czechami, Słowacją, Litwą i Węgrami.

Jednocześnie szansa ta nie jest dana raz na zawsze. Polska może stać się centrum regionalnego handlu gazem, ale może też pozostać wyłącznie krajem tranzytowym i importowym, jeżeli nie rozwinie giełdy, nie obniży barier wejścia, nie zapewni konkurencyjnych taryf, nie rozbuduje magazynów i nie przyspieszy decyzji inwestycyjnych. Infrastruktura fizyczna tworzy możliwość. Rynek decyduje, czy możliwość zamieni się w pozycję strategiczną.

Gaz ziemny powinien być w tej strategii rozumiany jako paliwo niezależności, elastyczności i odporności. W polskich realiach najbliższe dwie dekady będą wymagały

jednoczesnego rozwoju OZE, przygotowania energetyki jądrowej, modernizacji ciepłownictwa, ochrony przemysłu i zapewnienia bezpieczeństwa dostaw. Gaz może być spoiwem tych procesów.

Najważniejszy wniosek praktyczny brzmi: Polska powinna działać równolegle na trzech poziomach. Po pierwsze, inwestować w FSRU, magazyny i korytarze północ-południe. Po drugie, budować płynny rynek giełdowy z udziałem zagranicznych partnerów. Po trzecie, prowadzić dyplomację energetyczną, która przekona Czechy, Słowację, Ukrainę, Litwę i Węgry, że północna brama LNG przez Polskę jest bezpieczna, konkurencyjna i trwała. Jeżeli te trzy poziomy zostaną zintegrowane, Polska może nie tylko uniezależnić się energetycznie, ale także stać się jednym z architektów bezpieczeństwa gazowego nowej Europy.

Źródła

[1] GAZ-SYSTEM, Krajowy Dziesięcioletni Plan Rozwoju systemu przesyłowego na lata 2026-2035; komunikat URE o uzgodnieniu planu rozwoju operatora.

[2] GAZ-SYSTEM, informacje projektowe dotyczące terminalu FSRU w rejonie Gdańska oraz komunikat o rozbudowie Terminalu LNG w Świnoujściu do 8,3 mld m^3 rocznie.

[3] GAZ-SYSTEM, materiały „Baltic Sea and Amber Gas Corridors" oraz dane o przepustowościach terminali, Baltic Pipe i połączeń międzysystemowych.

[4] Komisja Europejska i Rada UE, materiały dotyczące rozporządzenia przyjętego w 2026 r. w sprawie stopniowego zakazu importu rosyjskiego gazu w ramach REPowerEU.

[5] Urząd Regulacji Energetyki, Charakterystyka rynku paliw gazowych w Polsce za 2024 r.

[6] Towarowa Giełda Energii, informacje o rynkach gazu oraz podsumowanie aktywności handlowej w 2025 r.

[7] Oxford Institute for Energy Studies, analiza polskiego rynku gazu i pozycji ORLEN/PGNiG po konsolidacji.

[8] U.S. Department of Energy, Office of Fossil Energy and Carbon Management, zestawienie autoryzacji eksportowych LNG, stan na marzec 2026 r.

[9] U.S. Energy Information Administration, informacje o rozwoju zdolności eksportowych LNG w USA i Ameryce Północnej do 2029 r.

[10] GAZ-SYSTEM, materiały dotyczące badania rynku i procedury Open Season dla drugiej jednostki FSRU o planowanej przepustowości 4,5 mld m^3 rocznie.

Energia jako dobro konstytucyjne

Michał Moskal

Abstrakt:

Artykuł analizuje tezę o energii jako jednej z wartości konstytucyjnych. Autor wykazuje, że dostęp do energii można wywodzić z konstytucyjnych gwarancji godności, równości i ochrony praw socjalnych. Na tle kryzysu cenowego lat 2022–2023 wskazuje na praktyczne konsekwencje tej tezy dla polityki regulacyjnej, ochrony odbiorców wrażliwych i zobowiązań państwa w zakresie zapewnienia dostępu do przystępnej cenowo energii.

Słowa kluczowe: dobro konstytucyjne, energia, prawa człowieka, Konstytucja RP, ubóstwo energetyczne, regulacja energii, prawo unijne

Energia w prawie polskim i unijnym już dziś przestaje być traktowana jak zwykły przedmiot obrotu, choć w Polsce nie została jeszcze nazwana wprost dobrem konstytucyjnie chronionym. Komisja Europejska wskazuje, że energia jest potrzebna w codziennym życiu w celu zapewnienia warunków ogrzewania, chłodzenia i oświetlenia, ważnych dla godnego poziomu życia i zdrowia. Europejski Filar Praw Socjalnych zalicza energię do usług podstawowych, do których każdy powinien mieć dostęp. Podobnie unijne przepisy definiują ubóstwo energetyczne jako brak dostępu gospodarstwa domowego do podstawowych usług energetycznych, których zapewnienie warunkuje elementarny standard życia i zdrowia. Polski ustawodawca poszedł w tym samym kierunku. W prawie energetycznym zdefiniowano ubóstwo energetyczne, a Prezes Urzędu Regulacji Energetyki (URE) opisuje szczególne zabezpieczenia dla odbiorców wrażliwych, w tym zakaz odłączeń w części okresu zimowego oraz obowiązek szybkiego wznowienia dostaw po złożeniu reklamacji.

Międzynarodowa Agencja Energetyczna (IEA) podkreśla, że energia jest kluczowym nakładem we wszystkich sektorach produkcyjnych, a jej koszt wpływa

na inwestycje, zatrudnienie i konkurencyjność. Organizacja Współpracy Gospodarczej i Rozwoju (OECD) zwraca uwagę, że w 2024 r. hurtowe ceny gazu w UE były niemal pięciokrotnie wyższe niż w Stanach Zjednoczonych, co przełożyło się na ceny energii elektrycznej. IEA wskazuje zarazem, że w 2025 r. ceny energii elektrycznej dla przemysłu energochłonnego w UE utrzymywały się na poziomie ponad dwukrotnie wyższym niż w USA i o blisko połowę wyższym niż w Chinach. W Polsce obciążenie gospodarstw domowych pozostało wysokie: według Eurostatu w drugiej połowie 2025 r. cena energii elektrycznej dla gospodarstw domowych liczona w standardzie siły nabywczej była trzecią najwyższą w UE, a udział nieodzyskiwalnych podatków i opłat w cenie energii dla odbiorców niebędących gospodarstwami domowymi był w Polsce najwyższy we Wspólnocie.

Teza o energii jako dobru konstytucyjnym da się obronić w ramach obowiązującej Konstytucji, nawet zanim doszłoby do jej formalnej nowelizacji. Perspektywa ustrojowa otwiera się przede wszystkim przez art. 20 Konstytucji RP, który ustanawia społeczną gospodarkę rynkową jako podstawę ustroju gospodarczego, oraz przez art. 5, nakładający na Rzeczpospolitą obowiązek zapewnienia bezpieczeństwa obywateli i ochrony środowiska przy poszanowaniu zasady zrównoważonego rozwoju. Do tego dochodzi art. 30 Konstytucji chroniący godność człowieka, art. 68 o prawie do ochrony zdrowia, art. 74 o bezpieczeństwie ekologicznym i art. 76 o ochronie konsumentów przed działaniami zagrażającymi zdrowiu, bezpieczeństwu i przed nieuczciwymi praktykami rynkowymi. W doktrynie prawa konstytucyjnego wyraźnie podkreślono, że art. 20 wyznacza odpowiedzialność państwa za sytuację gospodarczą wspólnoty i społeczne skutki działań gospodarczych, a orzecznictwo sądowe konsekwentnie akcentuje konstytucyjny ciężar ochrony konsumenta.

Z tego punktu widzenia energia nie musi być rozumiana jako odrębne, samoistne prawo podmiotowe do określonej ceny kWh. Wystarczy przyjąć, że dostęp do niej stanowi dobro o znaczeniu ustrojowym, bez którego iluzoryczne stają się inne konstytucyjne wolności i gwarancje. Brak ogrzewania, oświetlenia, chłodzenia czy zasilania podstawowych urządzeń może uderzać zarówno w godność, zdrowie, bezpieczeństwo, jak i realnie uniemożliwiać dostęp do uczestnictwa w życiu społecznym. Również obowiązujące w Polsce prawo energetyczne potwierdza tę logikę. Ustawa ta reguluje zasady kształtowania polityki energetycznej państwa, definiuje zjawisko ubóstwa energetycznego i przewiduje szczególną ochronę odbiorców wrażliwych oraz mechanizmy kontynuacji dostaw w razie sporu. To język dotyczący dobra wymagającego ochrony publicznoprawnej.

Po kryzysie cenowym lat 2022–2023 spór o energię przestał być zagadnieniem sektorowym. Rada UE i Komisja Europejska, reformując rynki energetyczne w 2024 r., wprost przyznały, że potrzebne są rozwiązania ograniczające zależność cen energii elektrycznej od niestabilnych cen paliw kopalnych, lepiej chroniące konsumentów oraz tworzące bardziej przewidywalne warunki dla przedsiębiorstw. Reformy przewidują większą dostępność umów na czas określony ze stałą ceną, wzmocnienie roli sprzedawców z urzędu i dostawców taniej energii, łatwiejsze wykorzystanie długoterminowych umów na dostawy energii (PPA) oraz powszechniejsze wprowadzenie kontraktów różnicowych dla nowych inwestycji. Sama Unia Europejska uznała, że nie sposób budować nowoczesnej gospodarki na energii, której cena pozostaje zakładnikiem szoków surowcowych.

W realiach polskich argument ten jest jeszcze mocniejszy. Prezes URE pokazuje, że średnia cena energii elektrycznej dla gospodarstw domowych, uwzględniająca także koszty dystrybucji, wzrosła z 0,8280 zł/kWh w 2024 r. do łącznie około 0,9198 zł/kWh w 2025 r., czyli o ponad 11%. Równocześnie średnia roczna cena sprzedaży energii elektrycznej na rynku konkurencyjnym spadła z 759,29 zł/MWh w 2023 r. do 518,81 zł/MWh w 2024 r. i 458,24 zł/MWh w 2025 r., co najlepiej pokazuje skalę wahań cen ostatnich lat. Chociaż od 1 stycznia 2026 r. średnia cena energii elektrycznej w taryfach dla gospodarstw domowych zatwierdzona przez Prezesa URE wynosi 495,16 zł/MWh, a więc jest niższa od ceny „mrożonej" z 2025 r., nie usuwa to problemu strukturalnego. Należy zwrócić przy tym uwagę, że pełny rachunek za energię elektryczną, analizowany przez Prezesa URE, zależy nie tylko od kosztów samej energii, lecz także od kosztów eksploatacji sieci, opłat i podatków. Z perspektywy ustroju gospodarczego nie chodzi więc wyłącznie o to, by cena była w danym kwartale niższa, lecz by była przewidywalna i społecznie akceptowalna.

Kolejnym aspektem, który musi być uwzględniany w analizie systemu elektroenergetycznego jest kwestia suwerenności państwa i kierunku publicznych inwestycji. IEA wskazuje, że polski system elektroenergetyczny nadal w znacznym stopniu opiera się na krajowym wydobyciu węgla kamiennego i brunatnego, mimo że w ostatnich latach znacząco wzrosło znaczenie fotowoltaiki, a także realizowane są inwestycje w morskie farmy wiatrowe. Według danych IEA w 2024 r., węgiel pozostawał największym źródłem wytwarzania energii elektrycznej w Polsce, odpowiadającym za 56% produkcji.

Program polskiej energetyki jądrowej, rozważając uwarunkowania dotyczące budowy elektrowni jądrowych w Polsce, uzasadnia rozwój inwestycji jądrowych

potrzebą zwiększenia bezpieczeństwa energetycznego i zapewnienia bardziej stabilnych cen dla odbiorców końcowych, zaś Polskie Sieci Elektroenergetyczne S.A., operator systemu przesyłowego (PSE), podkreśla, że rozbudowa i cyfryzacja sieci przesyłowych służą bezpieczeństwu dostaw. Również pozostałe polskie dokumenty strategiczne wskazują energię jako dźwignię rozwoju gospodarczego oraz potrzebę oparcia zapotrzebowania na moc na zdywersyfikowanych źródłach krajowych. Wniosek jest prosty, a zarazem ustrojowo istotny: państwo, które chce chronić rodzinę i przemysł, nie może redukować polityki energetycznej wyłącznie do reakcji na bieżący, wąsko pojmowany rachunek ekonomiczny.

Energia musi być traktowana jako dobro konstytucyjne w sensie aksjologicznym, zaś teza ta musi zostać przełożona na działania legislacyjne. Działanie takie będzie zgodne z konstytucyjnym modelem społecznej gospodarki rynkowej. Wyznaczałaby jego granice według kryteriów takich jak dobro wspólne, bezpieczeństwo i ochrona słabszego uczestnika obrotu. W praktyce oznaczałoby to ustawowe określenie minimum podstawowych usług energetycznych, silniejszy zakaz odłączeń w sytuacjach zagrażających zdrowiu i bezpieczeństwu, rozwinięcie ofert o przewidywalnej cenie na rynku detalicznym oraz bardziej trwałe powiązanie polityki osłonowej z kryterium rzeczywistej dostępności energii na poziomie gospodarstwa domowego. Takie instrumenty są zresztą zgodne z obecnym kierunkiem prawa unijnego, które stawia na umowy o stałej cenie, ochronę odbiorców wrażliwych i wsparcie dla osób potrzebujących jako element sprawiedliwej transformacji.

Docelowo warto otworzyć dyskusję o wyraźniejszym zakotwiczeniu tej zasady w samych przepisach Konstytucji, które powinno przybrać formę wyraźnie sformułowanego obowiązku władz publicznych do zapewnienia bezpieczeństwa energetycznego, dostępu do podstawowych usług energetycznych oraz prowadzenia polityki sprzyjającej stabilności dostaw i przystępności cenowej energii. Nie byłaby to konstytucyjna obietnica „taniego prądu", lecz norma wyznaczająca państwu trwały kierunek działania. Innymi słowy, celem nowelizacji Konstytucji powinno być ustanowienie materialnego obowiązku prowadzenia przez państwo polityki, która łączy bezpieczeństwo dostaw, ochronę zdrowia, ochronę konsumenta i konkurencyjność gospodarki na gruncie art. 20, 5, 30, 68, 74 i 76 Konstytucji. Jest to kierunek poważny, państwowy i zgodny z polską tradycją społecznej gospodarki rynkowej.

Odrębnie trzeba podkreślić, że konstytucyjne umocowanie energii jako dobra szczególnie chronionego nie byłoby jedynie deklaracją programową. Tak sformułowany przepis nakładałby na państwo i rząd realny obowiązek prowadzenia polityki,

która zapewnia stabilność dostaw oraz społecznie akceptowalny poziom cen. Władza publiczna nie mogłaby wówczas traktować gwałtownych wzrostów rachunków wyłącznie jako zjawiska zewnętrznego, za które nie ponosi odpowiedzialności. Musiałaby projektować podatki, opłaty, taryfy, inwestycje sieciowe, politykę surowcową i mechanizmy osłonowe w taki sposób, aby energia była dostępna dla rodzin, samorządów, instytucji publicznych i przedsiębiorców. Oczywiście do Konstytucji nie powinno się wpisywać przepisów ustanawiających konkretną cenę prądu czy gazu – bo byłoby to prawnie i gospodarczo nieracjonalne. Powinna jednak wyznaczać standard działania państwa: ceny energii powinny być stabilne, przewidywalne i możliwe do udźwignięcia przez obywateli i przedsiębiorstwa. W przeciwnym razie społeczna gospodarka rynkowa staje się pustą formułą, a bezpieczeństwo ekonomiczne obywateli zostaje pozostawione przypadkowi.

O sporze o energię w Polsce zbyt długo mówiliśmy tak, jakby chodziło wyłącznie o jedną pozycję na rachunku gospodarstwa domowego albo o koszt produkcji w bilansie przedsiębiorstwa. Tymczasem doświadczenie ostatnich lat odsłoniło prawdę dużo poważniejszą. Energia wyznacza granice bezpieczeństwa obywateli, sprawności państwa i możliwości rozwojowych gospodarki. Komisja Europejska stwierdza wprost, że bez energii zapewniającej ogrzewanie, chłodzenie i oświetlenie nie sposób utrzymać godnego poziomu życia i ochrony zdrowia. Europejski Filar Praw Socjalnych uznał energię za jedną z usług podstawowych, do których każdy powinien mieć dostęp. Już na tym poziomie widać, że nie rozmawiamy o zwykłym towarze, lecz o fundamencie współczesnego życia zbiorowego.

Z perspektywy konstytucyjnej nie jest to twierdzenie przesadne ani egzotyczne. Polska Konstytucja buduje ustrój gospodarczy na zasadzie społecznej gospodarki rynkowej. Państwo ma zapewniać bezpieczeństwo obywateli, szanować i chronić godność człowieka, chronić zdrowie, prowadzić politykę zapewniającą bezpieczeństwo ekologiczne i chronić konsumentów przed działaniami zagrażającymi ich zdrowiu oraz bezpieczeństwu. Patrząc systemowo, dostrzega się rzecz oczywistą: brak realnego dostępu do energii uderza jednocześnie w kilka konstytucyjnych wartości naraz. Właśnie dlatego teza, że energia powinna być uznana za dobro konstytucyjne jest logicznym dopowiedzeniem aksjologii ustawy zasadniczej.

W doktrynie prawa konstytucyjnego trafnie zauważono, że społeczna gospodarka rynkowa oznacza odpowiedzialność państwa za sytuację gospodarczą wspólnoty i społeczne skutki działań gospodarczych. Ten fragment debaty ustrojowej ma dziś znaczenie elementarne. Rynek energii pełni ważną funkcję, ale nie może decydować

o granicach ludzkiej godności, zdrowia i bezpieczeństwa. Nie sposób przyjąć, że państwo może uchylić się od odpowiedzialności za zjawisko ubóstwa energetycznego, zasłaniając się wyłącznie ceną wyznaczoną przez mechanizm rynkowy. Skoro konstytucja nakazuje łączyć wolność gospodarczą z solidarnością i ochroną dobra wspólnego, to energia – warunek codziennego funkcjonowania rodziny, szkoły, szpitala, gminy i przedsiębiorstwa – należy do sfery szczególnej odpowiedzialności władz publicznych.

Prawo energetyczne nie tylko określa zasady kształtowania polityki energetycznej państwa, lecz także definiuje ubóstwo energetyczne jako stan, w którym gospodarstwo domowe nie może zapewnić sobie wystarczającego poziomu ciepła, chłodu i energii elektrycznej do zasilania urządzeń i oświetlenia. Prezes URE przypomina ponadto, że odbiorcy wrażliwi objęci są dodatkową ochroną. W części okresu zimowego obowiązuje zakaz wstrzymywania dostaw energii, a po wniesieniu reklamacji przedsiębiorstwo energetyczne ma obowiązek w krótkim terminie wznowić dostawy i kontynuować je do czasu rozstrzygnięcia sprawy. Są to przepisy potwierdzające, że polski porządek prawny już teraz intuicyjnie uznaje energię za dobro, które wymaga ochrony silniejszej niż zwyczajny towar w obrocie gospodarczym.

Najważniejszy argument przemawia jednak z perspektywy gospodarczej. IEA nie pozostawia wątpliwości, że koszty energii są podstawowym nakładem we wszystkich sektorach produkcyjnych, a jej cena wpływa na rentowność inwestycji, miejsca pracy i długofalową konkurencyjność. OECD pokazała, że w 2024 r. hurtowe ceny gazu w Unii Europejskiej były niemal pięciokrotnie wyższe niż w Stanach Zjednoczonych, a IEA wskazała, że w 2025 r. energia elektryczna dla energochłonnego przemysłu w UE kosztowała nadal ponad dwa razy więcej niż w USA i prawie o połowę więcej niż w Chinach. W takim świecie energetyka jest nie tylko elementem infrastruktury, lecz także warunkiem utrzymania przemysłu, inwestycji i miejsc pracy w Europie, a tym bardziej w Polsce. Państwo, które nie potrafi nadać energii rangi dobra strategicznego, skazuje swój ustrój gospodarczy na trwałą słabość.

Polskie dane pokazują, że problem nie jest wyłącznie teoretyczny. Według URE średnia cena energii elektrycznej wraz z dystrybucją dla gospodarstw domowych wzrosła z 0,8280 zł/kWh w 2024 r. do 0,9198 zł/kWh w 2025 r., a więc o ponad 11%. Eurostat wyliczył zarazem, że w drugiej połowie 2025 r. Polska należała do państw o najwyższych kosztach energii dla gospodarstw domowych liczonych według siły nabywczej, zajmując trzecie miejsce w całej Unii. W tej samej publikacji wskazano, że udział nieodzyskiwanych podatków i opłat w cenie energii dla odbiorców

niebędących gospodarstwami domowymi był w Polsce najwyższy w UE. W takiej konfiguracji nie wystarczy już mówić o doraźnym „mrożeniu cen". Spór dotyczy samego modelu państwa: czy władza publiczna może biernie obserwować taki stan rzeczy, czy raczej ma obowiązek tworzyć trwałe struktury i instrumenty ochronne o wysokiej stabilności.

Uznanie energii za dobro konstytucyjne oznaczałoby, że państwo ma obowiązek tak kształtować regulacje, daniny publiczne i politykę inwestycyjną, aby dostęp do podstawowych usług energetycznych był realny, bezpieczny i przewidywalny dla rodziny, samorządu terytorialnego i przedsiębiorcy. Taka koncepcja pozostaje w pełnej zgodzie z unijną reformą rynku energii, która wzmacnia rozwiązania oparte o stałą cenę energii, ochronę odbiorców wrażliwych i mechanizmy ograniczające przenoszenie cenowych skutków szoków paliwowych na odbiorców indywidualnych.

W polskich warunkach prawnych i gospodarczych z powyższej zasady wynika jeszcze jedna konsekwencja, o której nie można zapominać: bezpieczeństwo energetyczne musi zostać wsparte przez stabilny i zdywersyfikowany miks energetyczny. Forum Energii wskazuje, że w 2025 r. 52% energii elektrycznej w Polsce nadal pochodziło z węgla, ale równolegle kraj szybko rozbudowuje fotowoltaikę i przygotowuje duże inwestycje w morską energetykę wiatrową. Oficjalny program energetyki jądrowej został uzasadniony potrzebą bezpieczeństwa energetycznego oraz bardziej stabilnych cen dla odbiorców, a PSE prowadzą inwestycje służące rozbudowie i cyfryzacji sieci. Państwo odpowiedzialne nie rozmontowuje istniejących filarów bezpieczeństwa przed zbudowaniem nowych. Państwo odpowiedzialne prowadzi transformację tak, by rachunek społeczny, przemysłowy i geopolityczny pozostawał pod kontrolą. To właśnie jest język racji stanu i język porządku konstytucyjnego.

Dlatego czas otworzyć w Polsce poważną dyskusję, która nie zatrzyma się na kolejnym okresie taryfowym i na kolejnym mechanizmie osłonowym. Pytanie nie brzmi już, czy państwo może ingerować w obszar energii, bo ingeruje od dawna – w taryfy, ochronę odbiorców wrażliwych, programy osłonowe, inwestycje sieciowe i strategiczne projekty wytwórcze. Właściwe pytanie brzmi, czy robi to doraźnie, czy w oparciu o jasną zasadę ustrojową. Jeżeli chcemy polskiej gospodarki opartej na produkcji, rodzinie, inwestycjach i bezpieczeństwie, musimy wreszcie przyznać to wprost, że energia jest prawem wspólnoty do normalnego funkcjonowania. W języku konstytucyjnym oznacza to jedno: energia powinna być uznana za dobro konstytucyjne.

Transformacja energetyczna, bezpieczeństwo energetyczne oraz rozwój projektów wiatrowych i gazowych

Maciej Olczak

ABSTRAKT:

Tekst omawia najważniejsze trendy globalnej transformacji energetycznej z perspektywy polskich potrzeb. Autor analizuje rozwój lądowej i morskiej energetyki wiatrowej, wzrost znaczenia LNG i pływających terminali FSRU oraz rosnące zapotrzebowanie na surowce strategiczne do budowy infrastruktury OZE. Wskazuje na kluczowe znaczenie dywersyfikacji źródeł energii i zrównoważenia celów klimatycznych z wymogami bezpieczeństwa dostaw.

Słowa kluczowe: transformacja energetyczna, offshore wind, OZE, LNG, FSRU, surowce strategiczne, bezpieczeństwo energetyczne

Transformacja energetyczna to dziś pojęcie odmieniane przez wszystkie przypadki na forach internetowych, konferencjach, spotkaniach i wywiadach. Dla uważnych obserwatorów i znawców tematu należy ona obecnie do najważniejszych procesów gospodarczych i geopolitycznych na świecie. Obejmuje ona równoległy rozwój odnawialnych źródeł energii, modernizację infrastruktury przesyłowej, zwiększanie efektywności energetycznej oraz utrzymanie bezpieczeństwa dostaw energii. Szczególne znaczenie, a jednocześnie najwięcej kontrowersji wywołują projekty związane z energetyką wiatrową na lądzie i morzu, rozwojem rynku gazu skroplonego LNG (Liquefied Natural Gas), w tym instalacjami pływających magazynów gazu skroplonego FSRU (Floating Storage Regasification Units) oraz inwestycjami gazowymi pełniącymi funkcję paliwa przejściowego.

Jednym z kluczowych wyzwań transformacji energetycznej jest rosnące zapotrzebowanie na surowce strategiczne, a co za tym idzie również ich ceny. Dość szczególne miejsce zajmuje tu miedź, której wykorzystanie dynamicznie wzrasta wraz z rozwojem elektromobilności, energetyki odnawialnej oraz cyfryzacji gospodarki. Samochody elektryczne zużywają nawet kilkukrotnie więcej miedzi niż pojazdy z silnikami spalinowymi. Dodatkowo ogromne ilości tego metalu wykorzystywane są w kablach przesyłowych dla farm wiatrowych na lądzie (tzw. onshore) i na morzu (tzw. offshore), w transformatorach, magazynach energii oraz systemach automatyki przemysłowej. W niektórych projektach operatorzy zaczynają stosować również kable aluminiowe, jednak miedź nadal pozostaje podstawowym materiałem dla infrastruktury przesyłowej. To samo dotyczy innych metali jak lit, aluminium, kobalt, nikiel czy srebro.

Rozwój energetyki wiatrowej na lądzie pozostaje jednym z najtańszych sposobów zwiększania produkcji energii elektrycznej ze źródeł odnawialnych, między innymi dlatego że nie zawiera komponentu związanego z kosztem paliwa. W wielu krajach europejskich projekty onshore wind osiągnęły wysoki poziom dojrzałości technologicznej i ekonomicznej, budowanej od prawie dwóch dekad. Jednocześnie sektor mierzy się z wyzwaniami związanymi z dostępnością gruntów, procedurami administracyjnymi oraz integracją nowych mocy z systemami elektroenergetycznymi. Pomimo tych ograniczeń energetyka wiatrowa na lądzie pozostaje istotnym elementem strategii dekarbonizacji gospodarek.

Jeszcze większe znaczenie przypisuje się obecnie morskim farmom wiatrowym. Offshore wind oferuje wyższe współczynniki wykorzystania mocy, większą skalę projektów oraz możliwość lokalizacji źródeł energii blisko dużych centrów przemysłowych i miejskich. Jednocześnie sektor ten doświadcza istotnych problemów kosztowych wynikających z inflacji, wzrostu cen surowców, wyższych kosztów finansowania, ograniczonej logistyki transportowej oraz napięć w globalnych łańcuchach dostaw.

Przykładem działań wspierających rozwój rynku offshore są zmiany regulacyjne w Danii. Po wcześniejszych nieudanych aukcjach władze zdecydowały się na zastosowanie mechanizmu Contracts for Difference (CfD), który gwarantuje inwestorom większą przewidywalność przychodów. Dzięki temu ponownie pojawiło się zainteresowanie deweloperów projektami morskich farm wiatrowych. Pokazuje to, że przyszłość sektora zależy nie tylko od technologii, ale również od stabilności otoczenia regulacyjnego i dostępności mechanizmów wsparcia.

W wielu regionach świata, w tym w Polsce, obserwowany jest dalszy rozwój dużych projektów offshore. W Europie i Azji realizowane są inwestycje wykorzystujące turbiny o mocy 15 MW, które należą do największych obecnie stosowanych jednostek na świecie. Zauważalnie wzrosła moc generowana z pojedyńczych farm wiatrowych. Większość farm to dziś projekty przekraczające 1 GW mocy wraz z rozbudowaną infrastrukturą kabli podmorskich oraz zapleczem serwisowym. W Wielkiej Brytani, Niemczech, Polsce czy Francji przygotowywane są kolejne wielkoskalowe inwestycje offshore, których wartość liczona jest w miliardach euro. Trend ten potwierdza, że energetyka morska pozostaje jednym z filarów długoterminowej transformacji energetycznej. Jednak przed sektorem stoją ogromne wyzwania i pojawia się coraz więcej wątpliwości o zasadność tych inwestycji. Budowa farm wiatrowych na morzu to proces, który zajmuje nawet 10-12 lat. Utrzymanie dynamiki tych inwestycji w dużej mierze zależy od dostępności finansowania i zasobności portfela inwestorów. Nawet do 20-30% całej inwestycji jest prowadzone z kapitału własnego inwestora. Kontrakty różnicowe, wprowadzone jako jeden z mechanizmów re-finansowania tych inwestycji dają bankom gwarancje wystarczające na udzielenie finansowania, ale poza wyzwaniami kapitałowymi, także stoją te technologiczne, związane choćby z rosnącą mocą turbin i brakiem gotowej wystarczająco gabarytowej logistyki nadążającej z rozwojem technologii turbin.

Rozwój offshore wind powoduje równocześnie znaczący wzrost zapotrzebowania na kable energetyczne, statki instalacyjne, porty serwisowe oraz wyspecjalizowane kadry. Coraz większe znaczenie zyskują krajowe łańcuchy dostaw oraz polityka przemysłowa państw, które chcą maksymalizować korzyści gospodarcze wynikające z realizowanych inwestycji.

Pomimo szybkiego rozwoju odnawialnych źródeł energii inne źródło energetyczne przejęło rolę medium pośredniego, które wpisuje się w politykę transformacji energetycznej oraz obniżonej emisji gazów cieplarnianych. Jest to gaz ziemny który nadal odgrywa ważną rolę w zapewnianiu stabilności systemów elektroenergetycznych. Elektrownie gazowe mogą szybko reagować na zmiany produkcji energii z wiatru i słońca, dzięki czemu wspierają bezpieczeństwo pracy sieci. Z tego względu wiele państw traktuje gaz jako paliwo przejściowe umożliwiające stopniowe odchodzenie od węgla.

W ostatnich latach szczególnego znaczenia nabrał rynek LNG. Skroplony gaz ziemny stał się jednym z najważniejszych produktów eksportowych Stanów Zjednoczonych. Rosnące moce eksportowe oraz rozwój terminali odbiorczych w Europie

i Azji przyczyniły się do zwiększenia płynności globalnego rynku gazu. LNG odgrywa obecnie istotną rolę nie tylko w handlu energią, ale również w polityce zagranicznej oraz budowaniu relacji strategicznych pomiędzy państwami.

W tym kontekście coraz większe znaczenie mają jednostki FSRU, czyli pływające terminale magazynowania i regazyfikacji gazu. Rozwiązanie to umożliwia szybkie zwiększenie zdolności importowych bez konieczności budowy pełnowymiarowych terminali lądowych. Polska, podobnie jak wiele innych państw europejskich, analizuje i rozwija projekty związane z wykorzystaniem FSRU jako elementu wzmacniającego bezpieczeństwo energetyczne oraz dywersyfikację kierunków dostaw. Pierwsza jednostka FSRU pojawi się w Polsce, na Zatoce Gdańskiej pod koniec roku 2027 i uruchomi proces regazyfikacji i transferu gazu w styczniu 2028. Aktualnie trwa proces związany z weryfikacją rynku (tzw. „open season"), który da odpowiedź czy powstanie zapotrzebowanie na drugą tego typu jednostkę. Inwestorem jest spółka Gaz System, która zapewnia całą infrastrukturę przesyłową a rezerwy mocy zostały zakontraktowane do spółki Orlen.

Bezpieczeństwo energetyczne przeszło w ostatnich latach istotną ewolucję. Coraz częściej mówi się nie tylko o bezpieczeństwie dostaw, ale również o dominacji energetycznej, czyli zdolności państwa do aktywnego kształtowania rynku energii i wykorzystywania własnych zasobów energetycznych jako źródła przewagi gospodarczej oraz politycznej. Dotyczy to szczególnie eksporterów LNG, którzy dzięki rozbudowie infrastruktury mogą wzmacniać swoją pozycję na rynkach międzynarodowych.

Istotnym wyzwaniem pozostaje również sytuacja geopolityczna. Rosyjska tzw. shadow fleet, czyli flota cieni wykorzystywana do transportu surowców objętych sankcjami, odgrywa coraz większą rolę w handlu LNG. Rozwijane są alternatywne schematy logistyczne obejmujące magazynowanie surowca na jednostkach pływających oraz wykorzystanie starszych gazowców do obsługi tras eksportowych. Pokazuje to, że rynek energii pozostaje silnie uzależniony od czynników politycznych oraz konfliktów geostrategicznych.

Dodatkowym źródłem niepewności są napięcia na światowych szlakach transportowych. Zakłócenia w rejonach kluczowych cieśnin morskich takich jak wcześniej Kanał Sueski i obecnie Cieśnina Ormuz, mogą wpływać na ceny ropy naftowej, gazu oraz koszty transportu. W efekcie inwestorzy i odbiorcy energii muszą uwzględniać coraz większą liczbę czynników ryzyka podczas planowania projektów energetycznych.

Transformacja energetyczna wiąże się również z rozwojem elektromobilności. Jednak tempo wzrostu rynku pojazdów elektrycznych nie jest obecnie tak

dynamiczne jak przewidywano jeszcze kilka lat temu. Wysokie ceny pojazdów, ograniczenia infrastruktury ładowania oraz niepewność konsumentów wpływają na spowolnienie części rynków. Nie zmienia to jednak długoterminowego trendu elektryfikacji transportu, który pozostaje jednym z głównych czynników zwiększających popyt na energię elektryczną oraz metale wykorzystywane w nowych technologiach.

Znaczący wpływ na kierunek transformacji mają także regulacje europejskie. System EU ETS rozszerza zakres oddziaływania na kolejne sektory gospodarki, w tym transport morski. Jednocześnie dyrektywa RED III wzmacnia cele związane z udziałem energii odnawialnej w końcowym zużyciu energii. Regulacje te zwiększają presję inwestycyjną, ale jednocześnie tworzą nowe możliwości rozwoju dla przedsiębiorstw działających w sektorach niskoemisyjnych.

Koszty transformacji energetycznej pozostają przedmiotem intensywnej debaty. Z jednej strony wymagane są ogromne nakłady inwestycyjne obejmujące budowę farm wiatrowych, sieci przesyłowych, magazynów energii, terminali LNG oraz infrastruktury ładowania pojazdów elektrycznych. Z drugiej strony brak inwestycji może prowadzić do wzrostu kosztów związanych z emisjami, importem paliw kopalnych oraz skutkami zmian klimatu. W praktyce kluczowym wyzwaniem staje się odpowiednie rozłożenie kosztów pomiędzy państwo, przedsiębiorstwa i odbiorców końcowych.

W perspektywie najbliższych lat sukces transformacji energetycznej będzie zależał od zdolności do zachowania równowagi pomiędzy trzema celami: dekarbonizacją, konkurencyjnością gospodarki oraz bezpieczeństwem energetycznym. Rozwój energetyki wiatrowej, infrastruktury LNG, projektów FSRU i nowoczesnych sieci elektroenergetycznych będzie wymagał nie tylko kapitału, ale również stabilnych regulacji oraz długoterminowej wizji strategicznej.

Podsumowując, współczesny sektor energetyczny znajduje się w okresie głębokich przemian, mamy do czynienia z jego ewolucją, która zachodzi w bardzo krótkim czasie. Energetyka wiatrowa na lądzie i morzu, gaz ziemny, LNG oraz nowe rozwiązania infrastrukturalne współtworzą złożony ekosystem, którego celem jest zapewnienie bezpiecznych, stabilnych i zrównoważonych dostaw energii. Ostateczny kształt transformacji będzie zależał od postępu technologicznego, decyzji politycznych, dostępności finansowania oraz zdolności państw do współpracy w coraz bardziej wymagającym środowisku geopolitycznym.

Inwestycje w infrastrukturę paliwową jako fundament odporności państwa na kryzysy geopolityczne

Paweł Stańczyk

Abstrakt:

Artykuł analizuje infrastrukturę paliwową jako filar odporności państwa na kryzysy geopolityczne. Autor omawia system logistyki ropy naftowej i paliw w Europie Środkowej i Wschodniej, stan magazynów strategicznych i system rezerw obowiązkowych. Wskazuje na rosnące zapotrzebowanie na paliwa, niedobory pojemności magazynowych i pilną potrzebę inwestycji w infrastrukturę jako warunek ciągłości dostaw w sytuacji kryzysowej.

Słowa kluczowe: infrastruktura paliwowa, bezpieczeństwo energetyczne, rezerwy strategiczne, ropa naftowa, logistyka energetyczna, odporność państwa

Budowanie nowoczesnej, konkurencyjnej gospodarki wymaga długookresowej współpracy pomiędzy administracją publiczną a przedsiębiorstwami działającymi w różnych sektorach rynku. Szczególnego znaczenia nabiera tworzenie sprzyjającego otoczenia dla inwestycji, wdrażania innowacyjnych rozwiązań oraz rozwoju zaawansowanych technologii. To właśnie te czynniki decydują o wzroście efektywności gospodarki i jej zdolności do konkurowania na arenie międzynarodowej. Jednym z fundamentów rozwoju państwa pozostaje sprawnie funkcjonujący system transportowy, warunkujący przepływ osób, towarów i usług. Rozbudowa infrastruktury drogowej, kolejowej, lotniczej i portowej prowadzi do zwiększenia zapotrzebowania na paliwa płynne, które nadal stanowią podstawowe źródło energii

dla sektora transportu. Prognozy wskazują, że w nadchodzących latach zużycie paliw będzie nadal rosło, osiągając stabilizację dopiero w dalszej perspektywie.

Istotnym elementem utrzymującym popyt na ropę naftową pozostaje rozwój przemysłu petrochemicznego. Mimo że nowe inwestycje w tym sektorze koncentrują się przede wszystkim w Stanach Zjednoczonych, krajach Bliskiego Wschodu oraz Azji, europejskie moce produkcyjne powinny utrzymać względnie stały poziom. Jednocześnie produkty petrochemiczne będą odgrywać coraz większą rolę w kształtowaniu globalnego zapotrzebowania na surowce energetyczne. Znaczenie petrochemii wykracza daleko poza tradycyjnie rozumiany przemysł paliwowy. Sektor ten dostarcza surowców niezbędnych do produkcji nowoczesnych materiałów wykorzystywanych w wielu gałęziach gospodarki. Tworzywa sztuczne, włókna syntetyczne, kompozyty czy elastomery znajdują zastosowanie między innymi w motoryzacji, lotnictwie, elektronice oraz technologiach addytywnych. Materiały powstające na bazie produktów petrochemicznych są również nieodzownym elementem instalacji odnawialnych źródeł energii, takich jak farmy fotowoltaiczne czy elektrownie wiatrowe. Coraz większe znaczenie odgrywają także w medycynie, zwłaszcza w obszarze biomateriałów i terapii regeneracyjnych. Nie można również pominąć ich kluczowej roli w produkcji nawozów oraz środków wspierających nowoczesne rolnictwo.

System logistyczny obsługujący dostawy ropy naftowej i paliw w Europie Środkowej i Wschodniej znajduje się obecnie w fazie głębokiej transformacji. Proces ten jest konsekwencją zmian geopolitycznych, wzrostu napięć międzynarodowych oraz przebudowy dotychczasowych kierunków zaopatrzenia w surowce energetyczne. Dzięki swojemu położeniu Polska pełni szczególnie ważną funkcję w regionalnym systemie energetycznym, będąc zarówno znaczącym odbiorcą węglowodorów, jak i istotnym ogniwem tranzytu oraz dystrybucji paliw dla państw sąsiednich. Agresywna polityka Federacji Rosyjskiej oraz wzrost ryzyka zakłóceń w dostawach energii uwidoczniły konieczność zwiększenia odporności infrastruktury krytycznej. Oznacza to potrzebę rozbudowy zdolności magazynowych, tworzenia alternatywnych kierunków dostaw oraz rozwijania systemów zapewniających ciągłość funkcjonowania sieci przesyłowych.

System zapasów ropy naftowej i paliw płynnych

Bezpieczeństwo energetyczne państwa w znacznym stopniu zależy od możliwości zapewnienia nieprzerwanych dostaw surowców energetycznych oraz utrzymywania

odpowiednich rezerw na wypadek sytuacji kryzysowych. W przypadku Polski kwestia ta ma szczególne znaczenie, ponieważ krajowe wydobycie ropy naftowej pokrywa jedynie niewielką część krajowego zapotrzebowania.

Krajowy rynek paliw opiera się również na znaczącym imporcie produktów gotowych. Od 2016 roku udział paliw sprowadzanych z zagranicy utrzymuje się na poziomie od 30 do 40 procent całkowitego zużycia. Struktura kierunków importu podlega wprawdzie zmianom ilościowym, jednak główni partnerzy handlowi pozostają stosunkowo stabilni. Oznacza to, że funkcjonowanie gospodarki oraz systemu transportowego jest silnie uzależnione od sprawnego działania międzynarodowych łańcuchów dostaw. Z tego względu szczególnego znaczenia nabiera infrastruktura umożliwiająca odbiór, transport i przechowywanie zarówno ropy naftowej, jak i paliw gotowych. Kluczowymi elementami tego systemu są terminale przeładunkowe, sieć rurociągów, rafinerie oraz bazy magazynowe. Choć w ostatnich latach nastąpił zauważalny rozwój infrastruktury magazynowej, tempo inwestycji nie zawsze odpowiada dynamice wzrostu krajowego rynku paliwowego. Rosnąca konsumpcja paliw, konieczność utrzymywania zapasów obowiązkowych oraz zmieniające się uwarunkowania geopolityczne powodują, że istniejące zdolności magazynowe wymagają dalszej rozbudowy.

Polski system rezerw ropy i paliw funkcjonuje w ramach wspólnotowych i międzynarodowych mechanizmów bezpieczeństwa energetycznego. Zgodnie z regulacjami Unii Europejskiej oraz wymogami Międzynarodowej Agencji Energetycznej państwa członkowskie zobowiązane są do utrzymywania zapasów odpowiadających co najmniej dziewięćdziesięciu dniom średniego importu netto. W Polsce obowiązują dwa podstawowe mechanizmy tworzenia rezerw. Pierwszy stanowią zapasy obowiązkowe utrzymywane przez przedsiębiorstwa zajmujące się produkcją oraz importem paliw. Drugi filar tworzą zapasy agencyjne pozostające w dyspozycji państwa i zarządzane przez Rządową Agencję Rezerw Strategicznych. Tak skonstruowany model ma zapewnić możliwość reagowania na zakłócenia dostaw oraz ograniczać ryzyko wystąpienia niedoborów na rynku. Według dostępnych danych wielkość krajowych rezerw odpowiada około dziesięciu milionom metrów sześciennych ropy naftowej i paliw. Około połowa tych zapasów powinna być utrzymywana w postaci surowca, natomiast pozostała część w formie produktów gotowych, co pozwala zachować odpowiednią elastyczność systemu. Całkowita pojemność magazynowa dostępna w Polsce szacowana jest na około piętnaście milionów metrów sześciennych, z czego blisko dziewięć milionów przypada na magazyny ropy naftowej, a ponad

sześć milionów na magazyny paliw gotowych. W praktyce jednak znaczna część tej przestrzeni wykorzystywana jest do bieżącej działalności operacyjnej przedsiębiorstw sektora paliwowego. Oznacza to, że rzeczywiste możliwości gromadzenia dodatkowych zapasów interwencyjnych są wyraźnie ograniczone.

Rosnące zużycie paliw powoduje, że już obecnie obserwowane są niedobory wolnych pojemności magazynowych, szczególnie w segmencie benzyn silnikowych. Przedsiębiorstwa zobowiązane do utrzymywania zapasów obowiązkowych coraz częściej sygnalizują trudności z pozyskaniem odpowiedniej przestrzeni magazynowej niezbędnej do realizacji ustawowych obowiązków. Szczególne znaczenie dla funkcjonowania całego systemu ma Podziemny Magazyn Ropy i Paliw w Górze koło Inowrocławia. Obiekt wykorzystujący kawerny solne dysponuje największą pojemnością magazynową w kraju i stanowi jeden z kluczowych elementów krajowego bezpieczeństwa paliwowego. W ostatnich latach jego możliwości operacyjne zostały jednak częściowo ograniczone. Zmniejszenie dostępnej pojemności magazynowej oraz ograniczenie zdolności do zagospodarowania solanki powstającej podczas eksploatacji kawern wydłuża proces ponownego napełniania magazynów po wykorzystaniu zgromadzonych rezerw. W konsekwencji obniża się elastyczność całego systemu reagowania kryzysowego.

Zapotrzebowanie na paliwa

Jednym z kluczowych czynników uzasadniających konieczność dalszej rozbudowy krajowej infrastruktury magazynowej jest systematyczny wzrost zużycia paliw płynnych. W ciągu ostatnich dwóch dekad polski rynek paliwowy rozwijał się bardzo dynamicznie, co było bezpośrednio związane z rozwojem transportu drogowego, wzrostem aktywności gospodarczej oraz zwiększającą się liczbą pojazdów wykorzystywanych zarówno przez przedsiębiorstwa, jak i gospodarstwa domowe. Istotnym momentem dla oceny rzeczywistej skali konsumpcji paliw było wprowadzenie w 2016 roku tzw. pakietu paliwowego. Uszczelnienie rynku ujawniło znaczący udział szarej strefy w obrocie paliwami, który według wcześniejszych szacunków mógł obejmować nawet blisko jedną trzecią rynku. W konsekwencji zweryfikowano dotychczasowe prognozy dotyczące faktycznego poziomu zużycia paliw oraz rozpoczęto działania mające na celu dostosowanie infrastruktury magazynowej do realnych potrzeb rynku.

Obecnie Polska należy do największych konsumentów paliw płynnych w Europie Środkowo-Wschodniej. Roczne zużycie paliw transportowych przekracza 39 mln m³, przy czym dominującą pozycję zajmuje olej napędowy wykorzystywany przede wszystkim przez sektor transportowy, logistyczny oraz przemysłowy. Rosnąca konsumpcja paliw przekłada się bezpośrednio na konieczność zwiększania wielkości zapasów obowiązkowych i agencyjnych. Obowiązujące regulacje wymagają bowiem utrzymywania rezerw adekwatnych do poziomu krajowego zużycia oraz importu. Oznacza to, że wzrost zapotrzebowania automatycznie generuje potrzebę tworzenia nowych pojemności magazynowych. Szacunki wskazują, że w perspektywie najbliższych lat deficyt dostępnych pojemności magazynowych może osiągnąć od 2 do 3 mln m³. Dodatkowym wyzwaniem będą zmiany legislacyjne przewidziane na 2029 rok, które zakładają zwiększenie udziału paliw gotowych w strukturze zapasów agencyjnych. W efekcie większa część rezerw będzie musiała być utrzymywana w postaci produktów gotowych, co wymaga znacznie większej liczby zbiorników magazynowych niż przechowywanie tej samej ilości energii w postaci surowej ropy naftowej.

Brak odpowiednio szybkiej rozbudowy infrastruktury może prowadzić do poważnych konsekwencji dla rynku paliwowego. Ograniczona dostępność magazynów utrudni przedsiębiorstwom realizację ustawowych obowiązków związanych z utrzymywaniem zapasów, a dodatkowe koszty pozyskania przestrzeni magazynowej mogą zostać przeniesione na odbiorców końcowych w postaci wyższych cen paliw. Nie można również wykluczyć, że nadmierne obciążenia regulacyjne i infrastrukturalne będą sprzyjały rozwojowi nielegalnych form obrotu paliwami. W perspektywie długoterminowej rozbudowa infrastruktury magazynowej powinna być traktowana nie tylko jako wymóg wynikający z przepisów, lecz przede wszystkim jako inwestycja wzmacniająca bezpieczeństwo energetyczne państwa i stabilność funkcjonowania gospodarki.

Infrastruktura magazynowa

Magazyny ropy naftowej i paliw stanowią jeden z najważniejszych elementów krajowego systemu bezpieczeństwa energetycznego. Ich podstawowym zadaniem jest zapewnienie ciągłości dostaw surowców i produktów paliwowych w przypadku wystąpienia zakłóceń w funkcjonowaniu rynku, ograniczenia importu lub wystąpienia sytuacji kryzysowych. Znaczenie infrastruktury magazynowej wykracza jednak poza funkcję tworzenia rezerw strategicznych. Odpowiednia pojemność zbiornikowa

umożliwia także efektywne zarządzanie przepływami paliw, ograniczanie skutków sezonowych wahań popytu oraz zwiększanie elastyczności działania całego systemu logistycznego. W okresach zwiększonego zapotrzebowania możliwe jest wykorzystanie zgromadzonych rezerw, natomiast w czasie spadku popytu magazyny pozwalają na czasowe gromadzenie nadwyżek produktów.

Z punktu widzenia odporności państwa szczególne znaczenie ma również właściwa struktura przestrzenna infrastruktury magazynowej. Nadmierna koncentracja zapasów w ograniczonej liczbie lokalizacji zwiększa podatność systemu na awarie techniczne, działania sabotażowe, cyberataki oraz zagrożenia militarne. W sytuacji kryzysowej może to prowadzić do utrudnień w dystrybucji paliw i ograniczać zdolność państwa do szybkiego reagowania na zakłócenia dostaw. Doświadczenia wynikające z konfliktów zbrojnych ostatnich lat pokazują, że obiekty paliwowe należą do infrastruktury szczególnie narażonej na działania przeciwnika. Z tego względu rozwój nowych pojemności magazynowych powinien uwzględniać zasadę dywersyfikacji lokalizacji oraz budowę rozproszonego systemu przechowywania zapasów. Rozproszenie magazynów niesie również korzyści operacyjne. Skrócenie odległości pomiędzy miejscem składowania paliwa a odbiorcą końcowym zwiększa efektywność transportu, ogranicza koszty logistyczne oraz poprawia zdolność do szybkiego reagowania na lokalne niedobory paliw. Współczesna infrastruktura magazynowa powinna być zatem postrzegana nie tylko jako element systemu zapasów obowiązkowych, lecz jako jeden z filarów bezpieczeństwa państwa, wspierający zarówno funkcjonowanie gospodarki, jak i zdolności obronne kraju. W warunkach rosnących zagrożeń geopolitycznych oraz wzrastającego zapotrzebowania na paliwa inwestycje w nowe pojemności magazynowe stają się jednym z najważniejszych wyzwań stojących przed polskim sektorem naftowym.

Rozbudowa infrastruktury magazynowej

Wobec rosnącego zapotrzebowania na paliwa płynne oraz zwiększających się wymagań dotyczących utrzymywania zapasów strategicznych, rozbudowa krajowej infrastruktury magazynowej staje się jednym z najważniejszych wyzwań stojących przed sektorem naftowym. Inwestycje w nowe pojemności magazynowe powinny być postrzegane nie tylko jako odpowiedź na potrzeby rynku, lecz także jako element wzmacniania bezpieczeństwa energetycznego i odporności państwa na sytuacje kryzysowe.

Kluczową rolę w realizacji tego procesu odgrywa spółka PERN, odpowiedzialna za eksploatację krajowego systemu rurociągów przesyłowych oraz znaczącej części infrastruktury magazynowej ropy naftowej i paliw. W ostatnich latach spółka zrealizowała szereg projektów mających na celu zwiększenie zdolności magazynowych i poprawę elastyczności systemu logistycznego. Jednym z najważniejszych przedsięwzięć była rozbudowa bazy paliwowej w Dębogórzu, położonej w bezpośrednim sąsiedztwie portu w Gdyni. W ramach inwestycji powstały nowe zbiorniki magazynowe, znacząco zwiększające możliwości przechowywania paliw. Projekt ten należy analizować nie tylko przez pryzmat zwiększenia pojemności magazynowej, ale również jako przygotowanie infrastruktury do obsługi większych jednostek transportujących paliwa drogą morską. Po zakończeniu modernizacji i pogłębieniu infrastruktury przeładunkowej możliwe będzie efektywniejsze wykorzystanie potencjału importowego regionu.

Fundamentalne znaczenie dla bezpieczeństwa dostaw ropy naftowej zachowuje również Naftoport. Jest on głównym morskim terminalem przeładunkowym surowca w Polsce i jednym z najważniejszych tego typu obiektów w regionie Morza Bałtyckiego. Dzięki wysokim zdolnościom przeładunkowym zapewnia nie tylko zaopatrzenie krajowych rafinerii, lecz także wspiera dostawy do zakładów zlokalizowanych poza granicami Polski. W warunkach ograniczenia importu rosyjskiej ropy znaczenie tego obiektu dla stabilności rynku energetycznego wyraźnie wzrosło. Istotnym elementem krajowego systemu logistycznego pozostają także bazy paliwowe zlokalizowane w centralnej części kraju. Obiekty takie jak Koluszki czy Nowa Wieś Wielka pełnią funkcję strategicznych węzłów dystrybucyjnych, integrując transport rurociągowy, kolejowy oraz drogowy. Ich położenie umożliwia sprawną obsługę znacznej części krajowego rynku paliwowego i zwiększa odporność systemu na zakłócenia.

Planowanie kolejnych inwestycji powinno uwzględniać nie tylko wzrost pojemności magazynowej, ale również odpowiednie rozmieszczenie nowych obiektów. Budowa rozproszonej sieci magazynów zwiększa bezpieczeństwo dostaw oraz ogranicza ryzyko wynikające z koncentracji zapasów w niewielkiej liczbie lokalizacji. Doświadczenia płynące z konfliktu rosyjsko-ukraińskiego pokazują, że terminale paliwowe należą do infrastruktury szczególnie narażonej na działania militarne. Z tego względu dywersyfikacja lokalizacji magazynów powinna stać się jednym z podstawowych kryteriów planowania nowych inwestycji. Dodatkowym argumentem przemawiającym za rozproszeniem infrastruktury jest poprawa efektywności logistycznej.

Mniejsze odległości pomiędzy miejscem magazynowania a odbiorcą końcowym pozwalają skrócić czas dostaw, ograniczyć koszty transportu i zwiększyć zdolność reagowania w sytuacjach nadzwyczajnych. Rozbudowa infrastruktury magazynowej powinna zatem obejmować zarówno zwiększanie pojemności istniejących obiektów, jak i tworzenie nowych punktów magazynowych w różnych częściach kraju.

Podsumowując, rosnące potrzeby rynku paliwowego, a także perspektywy dalszego rozwoju przemysłu chemicznego i petrochemicznego sprawiają, że polski sektor naftowy stoi przed szeregiem strategicznych wyzwań inwestycyjnych. Ich realizacja będzie miała znaczenie nie tylko dla utrzymania tempa wzrostu gospodarczego, lecz również dla zwiększenia bezpieczeństwa energetycznego oraz odporności państwa na potencjalne kryzysy.

Brak koordynacji transformacji energetycznej i nieokreślony model docelowy polskiego systemu elektroenergetycznego

dr inż. Paweł Szczeszek

Abstrakt:

Artykuł diagnozuje fundamentalne słabości polskiej transformacji energetycznej: brak jednego dokumentu strategicznego, fragmentaryczność procesu reform i nieokreślony model docelowy systemu elektroenergetycznego. Autor analizuje narastające koszty systemowe związane z rosnącym udziałem niesterowalnych OZE oraz krytycznie ocenia unijne regulacje Fit for 55 i ich wpływ na polską energetykę, przemysł i ciepłownictwo. Formułuje postulaty dotyczące pilnej potrzeby koordynacji procesu transformacji.

Słowa kluczowe: transformacja energetyczna, system elektroenergetyczny, OZE, koszty systemowe, polityka energetyczna, Fit for 55, koordynacja

Wprowadzenie

Transformacja energetyczna stanowi obecnie jeden z najważniejszych procesów gospodarczych i infrastrukturalnych zachodzących w Polsce oraz całej Unii Europejskiej. Skala zmian obejmuje jednocześnie sektor wytwarzania energii, przemysł, transport, budownictwo, rynek surowców oraz finanse publiczne. Proces ten wymaga nie tylko ogromnych nakładów inwestycyjnych, lecz przede wszystkim długoterminowej strategii państwa, zdolnej do pogodzenia bezpieczeństwa energetycznego oraz konkurencyjności gospodarki.

W ostatnich dwóch latach transformacja energetyczna w Polsce realizowana jest jednak w sposób, który budzi istotne wątpliwości natury strategicznej. Dotyczą one przede wszystkim braku spójnej koordynacji działań, nieokreślenia docelowego modelu krajowego systemu energetycznego oraz niedostatecznej transparentności w zakresie przyszłych kosztów energii elektrycznej. W efekcie rośnie ryzyko prowadzenia transformacji w sposób reaktywny, oparty na doraźnych decyzjach regulacyjnych i politycznych, zamiast na wieloletnim planowaniu systemowym.

Problemy te mają charakter fundamentalny, ponieważ wpływają zarówno na poziom bezpieczeństwa energetycznego państwa, jak i na zdolność polskiej gospodarki do utrzymania konkurencyjności w kolejnych dekadach.

1. Brak koordynacji transformacji energetycznej

1.1. Fragmentaryczny charakter procesu transformacji

Jednym z podstawowych problemów obecnej transformacji energetycznej jest brak jednego, konsekwentnie realizowanego centrum koordynacyjnego odpowiedzialnego za całość procesu. Poszczególne elementy transformacji rozwijane są w oderwaniu od siebie, często w różnych horyzontach czasowych i przy odmiennych założeniach ekonomicznych.

Dotyczy to w szczególności:

- rozwoju odnawialnych źródeł energii,
- modernizacji i rozbudowy sieci elektroenergetycznych,
- budowy magazynów energii,
- rozwoju energetyki jądrowej,
- rynku mocy,
- polityki dla źródeł opartych na paliwach kopalnych,
- oraz mechanizmów wsparcia dla przemysłu energochłonnego.

Brakuje instytucji posiadającej realne kompetencje do integrowania tych obszarów w jeden spójny model funkcjonowania systemu energetycznego. W rezultacie decyzje inwestycyjne podejmowane są często niezależnie od siebie, co zwiększa ryzyko powstawania kosztownych niespójności infrastrukturalnych.

Przykładem może być dynamiczny rozwój odnawialnych źródeł energii przy jednoczesnym niewystarczającym tempie modernizacji sieci przesyłowych i dystrybucyjnych. Powoduje to rosnące problemy z przyłączaniem nowych instalacji, częste ograniczenia generacji energii z OZE oraz coraz większe problemy dla systemu w okresach nieprzyjaznych pogodowo dla OZE. Oznacza to, że część inwestycji realizowana jest szybciej niż zdolność systemu do ich absorpcji.

1.2. Brak stabilności regulacyjnej

Transformacja energetyczna wymaga przewidywalności regulacyjnej w perspektywie co najmniej kilkunastu lat. Tymczasem w Polsce polityka energetyczna charakteryzuje się znaczną zmiennością przepisów i mechanizmów wsparcia.

W ostatnich latach wielokrotnie zmieniano:

- zasady funkcjonowania rynku energii,
- systemy wsparcia dla OZE,
- regulacje dotyczące energetyki prosumenckiej,
- zasady taryfowania energii,
- mechanizmy zamrażania cen,
- oraz przepisy wpływające na opłacalność inwestycji energetycznych.

Tego rodzaju niestabilność prowadzi do wzrostu ryzyka inwestycyjnego. Inwestorzy prywatni oraz instytucjonalni oczekują bowiem przewidywalności otoczenia regulacyjnego, szczególnie w sektorze wymagającym wielomiliardowych nakładów i wieloletnich okresów zwrotu.

Brak stabilności powoduje również wzrost kosztu kapitału, co bezpośrednio przekłada się na wyższe ceny energii dla odbiorców końcowych. Im większa niepewność regulacyjna, tym wyższe ryzyko uwzględniane przez instytucje finansowe w wycenie projektów energetycznych.

1.3. Niedostateczna synchronizacja polityki energetycznej i przemysłowej

Transformacja energetyczna nie jest wyłącznie projektem klimatycznym. W praktyce stanowi również głęboki proces przebudowy struktury gospodarki. Z tego

względu polityka energetyczna powinna być ściśle powiązana z polityką przemysłową państwa.

Obecnie trudno jednak dostrzec spójną strategię określającą:

- które sektory przemysłu mają zostać objęte szczególną ochroną konkurencyjności,
- jakie branże mają stanowić fundament nowej gospodarki niskoemisyjnej,
- oraz w jaki sposób państwo zamierza ograniczać ryzyko deindustrializacji wynikające z wysokich cen energii.

Problem ten jest szczególnie istotny dla przemysłu energochłonnego, który już obecnie mierzy się z istotnie wyższymi kosztami energii niż konkurenci spoza Europy. Bez odpowiedniej koordynacji transformacja może prowadzić do przenoszenia produkcji poza Unię Europejską, co osłabi zarówno krajową gospodarkę, jak i bezpieczeństwo ekonomiczne państwa.

2. Brak wskazanego docelowego modelu systemu energetycznego

2.1. Niejasność strategicznej wizji państwa

Jednym z najpoważniejszych problemów polskiej transformacji energetycznej jest brak jednoznacznie określonego modelu docelowego systemu elektroenergetycznego.

Nie przedstawiono dotychczas spójnej odpowiedzi na pytania:

- jaka ma być docelowa struktura miksu energetycznego,
- jaki udział mają posiadać poszczególne technologie,
- jaka będzie rola źródeł stabilnych,
- oraz w jaki sposób państwo zamierza utrzymać bezpieczeństwo dostaw energii w warunkach rosnącego udziału źródeł niestabilnych.

W debacie publicznej funkcjonują równolegle różne, często sprzeczne koncepcje rozwoju energetyki:

- model oparty głównie na OZE,
- model hybrydowy z istotną rolą gazu,
- model zakładający dominację energetyki jądrowej w długim okresie,
- oraz koncepcje oparte na energetyce rozproszonej i lokalnych magazynach energii.

Brak jednoznacznego określenia kierunku powoduje, że inwestycje infrastrukturalne realizowane są bez pełnej wiedzy o docelowej architekturze systemu.

2.2. Problem źródeł stabilnych i bezpieczeństwa systemu

Transformacja energetyczna oparta na dynamicznym wzroście udziału odnawialnych źródeł energii wymaga równoczesnego rozwijania źródeł stabilizujących system elektroenergetyczny.

Do dziś nie określono jednak precyzyjnie:

- jaka ma być rola gazu ziemnego jako paliwa przejściowego,
- jak długo i w jakim charakterze funkcjonować mają jednostki węglowe,
- jakie moce rezerwowe będą utrzymywane,
- oraz jaki poziom bezpieczeństwa energetycznego państwo uznaje za akceptowalny.

Brakuje także jasnej odpowiedzi dotyczącej docelowej roli energetyki jądrowej. Mimo wieloletnich deklaracji projekt elektrowni jądrowych nadal znajduje się na etapie przygotowawczym, co zwiększa niepewność dotyczącą przyszłej struktury systemu.

W konsekwencji powstaje ryzyko wystąpienia luki mocy w okresie przejściowym pomiędzy wygaszaniem źródeł konwencjonalnych a uruchomieniem nowych stabilnych jednostek wytwórczych.

2.3. Niedostosowanie infrastruktury sieciowej

Brak jasno określonego modelu docelowego utrudnia również planowanie rozwoju infrastruktury przesyłowej i dystrybucyjnej.

Innego typu sieci wymaga system:

- scentralizowany,
- oparty głównie na dużych elektrowniach jądrowych,
- a innego system rozproszony z dominacją lokalnych źródeł OZE i magazynów energii.

Bez określenia docelowej architektury trudno efektywnie planować:

- lokalizację inwestycji sieciowych,
- skalę koniecznych modernizacji,
- poziom cyfryzacji systemu,
- oraz rozwój inteligentnych sieci energetycznych.

W efekcie istnieje ryzyko ponoszenia wysokich kosztów infrastrukturalnych bez gwarancji, że będą one zgodne z długoterminowym kierunkiem rozwoju systemu.

3. Brak transparentnych symulacji kosztów energii elektrycznej

3.1. Niedostateczna przejrzystość ekonomiczna transformacji

Transformacja energetyczna jest procesem niezwykle kosztownym. Obejmuje bowiem:

- budowę nowych źródeł wytwórczych,
- modernizację sieci,
- rozwój magazynów energii,
- systemy bilansowania,
- koszty rezerw mocy,
- oraz finansowanie mechanizmów wsparcia.

Pomimo tego w debacie publicznej brakuje kompleksowych i transparentnych analiz pokazujących, jak obecny model transformacji wpłynie na ceny energii w perspektywie najbliższych 10–20 lat.

Społeczeństwo oraz przedsiębiorcy nie otrzymują pełnej informacji dotyczącej:

- prognozowanych kosztów systemowych,
- przewidywanych taryf,
- wpływu polityki klimatycznej,
- kosztów ETS,
- oraz skali koniecznych dopłat publicznych.

Brak takich analiz ogranicza możliwość prowadzenia racjonalnej debaty o kosztach i korzyściach transformacji.

3.2. Rosnące koszty systemowe

W dyskusji publicznej często eksponowane są spadające koszty produkcji energii z odnawialnych źródeł energii. Znacznie rzadziej analizowane są natomiast koszty systemowe wynikające z rosnącego udziału źródeł niestabilnych.

Należą do nich między innymi:

- koszty bilansowania systemu,
- koszty utrzymywania rezerw mocy,
- wydatki na magazyny energii,
- rozbudowa sieci przesyłowych,
- koszty redysponowania energii,
- oraz rekompensaty za ograniczenia generacji.

W praktyce oznacza to, że nawet przy spadku kosztów samej produkcji energii całkowite koszty funkcjonowania systemu elektroenergetycznego mogą nadal rosnąć.

Brak transparentnego przedstawiania tych zależności prowadzi do uproszczenia debaty publicznej i utrudnia ocenę rzeczywistej efektywności ekonomicznej poszczególnych technologii.

3.3. Ryzyko utraty konkurencyjności gospodarki

Jednym z kluczowych wyzwań transformacji energetycznej pozostaje utrzymanie konkurencyjności krajowej gospodarki. Wysokie ceny energii stanowią

obecnie jeden z głównych czynników wpływających na atrakcyjność inwestycyjną państwa.

Brak długoterminowych prognoz cen energii utrudnia przedsiębiorstwom:

- planowanie inwestycji,
- ocenę opłacalności produkcji,
- oraz budowanie strategii rozwoju.

Problem ten szczególnie dotyczy sektorów energochłonnych, takich jak:

- hutnictwo,
- chemia,
- produkcja nawozów,
- cementownie,
- oraz przemysł papierniczy i szklarski.

Jeżeli transformacja energetyczna będzie prowadzić do trwałego wzrostu kosztów energii bez odpowiednich mechanizmów kompensacyjnych, może dojść do stopniowej utraty części potencjału przemysłowego kraju.

4. Wnioski

Transformacja energetyczna jest procesem koniecznym i nieuniknionym. Jej powodzenie zależy jednak nie wyłącznie od skali inwestycji, lecz przede wszystkim od jakości zarządzania strategicznego państwa.

Obecny model transformacji w Polsce ujawnia trzy zasadnicze problemy:

- brak skutecznej koordynacji procesu,
- brak jasno określonego modelu docelowego systemu energetycznego,
- oraz brak transparentnych analiz dotyczących przyszłych kosztów energii.

Bez rozwiązania tych problemów istnieje ryzyko prowadzenia transformacji w sposób niespójny, kosztowny oraz obniżający konkurencyjność gospodarki.

Państwo powinno zatem skoncentrować się na:

- stworzeniu długoterminowej strategii energetycznej,
- określeniu docelowej architektury systemu,
- zapewnieniu stabilności regulacyjnej,
- oraz transparentnym komunikowaniu rzeczywistych kosztów transformacji.

Tylko wówczas możliwe będzie pogodzenie celów klimatycznych z bezpieczeństwem energetycznym i interesem gospodarczym państwa.

Wysokie koszty energii i pogarszająca się konkurencyjność polskiej gospodarki w świetle najnowszych regulacji unijnych i działań państw członkowskich UE

Mateusz Wodejko

Abstrakt:
Artykuł analizuje wpływ wysokich kosztów energii na konkurencyjność polskiej gospodarki. Autor ocenia skalę odpływu środków z tytułu ETS, koszty implementacji pakietu Fit for 55, dyrektywy EPBD i EED oraz rosnące zagrożenie dla polskiego ciepłownictwa i przemysłu. Wskazuje na brak spójnej polskiej odpowiedzi na europejski kryzys energetyczny i coraz wyraźniejszy efekt dezindustrializacji.
Słowa kluczowe: koszty energii, ETS, transformacja energetyczna, konkurencyjność gospodarcza, Fit for 55, EPBD, EED, przemysł

W 2025 roku ceny energii elektrycznej w Polsce znajdowały się w górnej połowie europejskiej stawki. Jednak wycena kontraktów na 2027 rok stawia nas wśród najdroższych rynków energii w Europie. Oznaczać to będzie znaczące negatywne konsekwencje dla odbiorców, zwłaszcza przemysłowych, którzy potrzebują przewidywalnych i konkurencyjnych cen energii, aby zaplanować

swoją produkcję. Będzie to dotykać zarówno istniejących biznesów w Polsce jak i możliwości pozyskania nowych inwestycji, np. w centra danych.

Jednocześnie globalne emisje rosną, choć UE i kraje członkowskie obciążają swoje gospodarki ogromnymi kosztami z tytułu Zielonego Ładu. Tym samym Unia Europejska pogrąża – według wszelkich danych ekonomicznych – swój przemysł i uzależnia się od produkcji innych krajów nie zwracających większej uwagi na swoje emisje.

W tym czasie z Polski wypływają miliardy euro na zakup uprawnień do emisji CO_2 ponad limity uprawnień jakimi dysponuje nasz kraj. Istotna część z polskich opłat za emisje CO_2 trafia do innych krajów Unii Europejskiej oraz na programy unijnego Zielonego Ładu.

Jak wyliczył Business Insider w artykule „Czy ETS to koszt dla polskiej gospodarki? Podajemy kluczowe liczby." z 24 marca 2026 r.: „Od 2018 r. do lutego br. Ministerstwo Finansów sprzedało uprawnienia do emisji CO_2 łącznie za 128 mld zł. W tym samym czasie polskie firmy były zmuszone kupić te same instrumenty za 174 mld zł, a są to dane niepełne, bo dla największych emitentów (PGE, Enea i Tauron) bez czwartego kwartału 2025 r., więc kwota będzie dużo wyższa.".

Nie jest zatem prawdą twierdzenie, że Polska zarabia na sprzedaży swoich praw do emisji CO_2 – prawdą jest twierdzenie, że polska gospodarka traci znaczące środki na unijnym systemie uprawnień do emisji CO_2 na rzecz gospodarek innych krajów unijnych. Część tych środków odzyskujemy w postaci unijnych subsydiów, które jednak trafiają głównie na wsparcie inwestycji w źródła energii, które dostarczają drogiej, a nie taniej energii.

Jednocześnie ostatnie lata to okres wzmożenia regulacyjnego Unii Europejskiej, szczególnie w zakresie dotykającym elektroenergetyki i energetyki cieplnej.

O szeregu regulacji unijnych dotyczących Zielonego Ładu – pakietu Fit for 55 w zakresie elektroenergetyki i ich destruktywnym wpływie na polską i unijną gospodarkę napisano wiele i nie ma potrzeby w niniejszym artykule powtarzać szerzej tych informacji.

Natomiast należy wskazać, że to dopiero początek klimatycznej rewolucji w rozumieniu Unii Europejskiej. UE zaostrza klimatyczny kurs. Komisja Europejska zaproponowała ścięcie emisji aż o 90 proc. do 2040 r. W rezultacie w marcu 2026 r. Rada UE przyjęła nowy pośredni cel klimatyczny dla państw członkowskich. Zakłada on redukcję emisji gazów cieplarnianych netto do 2040 r. o 90 proc. w porównaniu z poziomem z 1990 r. Jego realizacja ma przybliżyć UE do osiągnięcia neutralności klimatycznej do 2050 r. we wszystkich sektorach gospodarki.

Wdrożenie redukcji emisji o 90 proc. do 2040 r. de facto oznaczałoby likwidację polskiego przemysłu, usług transportowych i rolnictwa wielkoobszarowego. Wpływ na polską gospodarkę i na polskie PKB byłby katastrofalny.

W debacie publicznej w mniejszym stopniu niż w przypadku elektroenergetyki pojawiają się informacje o negatywnym wpływie unijnych regulacji na energetykę cieplną. Tymczasem ten negatywny wpływ na funkcjonowanie polskiej gospodarki i dobrobyt polskich obywateli będzie ogromny.

Do 29 maja 2026 r. Polska miała wdrożyć unijną dyrektywę budynkową EPBD. Całkowity koszt dostosowania do dyrektywy EPBD szacowany jest na ok. 2,5 biliona złotych (ok. 0,5 bln zł na przebudowę systemów ciepłowniczych i wymianę źródeł ciepła oraz ok. 2 bln złotych na termomodernizację). Za dostosowanie do dyrektywy budynkowej zapłacą właściciele domów, mieszkań, samorządy oraz firmy – 2,5 bln zł oznacza ok. 70 tys. zł kosztów na każdego mieszkańca naszego kraju, zatem przykładowo 75 tysięcy mieszkańców miasta Siedlce zapłaci łącznie ok. 5,3 mld zł.

Z kolei Ministerstwo Energii opublikowało projekt ustawy o zmianie ustawy – Prawo energetyczne (druk UC121) implementującej przepisy unijnej Dyrektywy EED w sprawie efektywności energetycznej – o ogromnym i negatywnym wpływie na polskie ciepłownictwo systemowe.

Dyrektywa EED narzuca rosnące wymogi dla polskiego ciepłownictwa m.in. wymuszające odejście od węgla, a docelowo od gazu – raport Polskiego Towarzystwa Energetyki Cieplnej z 2024 r. szacuje koszty wdrożenia tej dyrektywy czyli dekarbonizacji polskiego ciepłownictwa w zależności od przyjętego wariantu na kwoty od 299 mld zł do 466 mld zł – podczas gdy przykładowo łączne nakłady inwestycyjne polskiego ciepłownictwa systemowego za 2024 r. wg danych URE to ok. 4,7 mld zł.

Dyrektywa EED nakłada od roku 2028 kolejne rosnące wymogi co do uznania systemu ciepłowniczego za tzw. efektywny system ciepłowniczy – podczas gdy obecnie jedynie ok. 22% polskich ciepłowni spełnia kryterium efektywnego systemu ciepłowniczego. Tymczasem w świetle przepisów unijnych bez spełnienia tego kryterium nie będą dostępne dla ciepłowni środki rządowe na dofinansowanie modernizacji instalacji oraz nie będzie możliwości przyłączania nowych odbiorców i budynków (w związku z wymogami dyrektywy budynkowej).

Pomimo tych rozlicznych zagrożeń dla polskiego ciepłownictwa i dla Polaków wynikających z unijnych regulacji Zielonego Ładu brak jest jakichkolwiek konkretów co do przyszłości ciepłownictwa, np. mimo rządowych deklaracji brak jest strategii dla tego sektora.

Wdrożenie dyrektywy EED zaskutkuje ogromnymi podwyżkami cen ciepła dla Polaków. Zgodnie z aktualną informacją Prezesa URE dotyczącą średnich cen ciepła za ostatni rok (2025), cena ciepła wytworzonego w oparciu o paliwo węglowe jest bardzo konkurencyjna i wynosi 103,16 zł/GJ versus 131,95 zł/GJ ciepła wytworzonego w oparciu o paliwo gazowe – zatem ciepło z węgla jest średnio o 30% tańsze od ciepła z paliwa gazowego. Z kolei gdy ciepło z gazu zostanie zastąpione alternatywnymi rozwiązaniami wymagającymi ogromnych nakładów inwestycyjnych Polaków czekają dalsze rekordowe podwyżki cen ciepła systemowego.

Do ww. rosnących kosztów w obszarze ciepłownictwa dodajmy jeszcze koszty wynikające z wdrożenia ETS 2 – prawdopodobnie od 2028 r. – i mamy pełen obraz dramatu w tym obszarze dla Polaków i dla polskiej gospodarki. Dla polskiej gospodarki – bo rosnące koszty życia będą ograniczały dochód rozporządzalny polskich gospodarstw domowych zmniejszając zarówno wydatki na konsumpcję jak i oszczędności Polaków.

W tym miejscu należy pokrótce prześledzić działania jakie podejmowane były przez organy Unii Europejskiej i przez państwa członkowskiej aby ograniczyć wzrost kosztów energii i poprawić kondycję przemysłu w UE – ponieważ świadomość tych zagrożeń niewątpliwie zaistniała, natomiast unijne rozumienie problemu i proponowane przez UE rozwiązania z perspektywy Polski są kontrproduktywne.

W czerwcu 2024 r. weszło w życie rozporządzenie Unii Europejskiej tzw. Net Zero Industry Act, które miało na celu stworzenie sprzyjających warunków dla rozwoju technologii o zerowej emisji netto, usprawnienie procesów administracyjnych i pozwoleniowych, a także wspieranie innowacji i rozwój umiejętności w sektorze przemysłowym.

We wrześniu 2024 r. został opublikowany Raport Draghiego stanowiący de facto diagnozę braku konkurencyjności państw członkowskich w różnych obszarach gospodarki światowej, ze szczególnym uwzględnieniem sektora energetycznego i surowcowego. Draghi ostrzegł, że jeśli UE nie dogoni swoich rywali, czeka ją „powolna agonia". Wskazał, że UE potrzebuje znacznie bardziej skoordynowanej polityki przemysłowej, szybszych decyzji i ogromnych inwestycji, jeśli chce dotrzymać kroku Stanom Zjednoczonym i Chinom.

Ogłoszony w lutym 2025 r. Clean Industrial Deal – plan wzmocnienia konkurencyjności UE poprzez dekarbonizację i przyspieszenie elektryfikacji jako motory wzrostu przemysłu, które też miałyby poskutkować obniżeniem kosztów energii w UE.

CISAF (Clean Industrial Deal State Aid Framework) wszedł w życie w czerwcu 2025 r. – dokument określający ramowe zasady udzielania przez państwa

członkowskie UE pomocy publicznej przyspieszającej wdrażanie założeń Clean Industrial Deal. Generalnie w ramach CISAF pomoc publiczna jest możliwa jeżeli częściowo finansuje rozwój sektora OZE bądź innych „czystych" technologii.

Industrial Accelator Deal przedstawiony przez Komisję Europejską w marcu 2026 r. składa się z czterech filarów – (1) europejskiej preferencji w zamówieniach publicznych, (2) wymogów co do dzielenia się przez zagranicznych inwestorów technologiami, zatrudniania miejscowych pracowników czy tworzenia spółek joint venture wspólnie z europejskimi firmami, (3) przyspieszenia i usprawnienia procesu wydawania pozwoleń dla inwestycji w dekarbonizację, (4) tworzenie Industrial Accelertion Areas (obszarów przyspieszenia przemysłowego).

5 marca 2026 r. Rada UE przyjęła nowy pośredni cel klimatyczny dla państw członkowskich tj. ścięcie emisji aż o 90 proc. do 2040 r.,

Jednocześnie europejscy politycy obiecywali w I kwartale 2026 poluzowanie przepisów dot. emisji dla przemysłu. Na szczycie Rady Europejskiej, który zakończył się 20 marca 2026 r., rozważana była kwestia poprawy konkurencyjności przemysłu energochłonnego – poprzez obniżenie cen energii. Było to m.in. pokłosiem lutowego szczytu przemysłu europejskiego w Antwerpii, na którym najważniejsi politycy europejscy – w tym kanclerz Niemiec Friedrich Merz i prezydent Francji Emmanuel Marcon – spotkali się z przedstawicielami biznesu energochłonnego, aby omówić plan awaryjny poprawiający warunki funkcjonowania tych branż w Europie.

Efektem tego szczytu była seria politycznych wystąpień. A zbieżność z jednej strony decyzji o dalszym cięciu emisji a z drugiej strony dyskusji o poprawie konkurencyjności europejskiego przemysłu wydaje się absurdalna z polskiej perspektywy.

Oczywiście przedstawione przez Komisję Europejską w maju 2026 r., odnoszące się do oczekiwań Rady Europejskiej, propozycje zmian systemu ETS mają kosmetyczny charakter, a niektóre normy są wręcz zaostrzane. Rynek ETS zareagował na te propozycje wzrostem.

W propozycji Brukseli zdecydowana większość sektorów przemysłowych otrzyma mocno obcięty przydział darmowych uprawnień w porównaniu do stanu obecnego. Niektóre sektory, jak stalowy czy papierniczy, nawet ponad 30% niższy niż w latach 2021-2025.

Pokazuje to, że Komisja Europejska nadal porusza się przede wszystkim w logice zaostrzania reguł systemu ETS, choć polityczna debata po marcowej Radzie Europejskiej przesunęła się w stronę ochrony konkurencyjności przemysłu i problemu wysokich cen energii.

W wyniku takiego podejścia Brukseli do działań na poziomie UE obniżanie cen energii dla przemysłu zaczęło być realizowane za pośrednictwem subsydiów przez niektóre państwa członkowskie, skutkując przewagą konkurencyjną tych państw w Europie.

Na jesieni 2025 r. rządząca w Niemczech koalicja porozumiała się co do ograniczenia cen energii elektrycznej dla firm energochłonnych, np. z branż motoryzacyjnej, chemicznej czy stalowej. Po zatwierdzeniu programu przez UE w maju 2026 r. płacą one za połowę swojego zużycia energii cenę docelową wynoszącą 50 euro za megawatogodzinę, natomiast różnicę między ceną rynkową a tą stawką pokrywa państwo. Mechanizm został zaprojektowany tak, aby mieścił się w ramach nowego unijnego systemu CISAF, który określa maksymalny dopuszczalny poziom obniżki (do 50% ceny hurtowej) oraz dolny limit efektywnej ceny (50 euro za MWh). Preferencyjna cena obejmie maksymalnie połowę rocznego wolumenu energii zużywanego przez przedsiębiorstwo, natomiast pozostała część jest rozliczana według cen rynkowych.

Firmy korzystają z obniżonych stawek pod warunkiem spełnienia wymogów dotyczących energochłonności, wprowadzenia systemów zarządzania energią, przedstawienia planów inwestycji w efektywność energetyczną i dekarbonizację oraz utrzymania działalności produkcyjnej na terenie Unii Europejskiej. Środki mają przynieść przedsiębiorstwom i konsumentom ulgę rzędu dziesięciu miliardów euro rocznie.

Zgody na programy pomocy publicznej w ramach CISAF UE wydała również dla Włoch, Bułgarii, Słowenii, Francji, Hiszpanii, Węgier.

W ramach innych działań włoski rząd w lutym 2026 r. przyjął dekret energetyczny o wartości ponad 3 mld euro, którego kluczowym elementem jest refundacja kosztów uprawnień do emisji CO_2 dla elektrowni gazowych, Nowe rozwiązanie zakłada, że koszty emisji nie będą przenoszone na odbiorców końcowych. W praktyce oznacza to usunięcie wpływu cen uprawnień do emisji CO_2 z rachunków za prąd.

W następstwie kolejnej włoskiej inicjatywy Komisja Europejska ogłosiła 3 czerwca 2026 r., że wydatki państw związane z wysokimi cenami energii będą traktowane ulgowo w ramach unijnych reguł budżetowych. Taka klauzula zostanie dodana do obowiązującego już wyłączenia z unijnej dyscypliny wydatków na obronność. Na wniosek państwa członkowskiego zakres obecnej tzw. klauzuli wyjścia dla obronności może zostać rozszerzony. Państwa w ramach przewidzianego na wydatki obronne pułapu 1,5 proc. PKB będą mogły otrzymać roczny limit w wysokości 0,3 proc. PKB na wydatki związane z energią. Będzie on dostępny w latach 2026–2028 i łącznie wyniesie 0,6 proc. PKB. Państwa, które wykorzystały już pełną

elastyczność w ramach klauzuli wyjścia na wydatki obronne, będą mogły przekroczyć pułap 1,5 proc. PKB pod warunkiem przeprowadzenia dodatkowej oceny stabilności fiskalnej.

Z kolei pod koniec maja 2026 r. prezydent Emmanuel Macron postanowił skorzystać z tego, że dzięki energetyce jądrowej Francja jest jednym z nielicznych państw UE, które posiada zdolność produkowania relatywnie taniej i pogodowo-niezależnej energii, w ilościach powyżej własnych potrzeb. W rezultacie Macron ogłosił plan totalnego zelektryfikowania Francji -tzw. "Plan d'électrification des usages" (Plan elektryfikacji procesów użytkowych).

W następstwie corocznych inwestycji w wysokości 10 mld euro i administracyjnych nakazów energia elektryczna ma stanowić podstawowe źródło zasilania transportu drogowego, przemysłu, rolnictwa oraz budynków.

Jednocześnie Francja przygotowuje budowę sześciu nowych reaktorów jądrowych o łącznej mocy ok. 10 GW i planuje realizację kolejnych ośmiu reaktorów. Z kolei operator sieci energetycznych Francji RTE ma wydać 100 mld euro na modernizację i rozbudowę sieci energetycznych.

Te działania – oprócz wsparcia konkurencyjności francuskiego przemysłu – mają swój cel polityczny zewnętrzny, a mianowicie ograniczenie zależności od zagranicznych dostawców gazu i ropy oraz wpływanie na sąsiednie państwa zależne od stabilnych i konkurencyjnych cenowo dostaw francuskiej energii elektrycznej.

Plan prezydenta Macrona konkuruje ze wspieraną przez Berlin "European Grids Package", przyjętą w grudniu 2025 r. przez Komisję Europejską strategią zakładającą wydanie 1,2 biliona euro na modernizację, rozbudowę i centralizację sieci energetycznej w Unii Europejskiej. Tak aby w wietrzne i słoneczne dni, gdy nastąpi nadprodukcja energii elektrycznej w krajach takich jak Niemcy czy Hiszpania, była ona dystrybuowana na obszarze całej UE.

Zatem zapewnienie stabilnych i niedrogich dostaw energii elektrycznej staje się również kluczowym elementem realizowania polityki zagranicznej i budowania swojej pozycji czy wręcz elementem strategicznej rozgrywki na poziomie Unii Europejskiej.

Takich inicjatyw a jednocześnie nie prowadzących do realnych działań dyskusji w Brukseli będzie coraz więcej bo Europa w przyspieszonym tempie traci swoje zdolności przemysłowe.

Firmy uciekają z inwestycjami z Europy – nie tylko z powodu kosztów energii – ale również dlatego, że nie mogą przewidzieć, czy ich produkcja nie zostanie za jakiś czas obciążona zielonymi normami, uniemożliwiającymi prowadzenie rentownej

działalności. Przykładem jest choćby niemiecki koncern surowcowy Aurubis – do niedawna stawiany za wzór za zastępowanie wydobycia recyclingiem złomów miedzianych, a teraz uciekający z produkcją z Unii Europejskiej do Stanów Zjednoczonych.

Jak opisuje to Puls Biznesu w artykule z 2 czerwca 2026 chiński szok 2.0 dotarł też do nas. Tanie towary zaczynają niszczyć polski przemysł. Branże przemysłowe, które muszą bezpośrednio konkurować z chińskimi firmami, od kilku lat znajdują się w regresie. Od 2023 r. produkcja w branżach z wysoką ekspozycją na szok chiński – czyli tam, gdzie import z Chin do Polski rośnie najmocniej – skurczyła się o 5,8 proc. Jak słusznie wskazuje Puls Biznesu – zaczęła się kolejna era polityki przemysłowej. Brak polityki przemysłowej to najgorsza opcja. Takie są dziś realia światowej gospodarki.

Dominujący w takich krajach jak Niemcy paradygmat rozwoju gospodarczego opartego na inwestycjach w technologie OZE czy inne „czyste" technologie" okazał się być fałszywy. Chiny zdominowały świat i Europę w produkcji tych technologii. Zarazem w wyniku zamykania kopalń, braku nowych inwestycji, wzrosła zależność Europy od reszty świata w imporcie paliw kopalnych – węgla czy gazu.

Jak wskazano w niniejszym artykule organy Unii Europejskiej, czy zafiksowane na punkcie polityki klimatycznej kraje członkowskie UE, są w stanie odpowiedzieć na tę dramatyczną sytuację jedynie subsydiując tracącą konkurencyjność gospodarkę – dopóki można jeszcze pozyskać środki od unijnych obywateli czy z kolejnych zaciąganych długów.

Pozostaje zadać pytania – quo vadis Unio Europejska, dlaczego jest to droga samobójcza gospodarczo i czy my Polacy jesteśmy na nią skazani.

Społeczna akceptacja projektów wydobywczych surowców krytycznych jako warunek bezpieczeństwa gospodarczego i transformacji energetycznej Europy

Kasjan Wyligała

Abstrakt:
Artykuł analizuje problem społecznej akceptacji projektów wydobywczych surowców krytycznych jako kluczowy warunek realizacji europejskiej polityki surowcowej. Autor identyfikuje główne źródła konfliktów: obawy środowiskowe, niski poziom wiedzy o współczesnych technologiach wydobywczych, brak zaufania do instytucji publicznych i dezinformacja w mediach społecznościowych. Wskazuje na rozwiązania oparte na profesjonalnej komunikacji, edukacji i mechanizmach partycypacyjnych.
Słowa kluczowe: surowce krytyczne, akceptacja społeczna, wydobycie, NIMBY, komunikacja społeczna, bezpieczeństwo surowcowe, transformacja energetyczna

Wstęp

W XXI wieku surowce krytyczne stały się jednym z najważniejszych elementów globalnej rywalizacji gospodarczej oraz geopolitycznej. Dynamiczny rozwój technologii, transformacja energetyczna, cyfryzacja gospodarki, rozwój sektora elektromobilności oraz wzrost znaczenia przemysłu obronnego powodują systematyczny wzrost

zapotrzebowania na metale i minerały uznawane za strategiczne dla funkcjonowania nowoczesnych państw.

Do grupy surowców krytycznych zaliczane są między innymi lit, wolfram, molibden, miedź, nikiel, grafit, kobalt, mangan oraz pierwiastki ziem rzadkich. Ich znaczenie wykracza obecnie daleko poza tradycyjne zastosowania przemysłowe. Są one podstawą funkcjonowania nowoczesnych technologii, energetyki odnawialnej, przemysłu elektronicznego, telekomunikacyjnego oraz zbrojeniowego. Bez dostępu do tych surowców niemożliwe byłoby funkcjonowanie nowoczesnych gospodarek opartych na technologiach cyfrowych i transformacji energetycznej.

Jednocześnie Europa pozostaje w dużym stopniu uzależniona od importu strategicznych surowców z państw trzecich, przede wszystkim z Chin. W ostatnich latach coraz wyraźniej dostrzegalne stało się ryzyko związane z nadmierną koncentracją globalnych łańcuchów dostaw. Pandemia COVID-19, napięcia geopolityczne, wojna w Ukrainie oraz narastająca rywalizacja gospodarcza między Stanami Zjednoczonymi a Chinami pokazały, że bezpieczeństwo surowcowe powinno być traktowane jako jeden z fundamentów bezpieczeństwa państw.

W odpowiedzi na te wyzwania Unia Europejska rozpoczęła działania mające na celu zwiększenie niezależności surowcowej poprzez rozwój własnych projektów wydobywczych, przetwórczych oraz recyklingowych. Jednym z najważniejszych elementów tej strategii jest Critical Raw Materials Act (CRMA), którego celem jest przyspieszenie realizacji strategicznych inwestycji surowcowych na terenie Unii Europejskiej.

Rozwój nowych projektów wydobywczych w Europie napotyka jednak liczne bariery. Oprócz wyzwań administracyjnych, środowiskowych i finansowych coraz większego znaczenia nabiera kwestia społecznej akceptacji inwestycji. W wielu przypadkach to właśnie opór lokalnych społeczności staje się najpoważniejszym zagrożeniem dla realizacji projektów górniczych. W efekcie pojęcie Social License to Operate, czyli społecznej licencji na działalność, zaczyna odgrywać równie istotną rolę jak formalne decyzje administracyjne.

Znaczenie surowców krytycznych dla współczesnej gospodarki

Surowce krytyczne stanowią obecnie podstawę funkcjonowania nowoczesnej gospodarki światowej. Współczesny rozwój technologiczny jest bezpośrednio uzależniony

od dostępu do określonych metali i minerałów, których podaż staje się coraz bardziej ograniczona i skoncentrowana geograficznie.

Miedź jest jednym z najważniejszych surowców dla światowej energetyki i infrastruktury przesyłowej. Rozwój odnawialnych źródeł energii, sieci elektroenergetycznych oraz elektromobilności powoduje gwałtowny wzrost zapotrzebowania na ten metal. Samochody elektryczne wymagają wielokrotnie większej ilości miedzi niż pojazdy spalinowe, podobnie jak instalacje fotowoltaiczne czy farmy wiatrowe.

Lit, nikiel i kobalt są podstawowymi składnikami baterii wykorzystywanych w magazynowaniu energii oraz elektromobilności. Pierwiastki ziem rzadkich mają kluczowe znaczenie dla produkcji silników elektrycznych, turbin wiatrowych, elektroniki i nowoczesnych systemów wojskowych. Wolfram oraz molibden wykorzystywane są natomiast w sektorze obronnym, lotniczym oraz wysokotemperaturowym ze względu na swoje wyjątkowe właściwości fizyczne.

Znaczenie surowców krytycznych jest obecnie tak duże, że coraz częściej traktowane są one jako element strategicznej rywalizacji między państwami. Państwa posiadające kontrolę nad wydobyciem lub przetwórstwem tych surowców uzyskują istotną przewagę gospodarczą i polityczną.

Szczególne znaczenie posiadają Chiny, które dominują w globalnym przetwórstwie wielu surowców krytycznych. W przypadku niektórych pierwiastków kontrolują one ponad 80% światowych mocy przetwórczych. Taka sytuacja stanowi poważne zagrożenie dla bezpieczeństwa gospodarczego Europy i Stanów Zjednoczonych.

Europa przez wiele lat opierała swoją politykę gospodarczą na założeniu, że globalizacja zapewni stabilny i nieograniczony dostęp do surowców. Obecnie podejście to ulega zmianie. Coraz częściej podkreśla się konieczność budowy własnych zdolności wydobywczych i przetwórczych oraz skracania łańcuchów dostaw.

Rozwój projektów wydobywczych w Europie

Unia Europejska posiada znaczący potencjał geologiczny, jednak przez wiele lat rozwój sektora wydobywczego był ograniczany przez skomplikowane procedury administracyjne, wysokie koszty środowiskowe oraz brak społecznej akceptacji.

W wielu państwach europejskich górnictwo postrzegane było jako sektor schyłkowy, kojarzony przede wszystkim z negatywnym wpływem na środowisko.

Jednocześnie Europa stopniowo uzależniała się od importu surowców z państw trzecich, często o znacznie niższych standardach środowiskowych i społecznych.

W ostatnich latach podejście to zaczęło się zmieniać. Coraz częściej podkreśla się, że brak własnego wydobycia nie oznacza rezygnacji z eksploatacji surowców, lecz jedynie przeniesienie jej do innych części świata. W praktyce Europa nadal korzysta z ogromnych ilości metali i minerałów, jednak koszty środowiskowe i społeczne związane z ich wydobyciem ponoszą inne państwa.

W efekcie coraz większego znaczenia nabiera koncepcja odpowiedzialnego górnictwa realizowanego zgodnie z wysokimi standardami środowiskowymi, technologicznymi oraz społecznymi. Nowoczesne projekty wydobywcze wykorzystują zaawansowane technologie ograniczające wpływ na środowisko, systemy monitoringu jakości powietrza i wody, zamknięte obiegi technologiczne oraz cyfrowe systemy zarządzania procesami wydobywczymi.

Jednocześnie realizacja takich projektów wymaga bardzo wysokich nakładów inwestycyjnych oraz wieloletnich procedur administracyjnych. W wielu przypadkach proces od rozpoczęcia prac poszukiwawczych do uruchomienia kopalni trwa kilkanaście lat.

Dlatego jednym z najważniejszych wyzwań staje się ograniczenie ryzyk społecznych i politycznych, które mogą prowadzić do wieloletnich opóźnień lub całkowitego zablokowania inwestycji.

Social License to Operate – definicja i znaczenie

Pojęcie Social License to Operate oznacza poziom społecznej akceptacji dla działalności przedsiębiorstwa lub inwestycji. Nie jest to dokument administracyjny ani formalna zgoda wydawana przez urząd. Jest to raczej społeczny poziom zaufania wobec inwestora oraz przekonanie lokalnej społeczności, że działalność prowadzona jest w sposób odpowiedzialny, bezpieczny i transparentny.

W sektorze górniczym kwestia ta ma szczególne znaczenie ze względu na charakter inwestycji wydobywczych. Projekty górnicze są inwestycjami wieloletnimi, wymagającymi intensywnej ingerencji w środowisko naturalne oraz przestrzeń lokalną. Wpływają one na funkcjonowanie społeczności lokalnych, gospodarkę regionu, rynek pracy oraz infrastrukturę.

W praktyce brak społecznej akceptacji może prowadzić do licznych protestów, sporów sądowych, blokad administracyjnych oraz kampanii medialnych wymierzonych

przeciwko inwestycji. Coraz częściej okazuje się, że formalne uzyskanie wszystkich decyzji administracyjnych nie gwarantuje możliwości realizacji projektu.

Społeczna licencja na działalność opiera się przede wszystkim na zaufaniu. Mieszkańcy muszą mieć przekonanie, że inwestor działa w sposób odpowiedzialny i uwzględnia interes lokalnej społeczności. Kluczowe znaczenie ma tutaj transparentność komunikacji oraz gotowość do dialogu.

Istotnym elementem jest również długofalowe podejście do relacji społecznych. Budowanie społecznej akceptacji nie może ograniczać się wyłącznie do działań wizerunkowych prowadzonych na etapie uzyskiwania pozwoleń. Musi stanowić integralny element strategii funkcjonowania projektu przez cały okres jego realizacji.

Źródła konfliktów społecznych wokół inwestycji górniczych

Jednym z głównych powodów konfliktów społecznych jest obawa mieszkańców przed negatywnym wpływem inwestycji na środowisko naturalne. Szczególne emocje budzą kwestie związane z jakością wody, emisją hałasu, wpływem na krajobraz oraz potencjalnym zagrożeniem dla zdrowia mieszkańców.

W wielu przypadkach obawy te wynikają z doświadczeń historycznych związanych z działalnością przemysłową prowadzoną w przeszłości bez odpowiednich zabezpieczeń środowiskowych. W świadomości społecznej nadal funkcjonuje obraz górnictwa jako sektora silnie degradującego środowisko naturalne.

Drugim istotnym problemem jest niski poziom wiedzy dotyczącej współczesnych technologii wydobywczych. Współczesne projekty górnicze funkcjonują w zupełnie innych realiach technologicznych niż kilkadziesiąt lat temu. Stosowane są zaawansowane systemy zabezpieczeń środowiskowych, monitoring hydrogeologiczny oraz technologie minimalizujące wpływ na otoczenie.

Mimo to społeczeństwo często nie posiada wystarczającej wiedzy na temat nowoczesnego górnictwa. Powoduje to łatwość rozpowszechniania dezinformacji oraz wzrost emocji społecznych wokół projektów wydobywczych.

Istotnym źródłem konfliktów jest również brak zaufania do instytucji publicznych. W wielu państwach europejskich obserwowany jest spadek zaufania społecznego wobec administracji oraz dużych przedsiębiorstw. W efekcie mieszkańcy często zakładają, że inwestorzy ukrywają rzeczywiste ryzyka związane z projektem.

Coraz większą rolę odgrywają również media społecznościowe, które umożliwiają bardzo szybkie rozpowszechnianie informacji, często niezweryfikowanych lub opartych na emocjach. Konflikty lokalne mogą w krótkim czasie przekształcić się w ogólnokrajowe kampanie medialne.

Znaczenie edukacji i komunikacji społecznej

Współczesne projekty wydobywcze wymagają profesjonalnego podejścia do komunikacji społecznej. Coraz częściej podkreśla się, że dialog z lokalną społecznością powinien rozpoczynać się już na etapie prac poszukiwawczych.

Kluczowe znaczenie ma przekazywanie mieszkańcom rzetelnych informacji dotyczących charakteru projektu, technologii wydobywczych, potencjalnych zagrożeń oraz planowanych zabezpieczeń środowiskowych. Bardzo ważne jest również umożliwienie społeczności lokalnej realnego udziału w dyskusji.

Proces komunikacji nie może opierać się wyłącznie na jednostronnym przekazie informacyjnym. Mieszkańcy oczekują możliwości zadawania pytań, zgłaszania wątpliwości oraz uzyskiwania odpowiedzi od ekspertów.

Ważnym elementem budowania społecznej akceptacji jest również edukacja dotycząca znaczenia surowców krytycznych dla współczesnej gospodarki. Wielu mieszkańców nie zdaje sobie sprawy, że rozwój gospodarczy i technologiczny wymaga ogromnych ilości metali i minerałów.

Powstaje tutaj pewien paradoks. Społeczeństwa europejskie oczekują rozwoju nowoczesnych technologii, przemysłu zbrojeniowego, elektromobilności jednocześnie często sprzeciwiając się realizacji projektów wydobywczych niezbędnych do produkcji tych technologii.

Dlatego coraz częściej podkreśla się konieczność prowadzenia szerokiej debaty publicznej dotyczącej bezpieczeństwa surowcowego Europy oraz rzeczywistych kosztów transformacji energetycznej.

Polska i potencjał rozwoju projektów surowców krytycznych

Polska posiada istotny potencjał geologiczny w zakresie surowców strategicznych. Szczególne znaczenie mają zasoby miedzi, srebra, molibdenu oraz wolframu. Rozwój

nowych projektów wydobywczych może odegrać ważną rolę w budowie bezpieczeństwa surowcowego Europy.

Jednocześnie Polska posiada wieloletnie tradycje górnicze oraz rozwinięte kompetencje techniczne i inżynieryjne. Może to stanowić istotną przewagę konkurencyjną w rozwoju nowoczesnego sektora surowców krytycznych.

Rozwój takich inwestycji może przynieść szereg korzyści gospodarczych, w tym tworzenie nowych miejsc pracy, rozwój infrastruktury, wzrost wpływów podatkowych oraz zwiększenie znaczenia Polski w europejskim łańcuchu dostaw surowców strategicznych.

Jednak również w Polsce coraz większego znaczenia nabierają kwestie społeczne i środowiskowe. Sukces nowych projektów wydobywczych będzie zależał nie tylko od jakości złóż czy dostępności kapitału, ale również od zdolności budowania trwałych relacji społecznych.

Kluczowe znaczenie będzie miało odpowiedzialne podejście inwestorów do komunikacji społecznej, transparentności działań oraz uwzględniania interesów lokalnych społeczności.

Podsumowanie

Surowce krytyczne stają się jednym z najważniejszych elementów współczesnego bezpieczeństwa gospodarczego i technologicznego. Rozwój przemysłu zbrojeniowego oraz nowoczesnych technologii powodują systematyczny wzrost zapotrzebowania na strategiczne metale i minerały.

Europa stoi obecnie przed koniecznością zwiększenia własnej niezależności surowcowej. Oznacza to potrzebę rozwoju nowych projektów wydobywczych realizowanych zgodnie z wysokimi standardami środowiskowymi i społecznymi.

Jednym z kluczowych warunków sukcesu takich inwestycji staje się budowa społecznej akceptacji. Social License to Operate przestaje być jedynie dodatkowym elementem działalności przedsiębiorstw, a staje się jednym z podstawowych filarów realizacji projektów surowcowych.

Nowoczesne górnictwo nie może funkcjonować bez dialogu społecznego, transparentności oraz odpowiedzialnej komunikacji. O powodzeniu projektów wydobywczych coraz częściej decydować będzie nie tylko geologia i ekonomia, ale również poziom zaufania społecznego.

W perspektywie najbliższych lat odpowiedzialnie prowadzone projekty wydobywcze mogą stać się ważnym elementem bezpieczeństwa gospodarczego Europy. Warunkiem sukcesu będzie jednak połączenie nowoczesnych technologii, wysokich standardów środowiskowych oraz realnego partnerstwa z lokalnymi społecznościami.

Biogaz jako dyspozycyjne źródło energii oraz biometan jako krajowy zasób gazowy

Artur Zawisza

Abstrakt:

Artykuł prezentuje biogaz i biometan jako dyspozycyjne, sterowalne źródła energii o kluczowym znaczeniu dla bezpieczeństwa energetycznego Polski. Autor omawia strukturę krajowego sektora biogazowego, jego potencjał produkcyjny na tle europejskim oraz dystans do celów REPowerEU. Analizuje ścieżkę biometanową jako kierunek strategicznego rozwoju, wskazując na regulacyjne i rynkowe bariery ją hamujące, oraz formułuje tezy o konieczności wprowadzenia podziałów na źródła dyspozycyjne i niedyspozycyjne w polskim miksie energetycznym.

Słowa kluczowe: biogaz, biometan, bezpieczeństwo energetyczne, OZE, biogazownia, REPowerEU, sektor rolniczy

1. UPEBBI

Unia Producentów i Pracodawców Przemysłu Biogazowego i Biometanowego (UPEBBI) powstała w 2012 roku. Jesteśmy związkiem pracodawców działającym na podstawie ustawy o organizacjach pracodawców i mamy wszystkie profity związane z tym szczególnym statusem. Skupiamy przedsiębiorstwa przede wszystkim prowadzące, a także projektujące, budujące i serwisujące biogazownie i biometanownie oraz podmioty z otoczenia biznesu (zajmujące się np. obrotem energią, dotacjami unijnymi czy ubezpieczeniami instalacji). Skrót UPEBBI (będący skrótem angielskojęzycznej nazwy Union of Producers and Employers of Biogas and Biomethane

Industry) oznacza innymi słowy RAZEM DLA BIOGAZU. Dlatego też podejmujemy wspólne starania, aby branża biogazu i biometanu rolniczego, ściekowego i odpadowego miała coraz lepsze warunki do rozwoju. Naszym celem jest wspólna praca na rzecz przemysłu biogazowego i biometanowego w kraju oraz w Europie i na świecie (jako uczestnik European Biogas Association, World Biogas Association i Biomethane Industrial Partnership). W ramach unijnego programu Erasmus+ podejmujemy współpracę międzynarodową, np. z analogicznymi organizacjami z Czech i Łotwy w projekcie „Kształcenie kadr dla europejskiego sektora biogazu"

Nadrzędnym celem UPEBBI jest udzielanie członkom wszechstronnej pomocy i ochrony prawnej oraz kształtowanie jednolitego stanowiska we wszystkich sprawach związanych z prowadzoną przez nich działalnością gospodarczą. Jesteśmy największą organizacją branżową animującą Porozumienie dla Biogazu i Biometanu składające się z siedmiu podmiotów reprezentujących przeważającą część sektora. Pracujemy na stałe z prawnikami, ekspertami, naukowcami, urzędnikami i praktykami branży w celu optymalizacji efektów działania.

Współpracujemy z instytucjami naukowo-badawczymi (uniwersytety, akademie i państwowe instytuty badawcze) w celu wypracowania innowacyjnych rozwiązań technologicznych przyczyniających się do bardziej dynamicznego rozwoju branży w Polsce i na świecie. Razem z Uniwersytetem Przyrodniczym w Lublinie i Instytutem Biotechnologii Przemysłu Rolno–Spożywczego oraz Centrami Kształcenia Rolniczego tworzymy Branżowe Centra Umiejętności w dziedzinie bioenergetyki (na Lubelszczyźnie i na Pomorzu) przeznaczone do kształcenia uczniów, nauczycieli i dorosłych.

Prowadzimy działalność edukacyjną i promocyjną w celu podniesienia stanu wiedzy społeczeństwa na temat możliwości wytwarzania i wykorzystywania biogazu jako odnawialnego źródła energii i biometanu jako paliwa gazowego, np. prowadząc dla setek osób w skali kraju (potencjalni inwestorzy, pracownicy jednostek samorządu terytorialnego i uczniowie szkół rolniczych) warsztaty na zlecenie Krajowego Ośrodka Wsparcia Rolnictwa lub szkoląc pracowników Wojewódzkiego Funduszu Ochrony Środowiska i Gospodarki Wodnej w Białymstoku.

Wielokrotnie skutecznie interweniujemy na etapie tworzenia ustaw i rozporządzeń dotyczących branży biogazowej. Utrzymujemy robocze kontakty z Ministerstwem Klimatu i Środowiska (piony odnawialnych źródeł energii i gospodarki odpadami) oraz Ministerstwem Rolnictwa i Rozwoju Wsi (pion transformacji energetycznej obszarów wiejskich), a także Narodowym Funduszem Ochrony Środowiska i Gospodarki Wodnej czy Instytutem Ochrony Środowiska. Bierzemy regularny udział

w pracach legislacyjnych i konsultacyjnych na poziomie Sejmu i Senatu, uczestnicząc w posiedzeniach komisji i zespołów oraz rozmawiając ze szczególnie zainteresowanymi posłami i senatorami.

Uczestniczymy w konsultacjach społecznych oraz udzielamy informacji na temat biogazu i biometanu wszystkim zainteresowanym tą tematyką. Propagujemy technologię biogazową w mediach konwencjonalnych i społecznościowych oraz na wszelkich wydarzeniach, konferencjach i targach związanych z odnawialnymi źródłami energii (np. na Forum Ekonomicznym w Karpaczu, Europejskim Kongresie Gospodarczym w Katowicach, Kongresie Energetyki Rozproszonej w Krakowie, Poznańskiego Kongresu Gospodarczego w Poznaniu, Ekoforum w Supraślu i Zamościu czy podczas Centralnych Targów Rolniczych w Warsaw Ptak Expo).

Organizujemy Green Gas Poland [https:**/**greengaspoland.pl/] jako doroczną międzynarodową konferencję branży biogazu i biometanu, która przez sześć edycji przyciągnęła setki uczestników: przedstawicieli firm prywatnych i Skarbu Państwa, urzędów państwowych i agend rządowych, mediów energetycznych i biogazowych oraz naukowców, inwestorów, rolników i samorządowców.

W ramach prac Branżowych Centrum Umiejętności w dziedzinie bioenergetyka w Jabłoniu (pow. parczewski, woj. lubelskie) i Swarożynie (pow. tczewski, woj. lubelskie), w których UPEBBI jest partnerem obowiązkowym, powstały raporty autorstwa pracowników naukowych, menedżerów rynku rynkowych i ekspertów branżowych, przywoływane w cytatach w dalszej części tego artykułu dla uzasadnienia jego tytułu i tez w nim stawianych.

2. Pierwsza teza główna: biogaz jako dyspozycyjne źródło energii.

Biogazownie jako OZE stabilne, sterowalne i dyspozycyjne:

- biogaz produkowany jest w sposób ciągły (ponad osiem tysięcy godzin rocznie w porównaniu do jednego tysiąca godzin pracy fotowoltaiki czy kilku tysięcy godzin pracy instalacji wiatrowych);
- ale może być magazynowany w zbiornikach, a następnie przetwarzany na energię (prąd/ciepło) w kogeneratorach dokładnie wtedy, kiedy jest to potrzebne;

- energia elektryczna wytworzona z biogazu jest dyspozycyjna wobec sieci elektroenergetycznej: dyspozycyjne źródło energii to jednostka wytwórcza, której pracą można sterować, dostosowując produkcję do zapotrzebowania w dowolnym momencie. Zapewnia stabilność systemu elektroenergetycznego (KSE), w przeciwieństwie do niestabilnych źródeł OZE (wiatr, słońce) – wedle definicji z opracowania „Jak funkcjonuje krajowy system elektroenergetyczny?" dostępnego na www Polskie Sieci Elektroenergetyczne SA.

Wobec powyższego konkluzja co do miksu energetycznego:

- odejdźmy od błędnego podziału źródeł energii na: konwencjonalne i OZE;
- stosujmy właściwy podział źródeł energii na: dyspozycyjne i niedyspozycyjne (energia ze słońca i z wiatru);
- OZE niestabilne i niesterowalne nie mogą stanowić fundamentu systemu energetycznego bez wsparcia źródeł dyspozycyjnych;
- podstawą miksu energetycznego muszą być źródła dyspozycyjne:m wysokoemisyjna energia z węgla, średnioemisyjna energia z gazu, niskoemisyjna energia atomowa/jądrowa i bezemisyjne OZE takie, jak: biogaz, geotermia i hydroenergetyka.

3. Druga teza główna: biometan jako krajowy zasób gazowy

(na podstawie raportu „Analiza porównawcza skutków makroekonomicznych import gazu ziemnego a krajowa produkcja biometanu" autorstwa dr inż. Bartosza Moszowskiego)

Koszt importu gazu to około 1,52 mld złotych za rok, natomiast wartość produkcji biometanu przy cenie referencyjnej wynosi około 5,53 mld złotych na rok. Różnica cenowa wynosi około 4,02 mld złotych za rok.

O ile koszt importowanego gazu stanowi w całości odpływ kapitału za granicę, o tyle w przypadku biometanu odpływ środków ogranicza się jedynie do importowanych elementów łańcucha wartości, takich jak komponenty inwestycyjne czy wybrane materiały eksploatacyjne.

Z punktu widzenia Polski istotna jest skala importu gazu. Według danych branżowych, w 2024 r. import gazu do Polski wyniósł około 16,80 mld m sześc. (netto-import około 15,20 mld m sześc.). Wolumen 1 mld m sześc./rok analizowany w niniejszej analizie odpowiada więc kilku procentom rocznego importu i jest miarodajny dla oceny wpływu na bilans handlowy oraz bezpieczeństwo dostaw.

Import paliwa jest w dużej części kosztem netto z punktu widzenia gospodarki krajowej (płatność za granicę). Natomiast wydatki na paliwo wytwarzane krajowo są w istotnej części wydatkiem krajowym, który zasila łańcuch wartości (rolnictwo, usługi, przemysł, budownictwo, serwis) i może poprawiać bilans handlowy poprzez zastępowanie importu.

Wniosek dotyczący korzystnego wpływu biometanu na saldo zewnętrzne gospodarki pozostaje stabilny przy typowych zakresach zmian cen gazu obserwowanych na rynku europejskim oraz przy umiarkowanych zmianach pozostałych parametrów modelu.

Warunkiem uzyskania korzyści gospodarczych i środowiskowych związanych z rozwojem biometanu pozostaje zrównoważony dobór substratów wykorzystywanych w produkcji. Największą akceptację społeczną i środowiskową mają projekty oparte na odpadach oraz pozostałościach pochodzenia rolniczego i rolno-spożywczego, przy jednoczesnym zachowaniu kryteriów zrównoważonego rozwoju.

Biometan to nie tylko źródło energii. To inwestycja w odporność gospodarki, bezpieczeństwo państwa i kapitał, który pozostaje w kraju. W czasach rosnącej niestabilności geopolitycznej oraz nieprzewidywalności rynku surowców własna, rozproszona produkcja energii staje się jednym z fundamentów bezpieczeństwa ekonomicznego państwa. Każda złotówka wydana na krajowy łańcuch wartości pracuje dla polskich przedsiębiorstw, samorządów i miejsc pracy zamiast zwiększać zależność od zagranicznych dostawców.

Rozwój rynku biometanu może stać się istotnym impulsem inwestycyjnym dla Polski. Aby osiągnąć produkcję na poziomie jednego mld m sześc. rocznie, potrzebnych byłoby około 600 instalacji biometanowych rozmieszczonych w różnych regionach kraju.

Szacowany poziom inwestycji wynosi od około 4,5 do ponad 10 mld zł. Rozwój sektora biometanu mógłby wygenerować od 7 do nawet ponad 10 tys. miejsc pracy – przede wszystkim na terenach wiejskich i w mniejszych miejscowościach. Chodzi nie tylko o obsługę samych instalacji, ale także transport, logistykę, serwis, rolnictwo i lokalne usługi.

Pełne wykorzystanie potencjału biometanu wymaga odpowiednio zaprojektowanych mechanizmów wsparcia oraz utrzymania możliwie wysokiego udziału krajowych komponentów i usług w całym łańcuchu dostaw.

4. Dane analityczne dotyczące biogazu rolniczego i komunalnego

(na podstawie raportów „Stan obecny i niezbędne zmiany regulacyjne w zakresie biogazu trwale i funkcjonalnie związanego z gospodarstwem rolnym lub zakładem produkującym odpady" autorstwa prof. Krzysztofa Pilarskiego oraz „Stan obecny i niezbędne zmiany regulacyjne w zakresie wsparcia wytwórców biogazu innego niż biogaz rolniczy" autorstwa dr Anny Pudełko)

Biogaz wytwarzany w instalacjach trwale i funkcjonalnie związanych z gospodarstwem lub zakładem stanowi szczególną kategorię technologii energetycznej, której znaczenie wykracza poza klasycznie rozumianą produkcję energii. W odróżnieniu od instalacji funkcjonujących przede wszystkim jako autonomiczne przedsięwzięcia rynkowe, jednostki tego rodzaju pozostają osadzone w konkretnym układzie gospodarczym, w którym powstawanie substratów, ich przetwarzanie, wykorzystanie energii oraz zagospodarowanie produktów procesu tworzą logiczną i funkcjonalną całość. Ta szczególna cecha biogazu zintegrowanego z działalnością rolniczą lub produkcyjną uzasadnia potrzebę odrębnego i pogłębionego spojrzenia na jego status regulacyjny. Są one zarazem źródłem energii odnawialnej, elementem lokalnej gospodarki materiałowej, instrumentem zagospodarowania substratów organicznych oraz – w wielu przypadkach – ogniwem gospodarki nawozowej i środowiskowej.

Szczególną kategorię stanowią te instalacje biogazowe, które nie funkcjonują jako byty oderwane od podstawowej działalności rolniczej lub produkcyjnej, lecz pozostają z nią w trwałym związku technologicznym, materiałowym, przestrzennym i gospodarczym. W takim ujęciu przez instalacje zintegrowane z gospodarstwem rolnym lub chowem i hodowlą zwierząt należy rozumieć przede wszystkim jednostki wykorzystujące substraty powstające w sposób ciągły, przewidywalny i naturalnie związany z podstawową działalnością gospodarstwa rolnego albo zakładu wytwarzającego odpady organiczne. Chodzi zatem o te przypadki, w których biogazownia stanowi element szerszego układu gospodarczego, służącego nie tylko do produkcji

energii, lecz również zagospodarowaniu produktów ubocznych, pozostałości poprodukcyjnych, odchodów zwierzęcych, resztek organicznych bądź innych frakcji biodegradowalnych, które bezpośrednio wynikają z charakteru działalności podstawowej.

Biogaz zintegrowany z gospodarstwem lub zakładem stanowi rozwiązanie o szczególnym znaczeniu technologicznym, środowiskowym, gospodarczym i energetycznym, ponieważ jego istota nie sprowadza się wyłącznie do wytwarzania energii, lecz polega na włączeniu procesu fermentacji metanowej w szerszy system racjonalnego gospodarowania materią organiczną. W odróżnieniu od instalacji funkcjonujących głównie jako niezależne przedsięwzięcia energetyczne, jednostki tego rodzaju są osadzone w rzeczywistym układzie produkcyjnym, w którym powstawanie substratów, ich przetwarzanie, wykorzystanie energii oraz zagospodarowanie produktów procesu pozostają wzajemnie powiązane. W warunkach gospodarstwa rolnego fermentacja metanowa może pełnić funkcję narzędzia pozwalającego na bardziej racjonalne wykorzystanie biomasy, nawozów naturalnych, pozostałości pożniwnych, resztek paszowych oraz innych materiałów organicznych, które w przeciwnym razie pozostawałyby źródłem emisji, kosztów logistycznych lub problemów związanych z magazynowaniem i zagospodarowaniem. Analogicznie, w zakładach przetwórczych lub innych jednostkach wytwarzających odpady organiczne biogazownia może stanowić element technologicznego domknięcia procesu produkcyjnego, umożliwiający odzysk energii z frakcji organicznych, które powstają w sposób ciągły i przewidywalny jako konsekwencja podstawowej działalności. Gospodarczo szczególne znaczenie analizowanego modelu polega na tym, że pozwala on na zwiększenie efektywności wykorzystania zasobów już obecnych w gospodarstwie lub zakładzie. Może to oznaczać ograniczenie kosztów związanych z postępowaniem z odpadami organicznymi, poprawę bilansu energetycznego gospodarstwa lub zakładu, a także zwiększenie odporności ekonomicznej na zmienność cen energii i paliw.

Równie ważny jest wymiar środowiskowy. Biogazownie zintegrowane z miejscem powstawania substratów mogą odgrywać istotną rolę w ograniczaniu niekontrolowanych emisji gazów i odorów związanych z przechowywaniem oraz naturalnym rozkładem materii organicznej. W efekcie uzyskuje się nie tylko energię, ale także ograniczenie obciążeń środowiskowych, które w przeciwnym razie byłyby rozproszone i trudniejsze do zarządzania. Środowiskowe znaczenie tego modelu wiąże się także z bardziej uporządkowanym obiegiem składników pokarmowych. W układzie zintegrowanym z gospodarstwem rolnym poferment może stanowić element racjonalnej gospodarki nawozowej, umożliwiając częściowy powrót składników pokarmowych

na grunty związane z miejscem ich pierwotnego wytworzenia. Ta właśnie właściwość odróżnia instalacje rzeczywiście zintegrowane od przedsięwzięć, które koncentrują się wyłącznie na energetycznym wykorzystaniu biomasy bez szerszego powiązania z gospodarką substancją organiczną i nawozową.

W praktyce administracyjnej warto wyraźnie odróżniać oddziaływania nowe od oddziaływań już istniejących w gospodarstwie lub zakładzie. Jeżeli biogazownia przejmuje gnojowicę, pomiot, odpady organiczne albo pozostałości poprodukcyjne, które i tak musiałyby być magazynowane lub zagospodarowane, ocena środowiskowa nie powinna ograniczać się do prostego wskazania dodatkowej instalacji. Należy oceniać nie tylko powstanie nowego obiektu technologicznego, lecz przede wszystkim zmianę bilansu środowiskowego całego gospodarstwa albo zakładu po jego uruchomieniu. Biogazownia lokalnie zintegrowana może ograniczać emisje rozproszone związane z dotychczasowym magazynowaniem materii organicznej, zmniejszać ryzyko odorowe, porządkować gospodarkę substratami oraz stabilizować zagospodarowanie pozostałości poprodukcyjnych. W wielu przypadkach taka instalacja nie zwiększa presji środowiskowej, lecz poprawia bilans całego układu poprzez kontrolowaną fermentację, odzysk energii, ograniczenie niekontrolowanego rozkładu substratów oraz włączenie pofermentu w racjonalną gospodarkę nawozową lub materiałową. Dlatego w ocenie środowiskowej nie powinno się traktować jej wyłącznie jako dodatkowego źródła potencjalnych emisji, ale jako element technologiczny, który może zmniejszać sumaryczne obciążenie środowiska wynikające z działalności podstawowej.

To zasadnicza różnica pomiędzy obiektem lokalnie zintegrowanym a instalacją dowożącą wsad z szerokiego rynku. W tym przypadku biogazownia pełni funkcję porządkującą wobec istniejących strumieni materii organicznej.

Sektor biogazu w Polsce stanowi istotny element transformacji energetycznej, wpisując się zarówno w krajowe cele zwiększenia udziału odnawialnych źródeł energii, jak i w unijną politykę klimatyczno-energetyczną oraz gospodarkę obiegu zamkniętego. Biogaz – jako stabilne, sterowalne źródło energii – odgrywa szczególną rolę w bilansowaniu systemu energetycznego oraz ograniczaniu zależności od paliw kopalnych.

Pomimo znaczącego potencjału rozwojowego, sektor ten – zwłaszcza w obszarze biogazu innego niż rolniczy – napotyka szereg barier regulacyjnych i systemowych. W szczególności wskazuje się na brak kompleksowego i spójnego systemu wsparcia, niejednoznaczność przepisów oraz ich zmienność, co ogranicza skłonność inwestorów do podejmowania nowych przedsięwzięć.

Dotychczasowe rozwiązania legislacyjne w Polsce koncentrowały się głównie na biogazie rolniczym, pozostawiając pozostałe segmenty rynku – w tym instalacje wykorzystujące odpady komunalne, przemysłowe czy osady ściekowe – w relatywnie mniej uprzywilejowanej pozycji regulacyjnej. Jednocześnie obserwowane w ostatnim czasie zmiany legislacyjne, w tym nowelizacje prawa energetycznego oraz planowane mechanizmy wsparcia (np. systemy aukcyjne dla biometanu), wskazują na rosnącą świadomość potrzeby uporządkowania i rozszerzenia ram prawnych dla całego sektora biogazu.

Biogaz stanowi odnawialne paliwo gazowe powstające w procesie beztlenowej fermentacji substancji organicznych, takich jak odpady rolnicze, komunalne, przemysłowe czy osady ściekowe. Jego głównym składnikiem jest metan (CH_4), który decyduje o wartości energetycznej paliwa. W kontekście transformacji energetycznej biogaz traktowany jest jako stabilne i sterowalne źródło energii odnawialnej, umożliwiające zarówno produkcję energii elektrycznej i ciepła w kogeneracji, jak i – po odpowiednim oczyszczeniu – wprowadzanie do sieci gazowej w postaci biometanu.

Na gruncie prawa polskiego brak jest jednej, uniwersalnej definicji „biogazu" obejmującej wszystkie jego rodzaje. Ustawodawca posługuje się natomiast definicjami sektorowymi, w szczególności w ustawie z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (dalej: „ustawa OZE"). Zgodnie z art. 2 pkt 2 tej ustawy, przez biogaz rozumie się gaz uzyskiwany z biomasy, w szczególności z instalacji fermentacji metanowej.

Jednocześnie ustawa OZE wprowadza szczególne kategorie biogazu, w tym m.in. biogaz rolniczy, który został zdefiniowany w art. 2 pkt 2a jako gaz otrzymywany z surowców pochodzenia rolniczego (np. odchodów zwierzęcych, produktów ubocznych rolnictwa czy biomasy roślinnej). Definicja ta ma charakter zawężający i stanowi podstawę do wyodrębnienia tej kategorii w systemie wsparcia.

W konsekwencji, w praktyce regulacyjnej oraz rynkowej funkcjonuje pojęcie biogazu innego niż rolniczy, które obejmuje wszelkie rodzaje biogazu niespełniające kryteriów biogazu rolniczego. Do tej kategorii zalicza się w szczególności:

- biogaz ze składowisk odpadów,
- biogaz z oczyszczalni ścieków,
- biogaz powstający z odpadów komunalnych i przemysłowych,
- biogaz z instalacji przetwarzania bioodpadów.

Choć pojęcie to nie jest wprost zdefiniowane w przepisach ustawowych, jego zakres wynika pośrednio z konstrukcji systemu prawnego – poprzez wyłączenie biogazu

rolniczego jako odrębnej kategorii regulacyjnej. W konsekwencji, „biogaz inny niż rolniczy" ma charakter definicji negatywnej (resztowej), co w praktyce prowadzi do niejednoznaczności interpretacyjnych.

Z kolei w Rozporządzeniu Ministra Klimatu i Środowiska z dnia 8 listopada 2023 r. w sprawie ceny referencyjnej energii elektrycznej z odnawialnych źródeł energii, okresów obowiązujących wytwórców, którzy wygrali aukcje, oraz referencyjnych wolumenów sprzedaży energii elektrycznej (Dz.U. 2023 poz. 2440) wydzielono oddzielne ceny referencyjne dla następujących rodzajów biogazów ze względu na jego pochodzenie:

1. Biogaz rolniczy
2. Biogaz ze składowisk odpadów
3. Biogaz pozyskany z oczyszczalni ścieków
4. Biogaz inny niż wcześniej wymienione

Istotne znaczenie dla funkcjonowania sektora biogazu mają również przepisy innych aktów prawnych, w tym:

- ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, regulującej zasady wytwarzania i obrotu paliwami gazowymi,
- ustawy z dnia 14 grudnia 2012 r. o odpadach, określającej status substratów wykorzystywanych w procesie fermentacji,
- przepisów dotyczących gospodarki komunalnej i wodno-ściekowej, które mają zastosowanie do instalacji wykorzystujących odpady i osady ściekowe.

Na poziomie unijnym podstawowe znaczenie ma dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2001 (RED II), zmieniona dyrektywą RED III, która klasyfikuje biogaz jako odnawialne paliwo oraz określa ramy jego wsparcia, w tym w kontekście produkcji biometanu i dekarbonizacji sektora gazowego.

Szczególnego znaczenia nabiera biogaz wytwarzany z odpadów komunalnych, który – poza funkcją energetyczną – pełni istotną rolę w systemie gospodarki odpadami. Przetwarzanie bioodpadów w instalacjach fermentacji beztlenowej przyczynia się bezpośrednio do zwiększenia poziomów recyklingu i odzysku, wymaganych na gruncie prawa krajowego oraz unijnego (w szczególności dyrektywy 2008/98/WE w sprawie odpadów oraz przepisów krajowych implementujących te regulacje).

Zgodnie z dostępnymi danymi statystycznymi, w Polsce rocznie zbieranych jest około 1,9 mln ton bioodpadów komunalnych. Należy jednak podkreślić, że rzeczywista ilość wytwarzanych bioodpadów jest wyższa, ponieważ część z nich nadal trafia do strumienia odpadów zmieszanych i nie jest ujmowana w statystykach selektywnej zbiórki.

Potencjał energetyczny bioodpadów zależy od ich składu, wilgotności oraz zawartości substancji organicznych. W przypadku odpadów kuchennych, które cechują się wysoką zawartością łatwo biodegradowalnej materii organicznej, wydajność produkcji biogazu może wynosić średnio od 100 do 200 m³ biogazu z jednej tony wsadu. Z kolei odpady tzw. „zielone", takie jak trawa, liście czy odpady z pielęgnacji terenów zielonych, charakteryzują się niższą wydajnością – zwykle w przedziale od 60 do 120 m³ biogazu na tonę, co wynika z wyższej zawartości ligniny i trudniej rozkładalnych struktur roślinnych.

Przyjmując konserwatywne założenia, można oszacować, że całkowity potencjał produkcji biogazu z bioodpadów komunalnych w Polsce wynosi od około 150 do 300 mln m³ rocznie. Po przeliczeniu na energię elektryczną oznacza to możliwość wytworzenia nawet kilkuset GWh energii rocznie, przy jednoczesnym uzyskaniu znacznych ilości ciepła oraz produktu pofermentacyjnego.

Rozwój instalacji produkujących biogaz z odpadów komunalnych pozwala jednostkom samorządu terytorialnego oraz podmiotom odpowiedzialnym za gospodarowanie odpadami na ograniczenie ryzyka nieosiągnięcia wymaganych poziomów recyklingu. W konsekwencji przekłada się to na zmniejszenie potencjalnych obciążeń finansowych, w tym opłat i kar administracyjnych związanych z niewypełnieniem obowiązków ustawowych. Biogazownie pełnią zatem podwójną funkcję – jako element infrastruktury energetycznej oraz jako narzędzie wspierające realizację celów środowiskowych i optymalizację kosztów systemu gospodarki odpadami.

5. Dane analityczne dotyczące biometanu

(na podstawie raportu „Biometan w Polsce: nowe technologie, wykonawcy i realia wdrożeń" autorstwa mgra Łukasza Rosika)

Polska biogazownia rolnicza przez większość swojego życia zarabia na sprzedaży energii elektrycznej w systemie aukcyjnym FiT lub FiP. To model sprawdzony, stabilny i dobrze rozpoznany przez rynek. Biometan przez długi czas pozostawał w tle jako opcja teoretycznie atrakcyjna, a w praktyce zarezerwowana dla większych instalacji i krajów z lepiej rozwiniętą infrastrukturą gazową.

W ciągu ostatnich kilku lat sytuacja zmieniła się na tyle wyraźnie, że ignorowanie ścieżki biometanowej przestało być ostrożnością, a stało się ryzykiem. Strategia REPowerEU wyznaczyła dla Europy ambitne cele produkcji biometanu, a za nią ruszyły pierwsze krajowe projekty i mechanizmy finansowania. Pytanie nie brzmi już „czy biometan w Polsce się rozwinie", ale „kiedy i w jakiej formie"?

Na koniec marca 2025 roku w Polsce działało 415 biogazowni wszystkich typów. Spośród nich 181 stanowiły instalacje rolnicze zarejestrowane przez Krajowy Ośrodek Wsparcia Rolnictwa (KOWR), należące do 151 podmiotów, o łącznej zainstalowanej mocy elektrycznej 173 MW i potencjale produkcyjnym przekraczającym 755 mln m³ biogazu rocznie. Do tego dochodzi 195 instalacji komunalnych przy oczyszczalniach ścieków i składowiskach odpadów oraz 65 mikrobiogazowni rolniczych.

Liczby te nabierają właściwego wymiaru w zestawieniu z danymi europejskimi. W Europie funkcjonuje ponad 20 tysięcy biogazowni, z czego ponad 10 tysięcy w Niemczech. Dania, kraj o intensywnej produkcji zwierzęcej zbliżonej strukturą do polskiego rolnictwa, zbudowała swój sektor biogazowy przez 50 lat konsekwentnej polityki wsparcia – od pierwszych instalacji w połowie lat 70. aż po obecny stan, w którym biometan stanowi około 40% gazu w krajowej sieci dystrybucyjnej. Polska dysponując piątym co do wielkości potencjałem biomasy w UE, wykorzystuje zaledwie ułamek tych zasobów. W 2024 roku krajowe biogazownie wyprodukowały niespełna 1,6 TWh energii elektrycznej, poniżej 1% łącznej krajowej produkcji.

Szczególnie wymowna jest sytuacja po stronie biometanu. Urząd Regulacji Energetyki prowadzi od 2024 roku odrębny rejestr wytwórców biogazu i biometanu, gdzie przez cały 2024 rok nie dokonano w nim ani jednego wpisu. Dwie instalacje uruchomione w 2025 roku tylko nieznacznie zmieniły ten obraz.

Pierwsza to demonstrator technologiczny w Brodach koło Poznania, na terenie Rolniczego Gospodarstwa Doświadczalnego Uniwersytetu Przyrodniczego w Poznaniu, uruchomiony w lutym 2025 roku przy wsparciu Narodowego Centrum Badań i Rozwoju. Instalacja o mocy 0,499 MWe produkuje około 650 tys. m³ biometanu rocznie w postaci sprężonego bioCNG, przeznaczonego na rynek paliw transportowych.

Drugą i pod względem skali znacznie ważniejszą jest biometanownia w Cukrowni Strzelin (woj. dolnośląskie), należącej do Südzucker Polska. We wrześniu 2025 roku Polska Spółka Gazownictwa (PSG) przyłączyła tę instalację do krajowej sieci dystrybucyjnej jako pierwszą w Polsce. Biogazownia w Strzelinie działa od 2012 roku, a rozbudowana infrastruktura osiąga moc 45 MW, produkując ponad 9 tys. m³ biogazu na godzinę wyłącznie z wysłodków buraczanych powstających podczas produkcji

cukru. Biogaz wykorzystywany jest przede wszystkim na potrzeby własne cukrowni, a jego nadwyżki (po uszlachetnieniu do biometanu) trafiają do sieci przez wybudowany wspólnie z PSG gazociąg przyłączeniowy o długości 9 km. PSG zadeklarowała, że planuje przyłączyć łącznie kilka biometanowni w 2025 roku, a w 2026 roku kilkanaście kolejnych.

W maju 2022 roku Komisja Europejska opublikowała plan REPowerEU, wyznaczając cel produkcji 35 mld m³ biometanu rocznie w UE do 2030 roku. Cel ten ma charakter niewiążący dla państw członkowskich, ponieważ jego realizacja zależy od woli politycznej i instrumentów wsparcia na poziomie krajowym.

Produkcja biometanu w UE rośnie, ale dystans do celu 2030 jest nadal bardzo duży. Produkcja osiągnęła 4,9 mld m³ w 2023 roku, a zainstalowane moce ok. 7 mld m³ w 2025 roku. Inwestycje zakontraktowane do 2025 roku pozwolą osiągnąć szacunkowo 7,3 mld m³ mocy zainstalowanych do 2030 roku tj. około 20% zakładanego celu. Więcej niż statystyki mówią doświadczenia krajów, które ten rynek już zbudowały. Dania przez dekady budowała sektor biogazowy w oparciu o stabilne systemy wsparcia, standaryzację rozwiązań technicznych i ścisłą integrację z siecią gazową. Duński model oparty na współpracy publiczno-prywatnej, spółdzielniach rolniczych i centralnych biogazowniach przetwarzających substraty z wielu gospodarstw jednocześnie może być punktem odniesienia dla krajów wchodzących dopiero w ten rynek, w tym dla Polski.

Szacunki potencjału produkcji biometanu w Polsce różnią się w zależności od metodologii, ale wskazują na ten sam rząd wielkości. Krajowy Plan na rzecz Energii i Klimatu (KPEiK) określa potencjał techniczny na poziomie 8 mld m³ rocznie, co odpowiadałoby 46% krajowego zapotrzebowania na gaz ziemny. Organizacja Gas for Climate szacuje perspektywiczny potencjał do 2050 roku na 13 mld m³. Uwzględniając realne ograniczenia takie jak dostępność substratów w poszczególnych regionach i przepustowość sieci gazowej Dolnośląski Instytut Studiów Energetycznych (DISE) ocenia osiągalny potencjał na 3–4 mld m³ rocznie.

KPEiK wyznacza dla Polski produkcję biometanu na poziomie 1,1–1,5 mld m³ do 2030 roku i 2,6–3,9 mld m³ do 2040 roku. Osiągnięcie nawet dolnej granicy celu 2030 wymagałoby zbudowania od podstaw całego sektora biometanowego od instalacji produkcyjnych, przez infrastrukturę przyłączeniową, po łańcuch dostaw substratów i kadrę techniczną.

ROZDZIAŁ III.
TECHNOLOGIE

Przyszłość krajowej domeny internetowej wobec wyzwań suwerenności technologicznej

prof. Katarzyna Chałubińska-Jentkiewicz

Abstrakt:

Artykuł analizuje znaczenie krajowej domeny internetowej .pl jako elementu suwerenności technologicznej. Autorka omawia historię systemu domenowego internetu, identyfikuje zagrożenia dla środowiska domenowego oraz analizuje kwestię braku przepisów powszechnie obowiązujących w zakresie domen. Wskazuje na potrzebę systemowej regulacji krajowej przestrzeni domenowej jako elementu budowania cyfrowej suwerenności.

Słowa kluczowe: domena internetowa, suwerenność technologiczna, .pl, DNS, cyberbezpieczeństwo, regulacja cyfrowa

Środowisko nowych technologii i rozwój domen

Technologie informacyjne i komunikacyjne stwarzają nowe możliwości powszechnej konsumpcji. Dotyczy to także konsumpcji informacji. Dzisiaj paradygmat konsumenta zostaje zastąpiony paradygmatem użytkownika sieci – klienta, osoby której dane cyfrowe, treści cyfrowe, także generowane w ramach Internet behaviour, są powszechnie monetyzowane i wykorzystywane do działań marketingowych w ramach profilowani i targetowania. Coraz częściej działania te obejmują szeroko rozumiane aktywności związane z prowadzeniem polityki informacyjnej różnych grup społecznych a także władzy publicznej. Jednocześnie kluczowe znaczenie ma tzw. suwerenność technologiczna. Komisja Europejska definiuje suwerenność technologiczną

jako zdolność Europy do samodzielnego działania w świecie cyfrowym poprzez rozwijanie i kontrolowanie kluczowych technologii, danych i infrastruktury oraz ograniczanie zależności od dostawców spoza UE.

Idea komutacji pakietów i implementacja rozproszonych sieci cyfrowych pozwoliła na błyskawiczne przesyłanie danych między wieloma użytkownikami sieci jednocześnie. Dzięki współpracy z Rand Corporation organizacją badawczą działającą przy amerykańskich powietrznych siłach zbrojnych, naukowiec polskiego pochodzenia Paul Baran rozwinął swój projekt, opisując go w 11-tomowej monografii pt. On Distributed Communications, opublikowanej w 1964 r. Przy współpracy z ośrodkami akademickimi: Uniwersytetem Stanforda, Uniwersytetem w Utah i Uniwersytetem Kalifornijskim. ARPA stworzyła bazowy protokół TCP (ang. Transmission Control Protocol), którego efektem była sieć łącząca wymienione uczelnie wyższe, pozwalająca bezpiecznie przesyłać dane między nimi. Paul Baran był autorem artykułu naukowego opublikowanego w Rand Paper (P-3717) pt. Some changes in information technology affecting marketing in the year 2000 (lipiec 1968 r.), w którym opisał wizję przyszłości – roku 2000, wskazując rozwój e-commerce, opartego w znacznej mierze na komunikacji drogą elektroniczną oraz idei sklepów wirtualnych.

W 1990 r. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (ang. Defense Advanced Research Projects Agency – DARPA), przekształcona w 1972 r. z ARPA, oficjalnie zakończyła prace nad rozwojem sieci cywilnej. Połowa lat 90. XX wieku przyniosła nowe narzędzia internetowe: wyszukiwarki stron, komunikatory, urządzenia mobilne. Pierwszym portalem na krajowym rynku usług była Wirtualna Polska, udostępniona w 1995 r. W 1998 r. powstała amerykańska firma Google, zaś w 2004 r. – serwis społecznościowy Facebook. Polska została przyłączona do internetu w 1991 r. Dnia 20 kwietnia 1992 r. zarejestrowano pierwszą krajową domenę najwyższego stopnia z końcówką .pl. W pierwszych latach XXI wieku ich liczba sięgała 200 tys. aby w 2026 r. osiągnąć poziom 2,6 mln. Powyższy poziom plasuje Polskę na pozycji w rankingu europejskich rejestrów domeny ccTLD na 6 miejscu. Nie jest to rynek odporny na zmiany i pozbawiony zagrożeń.

Zmiany i zagrożenia

Podstawową konsekwencją zmian technologicznych stało się pojawienie nowej przestrzeni funkcjonowania jednostki, grup społecznych czy nawet państwa. Jest nią

cyberprzestrzeń. Dzisiaj jej analiza i próba zdefiniowania to praktycznie konieczność ustalenia zakresu przestrzennego oddziaływania norm prawnych odnoszących się do nowych technologii. Przestrzeń ta związana jest z systemem domen internetowych, jak również z innymi środowiskami funkcjonowania nas w sieci, nie pomijając mediów społecznościowych. Problematyka nowych regulacji obejmuje kwestie odnoszące się do konkretnych treści, jakie są rozpowszechniane za pośrednictwem sieci. Z nowymi mediami związane są działania korporacji – przedsiębiorców, których głównym celem jest zysk, wygenerowany m.in. poprzez handel w sieciach, oraz towarzyszące mu działania reklamowe. Dlatego analiza tych technik pozwoli na dokładne ustalenie przyszłych problemów związanych z funkcjonowaniem cyberprzestrzeni i środowiska sieciowego. Identyfikacja zagrożeń związanych z usługami sieciowymi oraz przegląd aktualnych zagadnień związanych z ochroną własności w sieci pozwolą postawić diagnozę co do konieczności redefinicji celów przyszłej regulacji w obszarze uprawnień właścicielskich związanych monopolem uprawnionych do dóbr niematerialnych, takich jak prawo autorskie i prawa pokrewne, tajemnica przedsiębiorcy, know-how, przedmioty ochrony własności przemysłowej oraz bazy danych. Zgodnie z ideą P. Weibela obok cyfrowego myślenia, którego oddziaływanie i sukcesy objęły już cały świat (bez „maszyn liczących" nie funkcjonowałyby bowiem żadne lotniska, fabryki, dworce, centra zakupowe, szpitale i inne) pojawia się również cyfrowa sztuka, której celem jest objęcie całego świata.

Jednak podstawowym elementem tego rozwoju staje się bezpieczeństwo. Dlatego kolejnym ważnym obszarem regulacji jest potrzeba zapewnienia cyberbezpieczeństwa, która wynika z kreacji wyzwalanej przez innowacje i nowe technologie. Jedną z nowych sfer regulacji stało się środowisko domen internetowych (obowiązki rejestrów ccTLD, dostawców usług DNS oraz rejestratorów określają dyrektywa NIS 2 i wdrażająca ją ustawa o krajowym systemie cyberbezpieczeństwa). W sensie faktycznym niezwykle ważnym elementem suwerenności działania na rynku e-commerce jest krajowa domena internetowa a kluczową jej cechą jest wymiar jej bezpieczeństwa.

Domena internetowa PL – dlaczego jest ważna?

Eksterytorialny charakter sieci pozwala na nieograniczoną wymianę informacji i działania komercyjne w skali globalnej. Aktywność w sieci obejmuje działalność

gospodarczą, naukową, społeczną przy użyciu narzędzi elektronicznych na odległość, ale dzieje się to przy znikomych ograniczeniach natury prawnej (np. poprzez regulaminy BIG TECH), z wykorzystaniem wolności rynkowej. Jednak system domen internetowych wydaje się coraz bardziej atrakcyjny. Dobór domeny internetowej jest równoznaczny z łatwym ustaleniem z jakim rodzajem aktywności mamy do czynienia. Zmiany związane z systemem weryfikacji danych pozwalają zwalczać sytuacje rejestracji domeny przez podmioty nieuprawnione. Dzisiaj aktywność w internecie podlega uprzedniej rejestracji domeny internetowej, która umożliwia uprawnionemu prowadzenie strony internetowej w warunkach rynkowych, z jednoczesnym zastrzeżeniem tych działań w oparciu o porządek i bezpieczeństwo publiczne. Domena internetowa w czasach hydrantu informacji i chaosie BIG DATA daje pewność identyfikacji własnego środowiska cyfrowego. Nadaje walor unikatowej tożsamości cyfrowej. Przyjęte reguły doboru nazwy domeny stworzyły możliwości nadawania najróżniejszych nazw domenom w warunkach „kto pierwszy, ten lepszy", co nadaje konkretnemu środowisku cyfrowemu spersonalizowany profil i trwałość działań e-commerce.

Miejsce regulacji

Dotychczas brak jest przepisów powszechnie obowiązujących w zakresie domen internetowych, podobnie jak w polskim systemie prawnym brak jest regulacji normatywnych właściwych dla materii domen internetowych, stąd w dużym stopniu wprowadzając niezbędne zmiany każdorazowo należy badać treść umów zawieranych z partnerami oraz ocenić dany stan prawny przez pryzmat potrzeb rynkowych. Coraz częściej obszar ten poddany jest regulacji na poziomie ustaw. Można tu przywołać rozwiązanie amerykańskie – Antycybersquatting Consumer Protection Act (ACPA) – ustawa uchwalona dnia 26 października 1999 r. (S 1255 EAH) oraz ustawę fińską z dnia 17 stycznia 2003 r. o domenie (Domain Name Act) – Law No. 228/2003 oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/517 z dnia 19 marca 2019 r. w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu, zmiany i uchylenia rozporządzenia (WE) nr 733/2002 oraz uchylenia rozporządzenia Komisji (WE) nr 874/2004. Bezpieczeństwo i porządek publiczny, potrzeba wprowadzenia ładu regulacyjnego także w tym środowisku, wymuszają nowe podejście do środowiska domen internetowych oraz idące za nim zmiany regulacyjne.

Nowe środowisko, stare zagrożenia

Ze względu na charakter pojęcia domeny internetowej, zarówno jako identyfikatora o charakterze technicznym, jak i jako oznaczenia odróżniającego (w szczególności mogącego pełnić funkcję znaku towarowego), możliwe stają się naruszenia spełniające przesłanki czynów nieuczciwej konkurencji, działania wkraczające w uprawnienia właścicielskie, zwłaszcza w kontekście własności przemysłowej ale także oszustwa komputerowe oparte na aktywności przed wszystkim w ramach tzw. phishingu. Powszechnie występujące zjawisko rejestrowania w nazwach domen internetowych znaków towarowych bądź oznaczeń przedsiębiorstw prowadzi do mnożących się sporów między dysponentami nazw domen a uprawnionymi do oznaczeń im odpowiadających. Domena internetowa wykorzystywana w adresie www pełni dwojaką funkcję: identyfikuje (lokalizuje) strony www, stając się elektroniczną formą informacji, lokalizującą aktywny „pod nią" podmiot, co stanowi zbliżenie do funkcji, jaką pełni adres e-mail, oraz odróżnia (indywidualizuje) podmiot prowadzący działalność w sieci, co stanowi o użyciu w funkcji oznaczenia. W celu rejestracji subdomeny konieczna jest uprzednia rejestracja domeny z końcówką wyższego poziomu. Stąd domena internetowa może być używana w charakterze znaku towarowego (bądź może być w ten sposób postrzegana przez użytkowników sieci), pełniąc rolę oznaczenia identyfikującego pochodzenie towaru lub usługi oferowanej poprzez strony www. Jednocześnie domena może być używana w charakterze oznaczenia przedsiębiorstwa, mając za cel jego identyfikację, pozwalającą na odróżnienie go od innych podmiotów działających na rynku, prowadzących działalność w sieci. W tym zakresie aktywności, możemy spotkać się z niepożądanymi zachowanymi osłabiania cudzego znaku towarowego jak rozmywanie, przyćmienie czy pasożytowanie. Trybunał Sprawiedliwości UE zdefiniował osłabienie znaku towarowego poprzez rozmywanie jako sytuację, gdy zdolność znaku do identyfikowania towarów lub usług, dla których został zarejestrowany i jest używany, jako pochodzących od uprawnionego z tego znaku, jest osłabiona. Pomocne tu stają się mediacje i działania arbitrażowe.

Analizując aktualny krajowy, polski system polubownych sposobów rozwiązywania sporów o domeny internetowe, należy odwołać się do systemu dwóch instytucji właściwych w zakresie sporów o domeny, tj. Sądu Arbitrażowego przy Krajowej Izbie Gospodarczej w Warszawie oraz Sądu Polubownego ds. Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji. Trzeba zaznaczyć, iż mediacje i arbitraż, które stają się standardem w rozwiązywaniu sporów związanych z usuwaniem

treści cyfrowych czy blokowaniem dostępu do kont poprzez wdrażanie nowych regulacji w środowisku internetowym (w szczególności dotyczy to konstytucji internetu – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)) stosowane są w dziedzinie domen internetowych na rynku polskim od wielu lat.

Nowe kierunki rozwoju środowiska domen internetowych a nowe zagrożenia

Należy zaznaczyć, że na kwestie bezpieczeństwa środowiska domenowego wpływ ma relacja zależności, która powoduje, że rejestracja domeny internetowej danego poziomu jest równoznaczna z uprawnieniem abonenta do rejestracji (w tym obrębie) innych domen, będących jej poddomenami. Przyjęte rozwiązanie pozwala na przyporządkowywanie wielu subdomen i tworzenie rozbudowanych serwisów internetowych, bez konieczności każdorazowej opłaty rejestracyjnej. Domena drugiego stopnia może mieć charakter funkcjonalny i regionalny, co pozwala na istnienie rozszerzeń. To w znaczącym stopniu wraz z rozwojem nowych technologii stwarza możliwości powstania coraz to nowszych obszarów zagrożeń. Może dochodzić do takich sytuacji, kiedy abonent masowo rejestruje wygasłe domeny. Po wejściu na domenę tego abonenta, użytkownik może być losowo przekierowywany na strony różnych usług komercyjnych, strony z niedozwoloną pornografią, jak również strony związane z fałszywymi inwestycjami. Przede wszystkim może to być środowisko treści nielegalnych czy szkodliwych. Jednak w takiej sytuacji sam abonent domeny – jej posiadacz – najczęściej nie jest powiązany ze stronami, na które następuje przekierowanie. Jako abonent domeny osoba taka korzysta z serwisu do monetyzacji (podobnie jak w przypadku niektórych tzw. domen zaparkowanych) i generuje zysk od każdego wejścia. Ponieważ są to przeważnie wygasłe domeny mogą się jeszcze wyświetlać w wynikach wyszukiwarek oraz znajdować w linkach na stronach oryginalnych (przykładem może być domena gwarancjebgk-konferencja.pl która należała kiedyś do banku BGK). Oczywiście wszystkie podobne sytuacje powodują natychmiastowe reakcje i aktywność rejestru na zasadzie *notice and take action*, co daje gwarancje bezpiecznego rozwoju biznesu w sieci internetowej, często w wyniku działań, które nie wymagają interwencji uprawnionych w długich procesach prowadzonych przez zagraniczne platformy internetowe.

Podsumowanie

Analizując kwestie bezpośrednio nawiązujące do regulacji w obszarze środowiska cyfrowego należy podkreślić, iż niezbędny wydaje się podział obszarów regulacji według określonych kategorii. Wynikiem takiego zabiegu mogłoby być ustalenie zakresu merytorycznego regulacji i dookreślenie podstaw redefinicji pojęcia cyberzagrożenia w kontekście krajowym. Analiza działań w sieci wymaga ustalenia, jakie istnieją podstawowe instrumenty prawne przeciwdziałania zagrożeniom związanym z cyberprzestrzenią i czy te wskazane w regulacjach UE są wystarczające dla polskiego eko systemu e-commerce. Rozwój technologii powoduje, że poszerza się zakres zagrożeń a kwestia odpowiedzialności także w kontekście tzw. głębokiej odpowiedzialności za działania w sieci to obszar, który będzie wymagał diagnozy i nowej weryfikacji, co stanowi kwestie natury moralnej, etycznej, związanej często z konkretną tożsamością narodową.

Bezpieczeństwo systemów informatycznych, których znaczenie w naszym społeczeństwie stale wzrasta, obejmuje wiele aspektów a zwalczanie cyberzagrożeń jest jego kluczowym elementem. W związku z tym stosowane na świecie metody przeciwdziałania zagrożeniom będą wymagały nowych możliwości regulacyjnych ale także technicznych. Środowisko domeny PL. staje się odpowiedzią na pytanie dotyczące alternatywy dla środowiska cyfrowego opartego na regulacjach wdrażanych przez BIG Techy. Rozstrzyganie sporów we własnym kraju w oparciu o krajowe reguły daje nowe możliwości dochodzenia swoich praw. Przegląd i redefinicja wybranych zagrożeń oraz odpowiadających im regulacji prawnych pozwoli dokonać oceny przyjętych standardów ochrony interesów w sieci, ale jednocześnie wnioski z tej analizy mogą stanowić wstęp do poszerzonej diagnozy związanej z nowym etapem rozwoju ery cyfrowej, uwzględniającym warunki krajowe.

Suwerenność technologiczna. Nowy wymiar polskiej racji stanu

Marietta Gieroń

Abstrakt

Artykuł analizuje znaczenie suwerenności technologicznej dla bezpieczeństwa i rozwoju współczesnych państw, ze szczególnym uwzględnieniem perspektywy Polski. Autorka stawia tezę, że w XXI wieku państwa rywalizują nie tylko potencjałem militarnym i gospodarczym, lecz również zdolnością do rozwijania, kontrolowania i zabezpieczania kluczowych technologii. Suwerenność technologiczna nie oznacza dążenia do pełnej samowystarczalności, lecz zdolność do świadomego zarządzania zależnościami technologicznymi oraz utrzymania kontroli nad obszarami mającymi strategiczne znaczenie dla bezpieczeństwa i funkcjonowania państwa. W artykule omówiono pięć filarów suwerenności technologicznej: sztuczną inteligencję, cyberbezpieczeństwo, dane, infrastrukturę cyfrową oraz technologie krytyczne. Autorka wskazuje, że dla Polski kluczowe znaczenie ma rozwijanie kompetencji w obszarach strategicznych, wzmacnianie odporności infrastruktury krytycznej oraz budowanie ekosystemu współpracy między administracją, nauką i biznesem. W konkluzji suwerenność technologiczna zostaje zidentyfikowana jako nowy wymiar polskiej racji stanu.

Słowa kluczowe: suwerenność technologiczna, racja stanu, bezpieczeństwo cyfrowe, sztuczna inteligencja, cyberbezpieczeństwo, infrastruktura krytyczna, geopolityka technologiczna

Wstęp

Jeszcze do niedawna technologie cyfrowe postrzegano przede wszystkim jako narzędzie rozwoju gospodarczego i innowacyjności. Dziś coraz wyraźniej widać, że stały się one również elementem bezpieczeństwa państwa oraz jednym z kluczowych czynników wpływających na układ sił we współczesnym świecie. O pozycji państw decydują już

nie tylko potencjał militarny, wielkość gospodarki czy dostęp do surowców strategicznych, ale również zdolność do rozwijania, wykorzystywania i ochrony technologii.

Potwierdzają to wydarzenia ostatnich lat. Wojna w Ukrainie pokazała znaczenie cyberbezpieczeństwa, komunikacji satelitarnej, systemów bezzałogowych oraz analizy danych dla współczesnych działań militarnych. Z kolei konflikt na Bliskim Wschodzie przypomniał, jak istotną rolę odgrywają technologie wykorzystywane do pozyskiwania i analizowania informacji. Przykładem mogą być kontrowersje związane z aplikacjami gromadzącymi dane lokalizacyjne użytkowników, które w określonych warunkach mogą mieć znaczenie nie tylko komercyjne, ale również wywiadowcze i bezpieczeństwa. Równocześnie rywalizacja pomiędzy Stanami Zjednoczonymi a Chinami o rozwój sztucznej inteligencji, produkcję półprzewodników czy kontrolę nad strategicznymi łańcuchami dostaw pokazuje, że technologia stała się jednym z najważniejszych zasobów geopolitycznych XXI wieku.[1]

W rezultacie coraz częściej mówi się o suwerenności technologicznej państw. Nie oznacza ona pełnej samowystarczalności technologicznej, która w warunkach globalnej gospodarki jest praktycznie niemożliwa do osiągnięcia. Oznacza natomiast zdolność do zachowania podmiotowości w obszarach mających strategiczne znaczenie dla bezpieczeństwa i rozwoju państwa. Dotyczy to przede wszystkim sztucznej inteligencji, cyberbezpieczeństwa, danych, infrastruktury cyfrowej oraz technologii krytycznych. Jednocześnie pojęcie to rodzi pytanie o granice dopuszczalności zależności technologicznej. W praktyce państwa nie są w stanie samodzielnie rozwijać wszystkich kluczowych rozwiązań, dlatego istotne staje się określenie, w jakich obszarach mogą korzystać z technologii zagranicznych, a w jakich powinny dysponować własnymi kompetencjami i kontrolą nad infrastrukturą. Coraz częściej znajduje to odzwierciedlenie w politykach publicznych państw, czego przykładem jest decyzja Francji o stopniowym zastępowaniu w administracji publicznej zagranicznych platform komunikacyjnych, takich jak Microsoft Teams czy Zoom, krajowym rozwiązaniem Visio.[2]

Dla Polski pytanie dziś nie brzmi, czy może stać się globalnym mocarstwem technologicznym na miarę Stanów Zjednoczonych czy Chin. Znacznie ważniejsze jest to, czy będzie dysponowała kompetencjami pozwalającymi chronić własne interesy,

[1] Miller C., *Wielka wojna o chipy. Jak USA i Chiny walczą o technologiczną dominację nad światem,* Warszawa 2023.

[2] Palczewski S., *Francja wyrzuca Zooma i Teamsa z administracji. Rząd podjął decyzję*, CyberDefence24, 27.01.2026, https://cyberdefence24.pl/polityka-i-prawo/francja-wyrzuca-zooma-i-teamsa-z-administracji-rzad-podjal-decyzje

zapewniać bezpieczeństwo obywatelom oraz ograniczać zależności w obszarach kluczowych dla funkcjonowania państwa. W świecie rosnącej rywalizacji technologicznej staje się to jednym z warunków zachowania podmiotowości i zdolności do samodzielnego kształtowania własnego rozwoju.

Celem artykułu jest analiza znaczenia suwerenności technologicznej dla bezpieczeństwa i rozwoju państwa oraz wskazanie jej roli jako jednego z elementów współczesnej racji stanu. Stawiam więc tezę, że w XXI wieku państwa konkurują nie tylko potencjałem militarnym i gospodarczym, ale również zdolnością do rozwijania, kontrolowania i zabezpieczania kluczowych technologii. Dlatego suwerenność technologiczna w mojej ocenie jest nowym wymiarem racji stanu.

Technologia jako nowy wymiar siły państwa

Przez większą część XX wieku technologie postrzegano przede wszystkim jako czynnik wzrostu gospodarczego. Państwa inwestowały w badania i rozwój, aby zwiększać konkurencyjność swoich gospodarek, wspierać innowacje oraz poprawiać jakość życia obywateli. Rozwój technologiczny był zatem kojarzony głównie z modernizacją i postępem ekonomicznym.

W XXI wieku sposób myślenia o technologii uległ jednak zasadniczej zmianie. Coraz częściej jest ona postrzegana nie tylko jako źródło wzrostu gospodarczego, ale również jako instrument wpływu politycznego, bezpieczeństwa oraz budowania przewagi strategicznej. Państwa konkurują dziś nie tylko o kapitał, zasoby naturalne czy przewagę militarną, lecz także o dostęp do danych, rozwój sztucznej inteligencji, kontrolę nad infrastrukturą cyfrową oraz technologiami krytycznymi. W efekcie technologia stała się jednym z kluczowych elementów współczesnej siły państwa.

Jak technologia stała się zasobem strategicznym

Dobrym przykładem zmiany znaczenia technologii są półprzewodniki. Chris Miller w książce „Wielka wojna o chipy"[3] pokazuje, że układy scalone stały się fundamentem

[3] Miller C., *Wielka wojna o chipy. Jak USA i Chiny walczą o technologiczną dominację nad światem,* Warszawa 2023.

funkcjonowania współczesnych gospodarek, administracji publicznej oraz systemów bezpieczeństwa. Bez zaawansowanych półprzewodników nie mogłyby działać nowoczesne systemy uzbrojenia, infrastruktura telekomunikacyjna, centra danych ani rozwiązania wykorzystujące sztuczną inteligencję.

To właśnie dlatego rywalizacja o dostęp do najbardziej zaawansowanych chipów stała się jednym z najważniejszych elementów współczesnej geopolityki. Ograniczenia eksportowe nakładane przez Stany Zjednoczone na Chiny pokazują, że technologie krytyczne są dziś traktowane podobnie jak strategiczne surowce. Państwo, które nie posiada dostępu do kluczowych technologii, może mieć ograniczone możliwości rozwoju gospodarczego, militarnego i technologicznego.

Przykład półprzewodników pokazuje, że technologia przestała być wyłącznie narzędziem wspierającym gospodarkę. Stała się zasobem strategicznym wpływającym na bezpieczeństwo i pozycję państw w systemie międzynarodowym.

Technologia jako narzędzie geopolityki

Rosnące znaczenie technologii sprawia, że stają się one również narzędziem realizacji celów politycznych. Henry Farrell i Abraham Newman zwracają uwagę, że państwa coraz częściej wykorzystują istniejące zależności gospodarcze i technologiczne jako instrument wpływu.[4] Kontrola nad sieciami komunikacyjnymi, przepływem danych czy kluczową infrastrukturą może być wykorzystywana do wywierania presji politycznej i gospodarczej.

W takim ujęciu technologia staje się elementem geopolityki. Państwa nie rywalizują już wyłącznie o terytorium czy surowce, ale również o kontrolę nad infrastrukturą cyfrową, standardami technologicznymi oraz strategicznymi łańcuchami dostaw. Rywalizacja pomiędzy Stanami Zjednoczonymi a Chinami dotycząca sztucznej inteligencji, półprzewodników czy sieci telekomunikacyjnych pokazuje, że przewaga technologiczna jest dziś postrzegana jako warunek utrzymania wpływów politycznych i gospodarczych.

Technologia jest również wykorzystywana przez państwa do zwiększania kontroli nad przestrzenią informacyjną i ograniczania wpływu podmiotów zewnętrznych

[4] Farrell H, Newman A., *Underground Empire. How America Weaponized the World Economy*, New York 2023.

na społeczeństwo. Szczególnie widoczne jest to w przypadku Chin i Rosji, które rozwijają rozwiązania umożliwiające częściową separację krajowej przestrzeni cyfrowej od globalnego Internetu. Chiny od lat budują system kontroli przepływu informacji określany mianem „Wielkiego Firewalla", natomiast Rosja rozwija koncepcję tzw. Suwerennego Internetu, zakładając możliwość funkcjonowania krajowej infrastruktury sieciowej niezależnie od globalnych połączeń. Działania te są uzasadniane względami bezpieczeństwa narodowego, jednak równocześnie zwiększają możliwości kontroli społeczeństwa i kształtowania obiegu informacji przez państwo.

Wojna w Ukrainie dodatkowo uwidoczniła znaczenie technologii dla bezpieczeństwa państwa. Kluczową rolę odegrały nie tylko tradycyjne systemy uzbrojenia, ale również komunikacja satelitarna, analiza danych, systemy bezzałogowe oraz cyberbezpieczeństwo. Pokazało to, że współczesne konflikty coraz częściej rozgrywają się równolegle w przestrzeni fizycznej i cyfrowej.

Państwa, Big Tech i nowy układ sił

Współczesna rywalizacja technologiczna nie dotyczy wyłącznie państw. Coraz większą rolę odgrywają również globalne korporacje technologiczne. Jak zauważa Sylwia Czubkowska w książce „Bóg techy"[5], największe firmy technologiczne dysponują zasobami danych, wiedzy i kapitału porównywalnymi z potencjałem wielu państw. Kontrolują również platformy komunikacyjne, usługi chmurowe oraz infrastrukturę cyfrową wykorzystywaną przez administrację, biznes i obywateli.

Dobrym przykładem jest wykorzystanie systemu Starlink podczas wojny w Ukrainie. Pokazało ono, że prywatna firma może odgrywać istotną rolę w zapewnianiu ciągłości komunikacji na obszarze objętym konfliktem zbrojnym. Jednocześnie rodzi to pytania o zakres zależności państw od podmiotów prywatnych oraz o granice ich wpływu na bezpieczeństwo narodowe.

Podobne wątpliwości dotyczą danych gromadzonych przez platformy cyfrowe i aplikacje mobilne. Informacje pozyskiwane pierwotnie w celach komercyjnych mogą mieć znaczenie wywiadowcze, polityczne lub strategiczne. Coraz częściej zwraca się uwagę również na rolę platform społecznościowych w kształtowaniu

[5] Czubkowska S., *Bóg techy. Jak wielkie firmy technologiczne przejmują władzę nad Polską i Światem*, Kraków 2025.

debaty publicznej oraz ich podatność na wykorzystywanie do działań dezinformacyjnych. Doświadczenia ostatnich lat pokazują, że media społecznościowe mogą być wykorzystywane do wpływania na procesy wyborcze, polaryzowania społeczeństwa czy prowadzenia operacji informacyjnych przez podmioty państwowe i niepaństwowe. W rezultacie pytanie o suwerenność technologiczną nie dotyczy już wyłącznie relacji pomiędzy państwami, lecz również relacji pomiędzy państwami a globalnymi korporacjami technologicznymi, które dysponują realnym wpływem na obieg informacji i funkcjonowanie współczesnych demokracji.

Technologia stała się zatem jednym z najważniejszych czynników kształtujących współczesny układ sił. O pozycji państw decyduje dziś nie tylko zdolność do wykorzystywania nowych technologii, ale również umiejętność zarządzania zależnościami, jakie technologie te tworzą.

Czym jest suwerenność technologiczna?

W debacie publicznej pojęcie suwerenności technologicznej pojawia się coraz częściej, jednak nadal nie ma jednej powszechnie akceptowanej definicji tego terminu.[6] Najczęściej jest ono rozumiane jako zdolność państwa do zachowania kontroli nad technologiami mającymi strategiczne znaczenie dla bezpieczeństwa, gospodarki oraz funkcjonowania administracji publicznej. W przypadku państw takich jak Polska nie chodzi przy tym o pełną samowystarczalność technologiczną, lecz o zdolność do podejmowania niezależnych decyzji i ograniczania ryzyka wynikającego z nadmiernych zależności od podmiotów zewnętrznych. W przypadku największych mocarstw technologicznych, takich jak Stany Zjednoczone czy Chiny, pojęcie to bywa rozumiane szerzej i obejmuje także zdolność do samodzielnego rozwijania kluczowych technologii, wyznaczania globalnych standardów oraz kształtowania międzynarodowych łańcuchów dostaw.

W praktyce pytanie o suwerenność technologiczną sprowadza się do bardzo konkretnych kwestii. Czy państwo potrafi ochronić swoją infrastrukturę przed cyberatakiem? Czy posiada dostęp do danych niezbędnych do podejmowania decyzji? Czy jest w stanie utrzymać funkcjonowanie administracji i usług publicznych w sytuacji kryzysowej? Czy dysponuje kompetencjami pozwalającymi rozumieć i rozwijać technologie mające znaczenie dla bezpieczeństwa narodowego?

[6] Pohle J., Thiel T., *Digital Sovereignty*, *Internet Policy Review*, vol. 9, no. 4, 2020.

Niezależność decyzyjna i odporność państwa

Jednym z kluczowych elementów suwerenności technologicznej jest zachowanie niezależności decyzyjnej państwa. Henry Farrell i Abraham Newman zwracają uwagę, że współczesne zależności technologiczne mogą być wykorzystywane jako narzędzie wpływu politycznego.[7] Kontrola nad infrastrukturą cyfrową, przepływem danych czy strategicznymi technologiami pozwala wywierać presję porównywalną z tradycyjnymi instrumentami polityki międzynarodowej.

W tym kontekście suwerenność technologiczna oznacza zdolność do prowadzenia polityki publicznej bez ryzyka, że dostęp do kluczowych technologii zostanie ograniczony przez podmioty zewnętrzne. Nie chodzi wyłącznie o bezpieczeństwo militarne, lecz również o możliwość zapewnienia ciągłości działania administracji publicznej, sektora finansowego, ochrony zdrowia czy infrastruktury krytycznej.

Znaczenie odporności technologicznej szczególnie wyraźnie ujawniło się podczas pandemii COVID-19 oraz późniejszych zakłóceń w globalnych łańcuchach dostaw. Problemy z dostępnością półprzewodników pokazały, jak silnie współczesne gospodarki uzależnione są od technologii produkowanych poza własnym terytorium. Podobne ryzyko dotyczy również usług chmurowych, systemów telekomunikacyjnych czy narzędzi sztucznej inteligencji

Ograniczanie zależności technologicznych

Suwerenność technologiczna nie oznacza rezygnacji z międzynarodowej współpracy ani budowania technologicznej autarkii. Współczesne państwa funkcjonują w globalnych sieciach zależności, a rozwój większości technologii opiera się na współpracy międzynarodowej. Problem pojawia się jednak wtedy, gdy zależności dotyczą obszarów mających znaczenie strategiczne dla bezpieczeństwa państwa.

Jak zauważa Sylwia Czubkowska, współczesne państwa są coraz bardziej uzależnione od usług świadczonych przez globalne korporacje technologiczne.[8] Dotyczy to nie tylko mediów społecznościowych, ale również usług chmurowych, systemów

[7] Farrell H, Newman A., *Underground Empire. How America Weaponized the World Economy*, New York 2023.

[8] Czubkowska S., *Bóg techy. Jak wielkie firmy technologiczne przejmują władzę nad Polską i Światem*, Kraków 2025.

operacyjnych, platform komunikacyjnych czy narzędzi wykorzystywanych przez administrację publiczną. Oznacza to, że pytanie o suwerenność technologiczną nie dotyczy wyłącznie relacji pomiędzy państwami, lecz również relacji pomiędzy państwami a globalnymi firmami technologicznymi.

Problem nie polega na samym korzystaniu z zagranicznych technologii. Problem pojawia się wtedy, gdy państwo nie posiada kompetencji pozwalających ocenić skalę ryzyka oraz świadomie zarządzać powstającymi zależnościami. Dlatego jednym z podstawowych celów suwerenności technologicznej jest identyfikacja obszarów szczególnie istotnych dla bezpieczeństwa państwa oraz rozwijanie kompetencji pozwalających ograniczać najbardziej ryzykowne zależności. Jednocześnie nie wszystkie zależności technologiczne mają charakter negatywny. W przypadku Unii Europejskiej współpraca technologiczna i gospodarcza może zwiększać odporność państw członkowskich poprzez tworzenie mechanizmów wzajemnego wsparcia w sytuacjach kryzysowych. Suwerenność technologiczna nie oznacza zatem eliminowania współzależności, ale budowanie takich relacji, które ograniczają ryzyko jednostronnej zależności i wzmacniają zdolność do reagowania na zagrożenia.

Polska, podobnie jak wiele państw europejskich, w znacznym stopniu opiera funkcjonowanie gospodarki cyfrowej na rozwiązaniach dostarczanych przez globalne korporacje technologiczne. Dotyczy to usług chmurowych, systemów operacyjnych, narzędzi komunikacyjnych czy platform cyfrowych. Taka sytuacja nie musi stanowić zagrożenia sama w sobie, jednak zwiększa znaczenie kompetencji pozwalających świadomie zarządzać powstającymi zależnościami. Nie można pominąć faktu, że elementem suwerenności technologicznej jest również interoperacyjność, rozumiana jako zdolność współpracy różnych systemów oraz możliwość przenoszenia danych i usług pomiędzy dostawcami. Znaczenie tego aspektu uwidoczniła wojna w Ukrainie, kiedy część danych administracji publicznej została przeniesiona do infrastruktury chmurowej poza granicami kraju, co pozwoliło zabezpieczyć kluczowe zasoby państwa oraz zapewnić ciągłość działania instytucji publicznych. Przykład ten pokazuje, że odporność państwa może wynikać nie tylko z posiadania własnych rozwiązań technologicznych, ale również z możliwości bezpiecznego korzystania z infrastruktury partnerów oraz sprawnego przenoszenia danych pomiędzy systemami.[9]

[9] Amazon Web Services, *Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future*, 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Suwerenność technologiczna nie jest więc pytaniem o to, czy państwo posiada własny odpowiednik Google, Microsoftu czy OpenAI. Jest pytaniem o to, czy potrafi chronić własne interesy w świecie, w którym kluczowe technologie coraz częściej znajdują się poza jego bezpośrednią kontrolą.

Filary współczesnej suwerenności technologicznej państwa

Suwerenność technologiczna nie sprowadza się do posiadania nowoczesnych technologii. O jej poziomie decyduje zdolność państwa do rozwijania, kontrolowania i zabezpieczania obszarów mających strategiczne znaczenie dla bezpieczeństwa, gospodarki oraz funkcjonowania instytucji publicznych. W praktyce można wskazać pięć filarów, które w największym stopniu wpływają na zdolność państwa do zachowania technologicznej podmiotowości: sztuczną inteligencję, cyberbezpieczeństwo, dane, infrastrukturę cyfrową oraz technologie krytyczne.

Sztuczna inteligencja

Państwo, które nie rozumie sztucznej inteligencji, ryzykuje utratę zdolności konkurowania gospodarczo i technologicznie. Henry Kissinger, Eric Schmidt i Daniel Huttenlocher w książce „The Age of AI"[10] wskazują, że sztuczna inteligencja może zmienić sposób funkcjonowania państw równie głęboko, jak wcześniej zrobiła to rewolucja przemysłowa. AI nie jest już wyłącznie narzędziem biznesowym. Wykorzystywana jest w analizie danych wywiadowczych, ochronie infrastruktury krytycznej, systemach rozpoznania oraz procesach wspierających podejmowanie decyzji.

Znaczenie sztucznej inteligencji wynika przede wszystkim z jej zdolności do przetwarzania ogromnych ilości danych w czasie niemożliwym do osiągnięcia przez człowieka. Państwa inwestujące w rozwój AI zyskują przewagę nie tylko gospodarczą, ale również administracyjną i militarną. Coraz częściej sztuczna inteligencja wykorzystywana jest również do analizy informacji wywiadowczych,

[10] Kissinger H., Schmidt E., Huttenlocher D., *The Age of AI: And Our Human Future*, Little, Brown and Company, 2021.

wykrywania zagrożeń w cyberprzestrzeni oraz wspierania procesów decyzyjnych w administracji publicznej i sektorze obronnym. Nieprzypadkowo rozwój sztucznej inteligencji stał się jednym z głównych obszarów rywalizacji pomiędzy Stanami Zjednoczonymi a Chinami.

Dla Polski kluczowe znaczenie ma nie tyle stworzenie własnego odpowiednika OpenAI, ile rozwijanie kompetencji pozwalających rozumieć, wdrażać i bezpiecznie wykorzystywać rozwiązania oparte na sztucznej inteligencji w administracji, gospodarce oraz sektorze bezpieczeństwa.

Cyberbezpieczeństwo

Państwo niezdolne do ochrony własnej infrastruktury cyfrowej może utracić zdolność skutecznego działania nawet bez użycia tradycyjnych środków militarnych. Wraz z postępującą cyfryzacją administracji publicznej, sektora finansowego, energetyki czy transportu cyberbezpieczeństwo staje się jednym z podstawowych warunków funkcjonowania współczesnego państwa.

Jak zauważa Nicole Perlroth,[11] cyberprzestrzeń stała się obszarem rywalizacji państw, w którym przewaga nie zawsze wynika z liczebności armii czy potencjału gospodarczego, lecz ze zdolności do wykorzystywania podatności systemów informatycznych przeciwnika. Cyberataki mogą prowadzić do zakłócenia funkcjonowania administracji publicznej, systemów energetycznych, sieci telekomunikacyjnych czy usług finansowych, stając się narzędziem realizacji celów politycznych i militarnych.

Szczególnie wyraźnie pokazała to wojna w Ukrainie. Jednym z pierwszych działań poprzedzających rosyjską inwazję był cyberatak na satelitarną sieć Viasat, wykorzystywaną do komunikacji i transmisji danych.[12] Pokazało to, że działania prowadzone w cyberprzestrzeni mogą bezpośrednio wpływać na zdolność państwa do prowadzenia operacji wojskowych oraz utrzymania ciągłości działania kluczowych systemów.

Również Polska znajduje się w grupie państw regularnie narażonych na ataki wymierzone w administrację publiczną, przedsiębiorstwa infrastruktury krytycznej

[11] Perlroth N., *This Is How They Tell Me the World Ends. The Cyberweapons Arms Race*, Bloomsbury Publishing, 2021.

[12] Viasat, *KA-SAT Network Cyber Attack Overview*, KA-SAT Network cyber attack overview | Viasat

oraz sektor energetyczny. W takich warunkach rozwój krajowych kompetencji w zakresie cyberbezpieczeństwa staje się nie tylko kwestią techniczną, lecz jednym z fundamentów bezpieczeństwa narodowego.

Dane jako zasób strategiczny

Państwo, które nie kontroluje własnych danych, stopniowo traci zdolność do samodzielnego podejmowania decyzji. Dane stały się jednym z najcenniejszych zasobów współczesnego świata i podstawą funkcjonowania gospodarki cyfrowej. Stanowią fundament działania sztucznej inteligencji, systemów analitycznych oraz procesów decyzyjnych wykorzystywanych zarówno przez administrację publiczną, jak i sektor prywatny.

Yuval Noah Harari[13] zwraca uwagę, że dane stają się zasobem o znaczeniu porównywalnym do ziemi w epoce agrarnej czy kapitału w epoce przemysłowej. To właśnie dostęp do danych pozwala rozwijać modele sztucznej inteligencji, przewidywać zachowania społeczne, analizować zagrożenia oraz podejmować decyzje w oparciu o wiedzę, a nie wyłącznie intuicję. W tym sensie dane stają się jednym z kluczowych źródeł przewagi państw i organizacji.

Znaczenie mają nie tylko dane osobowe obywateli, ale również informacje dotyczące funkcjonowania administracji publicznej, infrastruktury krytycznej, procesów gospodarczych czy procedur bezpieczeństwa. Jak zauważa Sylwia Czubkowska, dane są dziś źródłem władzy i wpływu nie tylko dla państw, ale również dla globalnych korporacji technologicznych.[14] To właśnie dzięki dostępowi do ogromnych zbiorów danych największe platformy cyfrowe mogą rozwijać zaawansowane algorytmy, personalizować przekaz informacyjny oraz budować przewagę ekonomiczną.

Rosnące znaczenie danych wiąże się również z rozwojem Internetu Rzeczy (IoT), obejmującego coraz większą liczbę urządzeń podłączonych do sieci. Dane generują dziś nie tylko komputery i smartfony, ale również pojazdy, systemy monitoringu, urządzenia przemysłowe, inteligentne liczniki energii czy elementy infrastruktury miejskiej. Zatem pytanie o bezpieczeństwo danych staje się jednocześnie pytaniem

[13] Harari Y.N., *Homo Deus. Krótka historia jutra,* Wydawnictwo Literackie, 2018.

[14] Czubkowska S., *Bóg techy. Jak wielkie firmy technologiczne przejmują władzę nad Polską i Światem*, Kraków 2025.

o świadomy dobór technologii wykorzystywanych przez państwo oraz podmioty odpowiedzialne za infrastrukturę krytyczną. Dobrym przykładem są współczesne samochody wyposażone w zaawansowane systemy telematyczne, które gromadzą i przesyłają informacje o lokalizacji, sposobie użytkowania pojazdu czy jego otoczeniu. Pokazuje to, że bezpieczeństwo danych nie dotyczy już wyłącznie systemów informatycznych, ale również urządzeń fizycznych generujących i przetwarzających informacje, które stają się elementem infrastruktury cyfrowej państwa.

Państwo, które traci kontrolę nad strategicznymi zasobami danych, ogranicza swoją zdolność do samodzielnego kształtowania polityk publicznych i ochrony interesów narodowych. Dane są więc nie tylko zasobem gospodarczym, ale również instrumentem bezpieczeństwa narodowego oraz źródłem przewagi strategicznej. W świecie sztucznej inteligencji i gospodarki cyfrowej pytanie o dane staje się jednocześnie pytaniem o zakres technologicznej suwerenności państwa.

Infrastruktura cyfrowa

Suwerenność technologiczna nie jest możliwa bez infrastruktury umożliwiającej przetwarzanie, przechowywanie i przesyłanie informacji. Obejmuje ona między innymi centra danych, usługi chmurowe, sieci telekomunikacyjne, systemy łączności oraz infrastrukturę satelitarną. To właśnie na nich opiera się funkcjonowanie administracji publicznej, gospodarki cyfrowej i usług świadczonych obywatelom.

Współczesne państwo jest w coraz większym stopniu uzależnione od sprawnego działania infrastruktury cyfrowej. Zakłócenie funkcjonowania sieci telekomunikacyjnych, centrów danych czy usług chmurowych może prowadzić do problemów w administracji publicznej, sektorze finansowym, ochronie zdrowia oraz systemach odpowiedzialnych za bezpieczeństwo państwa. Oznacza to, że infrastruktura cyfrowa staje się elementem infrastruktury krytycznej, podobnie jak sieci energetyczne czy systemy transportowe. Natomiast największym wyzwaniem nie jest sama zależność od infrastruktury cyfrowej a skala skutków jej potencjalnego zakłócenia. Im więcej usług publicznych i sektorów krytycznych opiera się na wspólnych zasobach technologicznych, tym większe ryzyko, że awaria pojedynczego komponentu wywoła kaskadowe zakłócenia w funkcjonowaniu całego państwa. Z tego względu suwerenność technologiczna obejmuje również zdolność do utrzymania ciągłości działania w warunkach częściowej utraty infrastruktury lub niedostępności świadczonych usług przed podmioty zewnętrzne.

Znaczenie infrastruktury cyfrowej szczególnie wyraźnie uwidoczniła wojna w Ukrainie. Wykorzystanie systemu Starlink pozwoliło utrzymać łączność na obszarach objętych działaniami wojennymi, pokazując jednocześnie, jak istotną rolę mogą odgrywać prywatni dostawcy infrastruktury komunikacyjnej. Przykład ten unaocznił również nowe wyzwania związane z zależnością państw od technologii znajdujących się poza ich bezpośrednią kontrolą.[15]

Kontrola nad infrastrukturą cyfrową nie oznacza konieczności posiadania wszystkich technologii na własność. Oznacza natomiast zdolność do zapewnienia ciągłości funkcjonowania państwa, gospodarki oraz usług publicznych, a także świadomego zarządzania ryzykiem wynikającym z zależności technologicznych. W tym sensie infrastruktura cyfrowa stanowi jeden z podstawowych filarów współczesnej suwerenności technologicznej.

Technologie krytyczne

Współczesna gospodarka i bezpieczeństwo państw opierają się na technologiach, których większość obywateli nigdy nie zobaczy bezpośrednio. Dobrym przykładem są półprzewodniki. Jak wskazuje Chris Miller w książce „Wielka wojna o chipy"[16] pokazuje, że układy scalone stały się fundamentem nowoczesnej gospodarki, infrastruktury cyfrowej oraz systemów wojskowych. Bez nich nie działają smartfony, centra danych, sieci telekomunikacyjne, samochody, systemy uzbrojenia ani rozwiązania wykorzystujące sztuczną inteligencję.

Do technologii krytycznych zalicza się również technologie kwantowe, technologie kosmiczne, zaawansowaną elektronikę, technologie energetyczne oraz wybrane rozwiązania z obszaru biotechnologii. Ich znaczenie wynika z tego, że wpływają nie tylko na konkurencyjność gospodarki, ale również na zdolność państwa do ochrony infrastruktury, prowadzenia działań obronnych oraz uczestnictwa w globalnych łańcuchach wartości.

Rywalizacja pomiędzy Stanami Zjednoczonymi a Chinami pokazuje, że kontrola nad technologiami krytycznymi stała się jednym z głównych elementów współczesnej

[15] Satariano A., Reinhard S., Metz C., Frenkel S., Khurana M., *Elon Musk's Unmatched Power in the Stars,* The New York Times, 28.07.2023

[16] Miller C., *Wielka wojna o chipy. Jak USA i Chiny walczą o technologiczną dominację nad światem,* Warszawa 2023.

geopolityki. Ograniczenia eksportowe dotyczące zaawansowanych chipów nie są wyłącznie decyzjami handlowymi. Są elementem polityki bezpieczeństwa i próbą ograniczania zdolności technologicznych konkurenta.

Z perspektywy suwerenności technologicznej kluczowe nie jest to, aby każde państwo samodzielnie produkowało wszystkie technologie krytyczne. Istotne jest natomiast, aby potrafiło rozpoznać, które z nich mają znaczenie strategiczne, gdzie powstają najbardziej ryzykowne zależności oraz w jakich obszarach należy rozwijać własne kompetencje. W tym sensie technologie krytyczne są nie tylko przedmiotem polityki przemysłowej, ale również elementem strategii bezpieczeństwa państwa.

Polska wobec nowego wyścigu technologicznego

Debata o suwerenności technologicznej najczęściej koncentruje się na rywalizacji największych mocarstw, przede wszystkim Stanów Zjednoczonych i Chin. Dla Polski zasadnicze pytanie nie brzmi jednak, jak stać się globalnym liderem technologicznym. Znacznie ważniejsze jest to, czy państwo będzie posiadało kompetencje pozwalające chronić własne interesy i zapewniać bezpieczeństwo obywatelom w świecie, w którym technologie stają się jednym z głównych narzędzi wpływu politycznego, gospodarczego i militarnego.

Polska nie stoi dziś przed wyborem, czy uczestniczyć w wyścigu technologicznym. Ten wyścig już trwa. Państwa konkurują o dostęp do danych, rozwój sztucznej inteligencji, ochronę infrastruktury krytycznej oraz kompetencje specjalistów. W takich warunkach technologie przestają być wyłącznie elementem polityki gospodarczej i stają się jednym z filarów bezpieczeństwa państwa.

Zasadniczym wyzwaniem staje się określenie, w jaki sposób Polska może budować podmiotowość technologiczną nie poprzez próbę rywalizacji z największymi graczami, lecz przez rozwój wybranych specjalizacji, wzmacnianie krajowego zaplecza badawczo-rozwojowego oraz świadome lokowanie się w strategicznych segmentach rynku. Dla państwa średniej wielkości suwerenność technologiczna nie oznacza bowiem osiągnięcia pełnej samowystarczalności, lecz zdolność do rozwijania kluczowych kompetencji, ochrony strategicznych zasobów oraz zachowania możliwości samodzielnego podejmowania decyzji w obszarach istotnych dla bezpieczeństwa i rozwoju.

Technologie jako element bezpieczeństwa państwa

Bezpieczeństwo państwa coraz częściej zaczyna się od infrastruktury cyfrowej, danych i kompetencji technologicznych. Współczesne zagrożenia mają charakter hybrydowy i obejmują nie tylko działania militarne, ale również cyberataki, operacje informacyjne oraz próby destabilizacji kluczowych systemów państwa.

Wojna w Ukrainie pokazała, że skuteczność państwa zależy nie tylko od liczebności armii czy poziomu wydatków obronnych. Równie istotne są zdolności związane z cyberobroną, komunikacją satelitarną, analizą danych oraz wykorzystaniem nowoczesnych technologii na potrzeby bezpieczeństwa. Wnioski płynące z tego konfliktu mają szczególne znaczenie dla Polski, która funkcjonuje w bezpośrednim sąsiedztwie obszaru objętego działaniami wojennymi i pozostaje jednym z głównych celów działań prowadzonych w cyberprzestrzeni.

Szczególnego znaczenia nabiera w tym kontekście cyberodporność infrastruktury krytycznej. W warunkach wojny hybrydowej lub konfliktu zbrojnego celem działań przeciwnika mogą stać się nie tylko systemy wojskowe, lecz również sieci energetyczne, systemy łączności, infrastruktura transportowa, wodociągi czy placówki ochrony zdrowia. Zakłócenie ich funkcjonowania może prowadzić do paraliżu części usług publicznych, utrudniać prowadzenie działań obronnych oraz obniżać odporność społeczeństwa na sytuacje kryzysowe. Oznacza to, że zdolność do ochrony i szybkiego odtwarzania kluczowych systemów cyfrowych staje się jednym z warunków skutecznego funkcjonowania państwa w sytuacji zagrożenia.

Kompetencje jako fundament suwerenności technologicznej

Suwerenność technologiczna nie zaczyna się od technologii, lecz od ludzi. Nawet najbardziej zaawansowane rozwiązania nie zwiększą bezpieczeństwa państwa, jeśli zabraknie specjalistów zdolnych je rozwijać, wdrażać i bezpiecznie wykorzystywać.

Dlatego jednym z najważniejszych wyzwań stojących przed Polską jest rozwój krajowych kompetencji technologicznych. Dotyczy to zarówno ekspertów z zakresu cyberbezpieczeństwa, analizy danych i sztucznej inteligencji, jak również specjalistów zajmujących się infrastrukturą cyfrową, elektroniką czy technologiami kosmicznymi.

Polska nie startuje jednak od zera. Dysponuje wysoko wykwalifikowanymi specjalistami z zakresu cyberbezpieczeństwa, programowania, analizy danych czy nowych technologii, którzy od lat są cenieni na rynku międzynarodowym. Wyzwanie polega nie tyle na braku talentów, ile na tworzeniu warunków pozwalających wykorzystywać ich potencjał na rzecz rozwoju państwa i krajowej gospodarki. Wyzwaniem pozostaje nie tylko kształcenie nowych specjalistów, lecz również ograniczanie odpływu talentów do zagranicznych przedsiębiorstw oraz tworzenie warunków do rozwijania zaawansowanych projektów technologicznych w kraju. Warto również podkreślić, że niedobór specjalistów posiadających zaawansowane kompetencje cyfrowe nie jest problemem wyłącznie Polski, lecz całej Unii Europejskiej. Rosnące zapotrzebowanie na ekspertów z zakresu cyberbezpieczństwa, sztucznej inteligencji czy analizy danych sprawia, że państwa oraz przedsiębiorstwa konkurują o wykwalifikowane kadry, traktując je jako jeden z kluczowych zasobów strategicznych. W debacie o suwerenności technologicznej często koncentrujemy się na technologiach. Tymczasem ostatecznie to nie technologie, lecz ludzie decydują o zdolności państwa do ich rozwijania, rozumienia i bezpiecznego wykorzystywania.

Inwestowanie w edukację, badania naukowe oraz rozwój kadr powinno być postrzegane nie tylko jako element polityki rozwojowej, ale również jako inwestycja w długoterminowe bezpieczeństwo państwa. Kompetencje technologiczne stają się bowiem jednym z najważniejszych zasobów strategicznych współczesnych państw.

Technologie strategiczne z perspektywy Polski

Polska nie musi rozwijać wszystkich technologii przyszłości ani konkurować z największymi światowymi ośrodkami badawczymi. Kluczowe znaczenie ma natomiast świadome określenie tych obszarów, które mają strategiczne znaczenie dla bezpieczeństwa i rozwoju państwa.

Pytanie nie brzmi, czy Polska powinna konkurować technologicznie ze Stanami Zjednoczonymi lub Chinami. Pytanie brzmi, które technologie mają znaczenie dla bezpieczeństwa państwa i w których obszarach konieczne jest budowanie własnych kompetencji. Z perspektywy Polski szczególne znaczenie mają cyberbezpieczeństwo, sztuczna inteligencja, przetwarzanie danych, infrastruktura cyfrowa oraz technologie wykorzystywane w sektorze obronnym. Coraz większą rolę odgrywają

również technologie kosmiczne, systemy komunikacji satelitarnej oraz wybrane obszary zaawansowanej elektroniki.

Rozwijanie kompetencji technologicznych wymaga jednak odpowiedniego otoczenia regulacyjnego i instytucjonalnego. W warunkach szybkich zmian technologicznych nadmiernie rozbudowane procedury oraz utrudniona współpraca pomiędzy administracją publiczną a sektorem prywatnym mogą ograniczać tempo wdrażania innowacji. Szczególnie widoczne jest to w obszarach związanych z bezpieczeństwem i obronnością, gdzie szybkość działa coraz częściej staje się równie istotna jak dostęp do technologii.

Dobrym przykładem są technologie bezzałogowe. Doświadczenia wojny w Ukrainie pokazały, jak duże znaczenie ma zdolność szybkiego testowania, rozwijania i wdrażania nowych rozwiązań przy ścisłej współpracy państwa, wojska i przedsiębiorców.[17] Wnioski płynące z tego doświadczenia powinny stanowić ważną lekcję również dla Polski.

Świadome określenie priorytetów technologicznych oraz tworzenie warunków sprzyjających rozwojowi innowacji pozwala efektywniej wykorzystywać ograniczone zasoby finansowe i organizacyjne. W przypadku Polski nie chodzi o próbę osiągnięcia technologicznej samowystarczalności, lecz o rozwijanie kompetencji w obszarach mających kluczowe znaczenie dla bezpieczeństwa państwa i jego długoterminowego rozwoju. Ich wspólną cechą jest to, że stanowią technologie ogólnego zastosowania (general purpose technologies), wpływające równocześnie na bezpieczeństwo, konkurencyjność gospodarki oraz zdolność państwa do funkcjonowania w sytuacjach kryzysowych.

Współpraca nauki, biznesu i administracji

Budowanie suwerenności technologicznej wymaga sprawnego ekosystemu łączącego administrację publiczną, naukę i biznes. Żadne państwo nie jest dziś w stanie samodzielnie rozwijać wszystkich technologii kluczowych dla bezpieczeństwa i rozwoju. Jednocześnie bez zdolności państwa do wyznaczania priorytetów, finansowania badań, wykorzystywania zamówień publicznych oraz koordynowania działań

[17] Dr Watling J., Danylyuk O. V, Reynolds N., Royal United Services Institute (RUSI), *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War*, London 2023

różnych podmiotów trudno o trwałe budowanie krajowych kompetencji technologicznych. Z kolei bez zaplecza naukowego i przedsiębiorstw zdolnych do prowadzenia badań, wdrożeń i skalowania rozwiązań suwerenność technologiczna pozostaje tylko hasłem politycznym, a nie realną zdolnością państwa.

Polska dysponuje potencjałem naukowym, rozwijającym się sektorem nowych technologii oraz instytucjami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni. Kluczowym wyzwaniem pozostaje jednak nie tyle brak zasobów, ile zdolność do ich łączenia wokół jasno sprecyzowanych celów. Chodzi o takie mechanizmy współpracy, które pozwolą szybciej przekładać wyniki badan na wdrożenia, skuteczniej wykorzystywać zamówienia publiczne do stymulowania innowacji oraz rozwijać technologie istotne z perspektywy bezpieczeństwa państwa i odporności gospodarki.

Wymiar ten ma również znaczenie gospodarcze. Od jakości współpracy nauki, biznesu i administracji zależy, czy Polska pozostanie przede wszystkim miejscem wdrażania i obsługi technologii tworzonych gdzie indziej czy też będzie rozwijać kompetencje pozwalające projektować własne rozwiązania, budować przewagi w wybranych specjalizacjach oraz tworzyć miejsca pracy o wysokiej wartości dodanej. W tym aspekcie współpraca tych trzech środowisk jest nie tylko warunkiem bezpieczeństwa i odporności państwa, ale również jednym z warunków długofalowej modernizacji gospodarki.

Dla państwa średniej wielkości, jakim jest Polska, suwerenność technologiczna nie będzie wynikała z próby konkurowania z największymi mocarstwami we wszystkich obszarach technologicznych. Będzie natomiast zależała od zdolności do rozwijania wybranych specjalizacji, budowania własnych kompetencji oraz skutecznego wykorzystywania potencjału nauki, biznesu i administracji do realizacji celów strategicznych państwa.

Suwerenność technologiczna jako element polskiej racji stanu

Pojęcie racji stanu odnosi się do ochrony fundamentalnych interesów państwa oraz tworzenia warunków umożliwiających jego bezpieczny i stabilny rozwój. Przez dziesięciolecia kojarzono je przede wszystkim z bezpieczeństwem militarnym, integralnością terytorialną, niezależnością polityczną oraz rozwojem gospodarczym. W XXI wieku do tego katalogu należy dopisać również zdolność państwa do funkcjonowania w środowisku cyfrowym.

Technologie przestały być wyłącznie narzędziem wspierającym gospodarkę. Stały się elementem bezpieczeństwa narodowego, źródłem przewagi strategicznej oraz jednym z głównych obszarów rywalizacji geopolitycznej. Wojna w Ukrainie, rywalizacja technologiczna pomiędzy Stanami Zjednoczonymi a Chinami czy rosnąca rola globalnych korporacji technologicznych pokazują, że zdolność do rozwijania, wykorzystywania i ochrony technologii wpływa dziś bezpośrednio na pozycję państwa w systemie międzynarodowym.

W tym kontekście suwerenność technologiczna nie oznacza dążenia do pełnej samowystarczalności. Oznacza zdolność do świadomego zarządzania zależnościami oraz utrzymania kontroli nad obszarami mającymi strategiczne znaczenie dla bezpieczeństwa państwa. Chodzi przede wszystkim o kompetencje, wiedzę i zdolność do podejmowania decyzji w świecie, w którym coraz więcej procesów społecznych, gospodarczych i politycznych opiera się na technologiach cyfrowych.

Z perspektywy Polski pytanie o suwerenność technologiczną nie jest pytaniem o budowę własnego odpowiednika Google'a, Microsoftu czy OpenAI. Jest pytaniem o zdolność państwa do ochrony własnych interesów, zapewnienia bezpieczeństwa obywatelom oraz ograniczania ryzyk wynikających z nadmiernych zależności technologicznych. Oznacza to konieczność rozwijania kompetencji w obszarach mających znaczenie strategiczne, wzmacniania odporności infrastruktury krytycznej oraz budowania współpracy pomiędzy administracją publiczną, nauką i biznesem.

Polska, podobnie jak większość państw europejskich, funkcjonuje dziś w ekosystemie technologii tworzonych głównie przez globalne korporacje. Dotyczy to zarówno usług chmurowych, platform komunikacyjnych, jak i narzędzi wykorzystywanych przez administrację publiczną oraz sektor prywatny. W takich warunkach suwerenność technologiczna nie oznacza rezygnacji z tych rozwiązań, lecz zdolność do świadomego zarządzania zależnościami, które z nich wynikają.

Największym zagrożeniem nie jest brak własnego odpowiednika Google'a czy OpenAI. Znacznie większym ryzykiem jest sytuacja, w której państwo korzysta z technologii, których nie rozumie i których konsekwencji nie potrafi ocenić.

O sile państw XXI wieku decydują już nie tylko terytorium, zasoby naturalne i potencjał militarny. Coraz większe znaczenie mają zdolność tworzenia, wykorzystywania i ochrony technologii strategicznych. Z tego względu suwerenność technologiczna powinna być traktowana jako jeden z istotnych elementów polskiej racji stanu oraz jeden z warunków zachowania podmiotowości państwa w świecie rosnącej rywalizacji technologicznej.

Zakończenie

Technologie stały się jednym z najważniejszych czynników kształtujących bezpieczeństwo, rozwój gospodarczy oraz pozycję państw we współczesnym świecie. Rywalizacja o dane, sztuczną inteligencję, infrastrukturę cyfrową czy technologie krytyczne pokazuje, że przewaga technologiczna coraz częściej przekłada się na przewagę polityczną, gospodarczą i militarną.

Przeprowadzona analiza prowadzi do wniosku, że suwerenność technologiczna nie jest już wyłącznie zagadnieniem związanym z innowacyjnością czy polityką gospodarczą. Staje się elementem bezpieczeństwa państwa oraz warunkiem zachowania zdolności do samodzielnego podejmowania decyzji w świecie rosnących zależności technologicznych.

Dla Polski kluczowe znaczenie ma nie dążenie do statusu globalnego mocarstwa technologicznego, lecz rozwijanie kompetencji w obszarach mających strategiczne znaczenie dla bezpieczeństwa i odporności państwa. Pytanie nie brzmi bowiem, czy Polska będzie uczestniczyć w globalnym wyścigu technologicznym. Ten wyścig już trwa. Istotne jest natomiast to, czy będzie posiadała kompetencje pozwalające aktywnie kształtować własną przyszłość, czy też stanie się wyłącznie odbiorcą technologii rozwijanych przez innych.

W XXI wieku zdolność do rozwijania, rozumienia i ochrony technologii staje się jednym z warunków zachowania podmiotowości państwa. Dlatego suwerenność technologiczna powinna być postrzegana nie jako chwilowy trend polityczny, lecz jako trwały element polskiej racji stanu. Polska nie stoi dziś przed prostym wyborem pomiędzy statusem cyberpotęgi a rolą cyfrowych peryferii. Stoi przed znacznie bardziej praktycznym wyzwaniem: budowaniem kompetencji pozwalających zachować podmiotowość w świecie, w którym technologie stają się jednym z głównych źródeł siły państw.

Literatura

Czubkowska S., *Bóg techy. Jak wielkie firmy technologiczne przejmują władzę nad Polską i Światem*, Kraków 2025.

Farrell H, Newman A., *Underground Empire. How America Weaponized the World Economy*, New York 2023.

Harari Y.N., *Homo Deus. Krótka historia jutra,* Wydawnictwo Literackie, 2018.

Kissinger H., Schmidt E., Huttenlocher D., *The Age of AI: And Our Human Future*, Little, Brown and Company, 2021.

Miller C., *Wielka wojna o chipy. Jak USA i Chiny walczą o technologiczną dominację nad światem,* Warszawa 2023.

Perlroth N., *This Is How They Tell Me the World Ends. The Cyberweapons Arms Race*, Bloomsbury Publishing, 2021.

Artykuły i opracowania naukowe:

Pohle J., Thiel T., *Digital Sovereignty*, *Internet Policy Review*, vol. 9, no. 4, 2020.

Dokumenty i raporty:

European Commission, *Shaping Europe's Digital Future*, Communication from the Commission, Brussels–Luxembourg 2020.

Dr Watling J., Danylyuk O. V, Reynolds N., Royal United Services Institute (RUSI), *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War*, London 2023

Źródła Internetowe:

Amazon Web Services, *Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future*, 2022, https:/www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to--preserve-its-present-and-build-its-future

Palczewski S., *Francja wyrzuca Zooma i Teamsa z administracji. Rząd podjął decyzję*, CyberDefence24, 27.01.2026, https:/cyberdefence24.pl/polityka-i-prawo/francja-wyrzuca-zooma-i-teamsa-z-administracji-rzad-podjal-decyzje

Satariano A., Reinhard S., Metz C., Frenkel S., Khurana M., *Elon Musk's Unmatched Power in the Stars,* The New York Times, 28.07.2023

Viasat, *KA-SAT Network Cyber Attack Overview*, KA-SAT Network cyber attack overview | Viasat

Czy regulacja AI może być przewagą konkurencyjną? Modele regulacji AI a pozycja Europy i Polski w globalnej rywalizacji technologicznej

dr Karolina Grenda

ABSTRAKT:

Artykuł analizuje relację między modelem regulacji AI a pozycją konkurencyjną Europy i Polski. Autorka porównuje europejski model prewencyjny (AI Act) z podejściami USA, Chin, Wielkiej Brytanii, Włoch i Tajwanu. Stawia pytanie, czy regulacja AI może stać się przewagą konkurencyjną i analizuje polskie uregulowania implementujące AI Act. Autorka identyfikuje asymetrię regulacyjną jako asymetrię czasu, będącego zasobem krytycznym w wyścigu AI i podnosi problem shadow AI. Artykuł formułuje też pięć rekomendacji strategicznych, w tym stworzenie ścieżki dla dual-use AI oraz wykorzystanie pozycji filaru wschodniej flanki NATO w obszarze militarnych zastosowań AI.

Słowa kluczowe: regulacja AI, AI Act, sztuczna inteligencja, konkurencyjność, modele regulacyjne, piaskownica regulacyjna, suwerenność technologiczna

Wstęp

W edycji 2024 Global Innovation Index (GII) Polska zajmuje 40. miejsce wśród 133 badanych państw, ustępując większości krajów regionu, w tym Bułgarii, Litwie, Węgrom,

Słowenii, Czechom i Estonii[1]. Jednocześnie Polska dysponuje dziś największym centrum technologicznym w Europie Środkowo-Wschodniej, z ponad 650 tysiącami specjalistów IT[2], wydaje miliardy złotych na transformację cyfrową, osiągnęła wysoki poziom cyfryzacji usług publicznych i finansowych, a także zbudowała jedne z najlepszych na świecie Wojsk Obrony Cyberprzestrzeni. Mimo to, nasz kraj pozostaje w gronie państw definiowanych przede wszystkim przez potencjał, a nie przez osiągnięcia. Pytanie o ambitną strategię dla Polski, które wybrzmiewa w tytułach paneli dyskusyjnych Kongresu SET, w ramach którego powstał niniejszy artykuł, jest więc niezwykle słuszne, zwłaszcza w kontekście dynamicznego rozwoju przełomowych technologii, ze sztuczną inteligencją na czele.

AI w ciągu kilku ostatnich lat przestała być wyłącznie domeną inżynierów i laboratoriów badawczych, stając się technologią strategiczną, horyzontalną, elementem rywalizacji między mocarstwami, narzędziem przewagi gospodarczej i zasobem, który w ciągu najbliższych dekad może decydować o pozycji państw i przedsiębiorstw w globalnej hierarchii. W trwającej debacie o możliwościach i wyzwaniach związanych z AI, jako prawnik szczególną wagę przykładam do kwestii regulacyjnych. Decyzja o modelu regulacji to bowiem kwestia fundamentalna, która będzie rozstrzygać o konkurencyjności firm, państw, a nawet całych regionów.

Obserwując globalny krajobraz regulacyjny AI, trudno oprzeć się wrażeniu głębokiej asymetrii. Europa wybrała model ochrony praw i zarządzania ryzykiem – rozbudowany, kosztowny i wymagający. Azja, szczególnie Korea Południowa, Tajwan i Japonia, model strategicznego wsparcia innowacji, w którym regulacja jest instrumentem polityki przemysłowej, a nie mechanizmem kontroli. Stany Zjednoczone wprost deklarują chęć globalnej dominacji, hołdując podejściu skoncentrowanemu na konkurencyjności i deregulacji. Chiny przyjęły model rozproszony i sektorowy, gdzie jednocześnie AI musi służyć wartościom państwowym, a regulator sprawuje ścisłą kontrolę nad treściami. Skutek tej asymetrii jest natomiast dość prosty – europejski startup AI mierzy się z kosztami compliance, których jego azjatycki czy amerykański konkurent nie ponosi w ogóle.

[1] World Intellectual Property Organization, Global Innovation Index 2024, https://www.wipo.int/global_innovation_index/en/2024, dostęp 7.06.2026 r.

[2] Alcor, Software Development in Poland in 2025, https://alcor.com/software-development-in-poland-facts-and-new-reality/, dostęp 7.06.2026 r.

Polska jest w szczególnym położeniu. Jako państwo członkowskie UE podlega bezpośrednio przepisom europejskiego Aktu w sprawie sztucznej inteligencji[3] (dalej: AI Act) i nie ma możliwości wyboru innego modelu regulacyjnego. Jednocześnie, jako państwo będące w istocie zwornikiem wschodniej flanki NATO, bezpośrednio doświadczające konsekwencji rosyjskiej agresji na Ukrainę, Polska stoi przed wyzwaniami daleko wykraczającymi poza compliance, obserwując w czasie rzeczywistym lekcje płynące z rozwijających się militarnych zastosowań AI, a także postępującego wkraczania na pole walki innych przełomowych technologii.

Z tej szerszej perspektywy, uwzględniającej zarówno wymiar ściśle technologiczny, związany z kreowaniem nowych rozwiązań, jak też gospodarcze znaczenie innowacji, a także implikacje militarne, warto spoglądać na systemy regulacyjne, które mogą zarówno inspirować innowatorów do działania, jak też czynić z nich zakładników przepisów.

1. Europejski model regulacji AI: ochrona praw czy hamulec innowacji

Unijny AI Act, przyjęty 13 czerwca 2024 r. i stopniowo wchodzący w życie, jest pierwszym na świecie kompleksowym aktem prawnym regulującym sztuczną inteligencję na poziomie ponadnarodowym. Jego architektura opiera się na modelu *risk-based*, tzn. poziom wymagań regulacyjnych zależy od poziomu ryzyka, jakie niesie dany system AI. Rozporządzenie wyróżnia cztery kategorie: systemy o niedopuszczalnym ryzyku (zakaz stosowania)[4], systemy wysokiego ryzyka (rygorystyczne obowiązki ex ante)[5], systemy ograniczonego ryzyka (obowiązki informacyjne) oraz systemy minimalnego ryzyka (brak szczególnych wymagań).

Model nadzorczy AI Act jest modelem prewencyjnym, co oznacza, że zanim system AI trafi na rynek lub zostanie wdrożony u użytkownika, musi przejść ocenę zgodności,

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

[4] art. 5 – katalog praktyk zakazanych w zakresie sztucznej inteligencji

[5] art. 6-7 oraz Załącznik III – klasyfikacja systemów wysokiego ryzyka

uzyskać dokumentację techniczną, spełnić wymogi dotyczące danych treningowych, zapewnić mechanizmy nadzoru człowieka, a w wielu przypadkach zostać zarejestrowany w europejskiej bazie danych. Ciężar dowodu spoczywa na dostawcy, który musi wykazać, że jego system jest bezpieczny i zgodny z wymaganiami, zanim zostanie on dopuszczony do obrotu.

Z perspektywy innowacyjnych firm, zwłaszcza małych i średnich przedsiębiorstw, obciążenia wynikające z AI Act są znaczące. Spełnienie szeregu formalnych wymagań generuje koszty prawne, techniczne i organizacyjne. Dla korporacji zatrudniającej setki prawników i specjalistów ds. compliance jest to operacyjny koszt prowadzenia działalności. Dla startupu rozwijającego innowacyjne rozwiązanie AI może być barierą nie do pokonania. O wysokich kosztach zgodności regulacyjnej lubią jednak mówić także giganci branży, Raport Information Technology and Innovation Foundation z maja 2026 r. wskazuje, że „Firma Meta poświęciła 590 000 godzin pracy inżynierów na dostosowanie się do unijnego Digital Markets Act – co odpowiada 355 pełnoetatowym inżynierom, którzy przez cały rok zajmowali się dokumentacją zgodności zamiast pracą nad produktem. Nie tworzyli oni przełomowych modeli ani nie wzmacniali systemów bezpieczeństwa sztucznej inteligencji. Wypełniali dokumenty dla zagranicznego organu regulacyjnego".[6] Dalej ten sam raport wskazuje, że „firmy amerykańskie zapłaciły 83% wszystkich kar z tytułu RODO, mimo że stanowią zaledwie 10% importu usług informatycznych i telekomunikacyjnych do UE. Tylko w 2024 r. UE uzyskała 6,7 mld dolarów od amerykańskich firm technologicznych, co stanowi kwotę równą prawie 20% całkowitych dochodów UE z ceł"[7]. Amerykański raport, przygotowany przez organizację wprost wskazującą, iż jednym z jej celów jest obrona amerykańskiego przywództwa technologicznego, stwierdza dalej z tej właśnie perspektywy wprost, że „podczas gdy wiodące zachodnie firmy zajmujące się sztuczną inteligencją kierują talenty inżynieryjne i kapitał na zapewnienie zgodności z przepisami, chińscy konkurenci wspierani przez państwo działają bez porównywalnych obciążeń w kraju i dokonują agresywnej ekspansji na rynkach, na których firmy amerykańskie borykają się z najcięższymi ograniczeniami regulacyjnymi".[8]

---

[6] Raport Information Technology and Innovation Foundation, Foreign Regulations Are Undermining Western AI Competitiveness and Benefiting China, https://itif.org/publications/2026/05/08/foreign-regulations-undermining-competitiveness-benefiting-china/, dostęp 7.06.2026 r.

[7] Ibidem

[8] Ibidem

To oczywiście głos w trwającej globalnie debacie, dobrze obrazujący coraz silniejsze napięcia związane właśnie z modelami regulacji. Podkreślić przy tym należy, że głos nie pierwszy i z pewnością nie ostatni. Warto przywołać bowiem choćby szeroko komentowany, opublikowany we wrześniu 2024 r. raport „Przyszłość europejskiej konkurencyjności" (The Future of European Competitiveness) autorstwa byłego szefa Europejskiego Banku Centralnego Mario Draghiego, w którym na kilkuset stronach wskazywał on na utratę konkurencyjności Europy względem USA i Chin. Wskazywał m.in., iż „Problem nie polega na tym, że Europie brakuje pomysłów czy ambicji. Mamy wielu utalentowanych naukowców i przedsiębiorców, którzy zgłaszają patenty. Jednak innowacje utykają na kolejnym etapie: nie udaje nam się przełożyć ich na komercjalizację, a innowacyjne firmy, które chcą się rozwijać w Europie, napotykają na każdym kroku przeszkody w postaci niespójnych i restrykcyjnych przepisów. W rezultacie wielu europejskich przedsiębiorców woli szukać finansowania u amerykańskich inwestorów venture capital i rozwijać działalność na rynku amerykańskim. W latach 2008-2021 blisko 30% „jednorożców" – założonych w Europie start-upów, których wartość przekroczyła 1 mld USD – przeniosło swoje siedziby za granicę, przy czym zdecydowana większość z nich przeniosła się do Stanów Zjednoczonych".[9]

Świadoma tych problemów, Komisja Europejska zaproponowała w maju 2026 roku pakiet upraszczający regulacje cyfrowe, tzw. AI Omnibus[10]. Porozumienie polityczne zakłada szereg uproszczeń, a kierunek można uznać za właściwy, ale pojawia się pytanie, czy działania naprawcze nie przyszły za późno i nie mają zbyt wycinkowego charakteru, szczególnie w kontekście coraz szybciej rosnącej luki technologicznej między Europą a USA i Azją.

Fundamentalny dylemat europejskiego modelu regulacyjnego AI można sformułować następująco – czy AI Act stanie się globalnym standardem, podobnie jak system ochrony danych osobowych GDPR, wymuszając de facto jego przestrzeganie przez firmy działające na rynku europejskim i tym samym podnosząc globalny poziom ochrony? Czy raczej stanie się „regulacyjnym hamulcem" – instrumentem chroniącym co prawda prawa obywateli, ale jednocześnie utrwalającym peryferyjną

[9] The future of European competitiveness. Part A | A competitiveness strategy for Europe, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf, dostęp 7.06.2026 r., s.6

[10] EU agrees to simplify AI rules to boost innovation and ban 'nudification' apps to protect citizens, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1024, dostęp 7.06.2026 r.

pozycję europejskich firm w globalnym wyścigu AI? Odpowiedź na to pytanie zależy w dużej mierze od tego, czy Europa i poszczególne państwa członkowskie uzupełnią ramy regulacyjne o aktywną politykę przemysłową, która wyrówna szanse krajowych innowatorów.

Nie można przy tym lekceważyć faktu, iż wymagania AI Act wchodzą w życie stopniowo, a zwłaszcza w kontekście wyżej wspomnianego pakietu Omnibus – wiele obowiązków staje się wiążących dopiero w 2027 i 2028 r. W tym czasie globalna rywalizacja toczy się w pełnym tempie. Giganci technologiczni z USA i Chin inwestują miliardy dolarów w modele fundamentalne, czyli zasoby, którymi żadna europejska firma nie dysponuje w porównywalnej skali. Każda godzina, którą europejski startup AI poświęca na dokumentację techniczną zamiast na rozwijanie modelu, to godzina, której konkurent z San Francisco lub Hangzhou nie musi tracić. Asymetria regulacyjna jest zatem jednocześnie asymetrią czasu, a czas w sektorze AI jest zasobem absolutnie krytycznym.

2. Polski projekt ustawy o systemach sztucznej inteligencji – model nadzorczy

W dniu 31 marca 2026 r. Rada Ministrów przyjęła projekt ustawy o systemach sztucznej inteligencji, który 9 kwietnia 2026 r. wpłynął do Sejmu i jest procedowany jako Druk Sejmowy nr 2443. Projekt wyznacza krajową architekturę wdrażania wymagań AI Act. Jego przyjęcie będzie istotne także dlatego, iż Polska jest jednym z nielicznych państw UE, które nie wyznaczyły jeszcze krajowego organu nadzoru AI, tworząc stan regulacyjnej niepewności dla podmiotów stosujących systemy wysokiego ryzyka.[11]

Projekt ustawy opiera się na trzech głównych filarach. Pierwszym jest powołanie Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI) jako organu właściwego w rozumieniu AI Act. Projekt przewiduje wyposażenie Komisji w szerokie kompetencje: przeprowadzanie kontroli, prowadzenie postępowań administracyjnych, wydawanie nakazów i zakazów, nakładanie kar pieniężnych.

Wyróżniającym elementem projektu jest przy tym mechanizm łagodzenia kar inspirowany prawem konkurencji – tzw. leniency. Podmioty, które dobrowolnie zgłoszą

[11] Grenda K., From Regulation to Readiness: Operational Gaps in AI Governance under the EU AI Act, NIS2 and GDPR, European Cybersecurity Journal, vol. 11(1), 2026, s.26

naruszenie przepisów i aktywnie współpracują z organem, mogą liczyć na redukcję kary nawet o 70%, a w przypadku pełnej współpracy – o 90%. To rozwiązanie, które należy ocenić pozytywnie.

Kolejną ciekawą propozycją są wiążące opinie indywidualne. Za opłatą w wysokości zaledwie 150 zł podmiot może uzyskać wiążącą ocenę KRiBSI dotyczącą zgodności projektowanego systemu AI z wymaganiami, zanim system zostanie wdrożony. Rozwiązanie to może mieć ogromne znaczenie dla MŚP i startupów, które w fazie projektowej często nie dysponują środkami na zewnętrzne audyty compliance.

Trzecim elementem wyróżniającym projekt są bezpłatne piaskownice regulacyjne dla MŚP. Środowisko testowe, w którym firmy mogą sprawdzać swoje rozwiązania AI bez pełnego reżimu compliance, jest instytucją przewidzianą przez AI Act, ale decyzja o bezpłatnym dostępie dla małych podmiotów jest już krajowym wyborem.

Jednocześnie projekt ustawy zawiera istotne luki, które mogą ograniczyć jego praktyczne znaczenie. Przykładem może być brak sektorowych regulacji AI dla kluczowych sektorów, takich jak administracja publiczna, wymiar sprawiedliwości, czy ochrona zdrowia. Projekt świadomie pozostawia te obszary do odrębnych, przyszłych inicjatyw legislacyjnych. Problem z tym podejściem polega na tym, że jedną z głównych barier wdrażania AI w polskim sektorze publicznym jest właśnie brak precyzyjnych ram prawnych. Raport NASK „AI w e-administracji publicznej" wskazuje, że 73% urzędników identyfikuje niejasność regulacji lub ich brak jako główną przeszkodę we wdrażaniu AI.[12]

3. Model włoski jako alternatywa wewnątrzunijna

W lipcu 2025 roku Włochy przyjęły ustawę nr 132/2025 (Legge 132/2025)[13], obowiązującą w pełnym zakresie od kwietnia 2026 r. Jest to jeden z pierwszych kompleksowych krajowych aktów prawnych regulujących AI w Europie i wyraźnie odmienny od podejścia polskiego. O ile Polska postawiła na budowę architektury nadzorczej z obietnicą regulacji sektorowych w przyszłości, Włochy przyjęły model, w którym jeden akt prawny łączy nadzór z konkretnymi standardami operacyjnymi dla kluczowych sektorów.

[12] NASK, AI w e-administracji publicznej – perspektywa urzędników i instytucji, s. 8, https:/www.nask.pl/media/2026/03/AI-w-administracji-publicznej_.pdf, dostęp 7.06.2026 r.

[13] Legge 8 luglio 2025, n. 132 (Włochy) – ustawa o sztucznej inteligencji, https:/www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2025-09-23;132, dostęp 7.06.2026 r.

Szczególnie istotny jest art. 14 dotyczący administracji publicznej. Ustawodawca włoski nie poprzestaje na ogólnym dopuszczeniu AI w urzędach, lecz precyzuje zarówno cel (zwiększenie efektywności, skrócenie procedur, poprawa jakości usług), jak i warunki (przejrzystość, identyfikowalność, nadzór człowieka). Przepis jednoznacznie przesądza, że AI może mieć wyłącznie charakter instrumentalny i wspierający, a pełna odpowiedzialność za decyzje pozostaje po stronie człowieka.

W obszarze wymiaru sprawiedliwości art. 15 włoskiej ustawy jest równie precyzyjny – wszelkie decyzje dotyczące interpretacji prawa, oceny faktów i dowodów oraz rozstrzygnięć pozostają wyłącznie w gestii sędziego. AI może być używana jedynie pomocniczo, w obszarze organizacji pracy sądów i czynności administracyjnych. Testowanie systemów AI w sądownictwie wymaga zgody Ministerstwa Sprawiedliwości.

Na rynku pracy (art. 11) ustawa formułuje katalog zasad o charakterze zarówno ochronnym, jak i organizacyjnym. AI ma służyć poprawie warunków pracy i produktywności, ale musi działać w sposób przejrzysty, niedyskryminujący i nienaruszający godności pracownika. Pracodawca ma obowiązek informowania pracowników o stosowanych systemach AI. Uzupełnieniem jest art. 12 powołujący Obserwatorium ds. wdrażania AI na rynku pracy.

Zestawienie podejść polskiego i włoskiego prowadzi do wniosku, że oba kraje odpowiadają na to samo wyzwanie odmiennie. Polska buduje przede wszystkim architekturę nadzoru i egzekwowania prawa, zakładając, że szczegółowe regulacje sektorowe pojawią się później. Włochy równolegle definiują zasady stosowania AI w kluczowych obszarach, ograniczając niepewność regulacyjną na poziomie operacyjnym. Oba podejścia są w pełni zgodne z AI Act, różnią się jednak zakresem ambicji krajowego ustawodawcy.

Pytanie, które należy postawić, brzmi – czy polskie odesłanie do przyszłych inicjatyw legislacyjnych w obszarze sektorowym to ostrożność i pragmatyzm, czy też zwłoka, która utrwala lukę między prawem a wdrożeniami? Biorąc pod uwagę zjawisko *shadow AI* i jego implikacje dla bezpieczeństwa organizacji, o czym szerzej w dalszej części tekstu, to wątpliwość o ogromnym znaczeniu.

4. Globalne modele regulacji AI: prymat innowacji

Analizując podejście regulacyjne różnych jurysdykcji do sztucznej inteligencji, trudno oprzeć się wrażeniu, że Europa i reszta świata patrzą na tę samą technologię

przez zupełnie różne soczewki. Dla Europy AI jest przede wszystkim technologią niosącą ryzyko – dla praw podstawowych, bezpieczeństwa, demokracji. Dla Korei, Tajwanu i Japonii AI jest przede wszystkim szansą – na wzrost, na konkurencyjność, na wzmocnienie pozycji państwa. USA stawiają na globalną dominację i eliminowanie barier, które mogłyby temu celowi stać na przeszkodzie. Chiny traktują AI także jako narzędzie wzmacniania kontroli państwa i „socjalistycznych wartości podstawowych". Różnice perspektyw przekładają się na fundamentalnie odmienne architektury regulacyjne.

4.1. Korea Południowa – model rozwojowy z elementami obowiązków

Koreańska ustawa „Framework Act on the Development of Artificial Intelligence and Establishment of a Foundation for Trust" (AI Basic Act), uchwalona 21 stycznia 2025 r. i obowiązująca od 22 stycznia 2026 r.[14], stanowi jeden z pierwszych kompleksowych aktów regulujących AI na świecie i zarazem jeden z najlepszych przykładów modelu rozwojowego w tym obszarze. Punkt wyjścia koreańskiej regulacji jest wyraźnie różny od europejskiego – nie klasyfikacja ryzyka, lecz strategiczne znaczenie AI dla rozwoju gospodarczego i budowanie zaufania do technologii.

W zakresie obowiązków regulacyjnych ustawa wyróżnia kategorię *high-impact AI*, czyli systemów mogących istotnie oddziaływać na życie, bezpieczeństwo fizyczne lub prawa podstawowe człowieka. Dla systemów z tej kategorii ustawa wprowadza obowiązek oznaczania treści generowanych przez AI (art. 31) oraz zarządzania ryzykiem (art. 34). Kluczowa różnica wobec modelu europejskiego to jednak brak katalogu zakazów.

Tym, co wyróżnia koreańską ustawę na tle innych regulacji, jest rozbudowany komponent aktywnego wsparcia rozwoju AI przez państwo. Ustawa wprost zobowiązuje rząd do: wspierania badań i komercjalizacji (art. 13), rozwoju standardów (art. 14), promowania tworzenia i dystrybucji danych szkoleniowych (art. 15), wsparcia MŚP (art. 17), promocji startupów AI (art. 18), wsparcia klastrów technologicznych (art. 21) oraz ułatwień w tworzeniu centrów danych AI (art. 25). Prawo funkcjonuje tu jako instrument polityki przemysłowej, nie tylko jako system kontroli.

[14] Framework Act on the Development of Artificial Intelligence and Establishment of a Foundation for Trust (AI Basic Act), https://aibasicact.kr/explorer/, dostęp 7.06.2026 r.

4.2. Tajwan – prymat innowacji

Tajwańska Artificial Intelligence Basic Act, uchwalona 23 grudnia 2025 r. i obowiązująca od 14 stycznia 2026 r.[15], jest aktem wyjątkowo lapidarnym – liczy zaledwie 20 artykułów, ale niezwykle wyrazistym w swoich priorytetach. Podstawowe znaczenie dla zrozumienia stojącej za nią idei jest programowy art. 1, który wprost wskazuje AI jako technologię kluczową dla rozwoju kraju i jego międzynarodowej konkurencyjności. Prawo ma być instrumentem budowania przewagi, nie tylko zarządzania ryzykiem.

Kluczowy jest również art. 11 tajwańskiej ustawy, wyrażający zasadę *Innovation First*. Przepis stanowi, że jeżeli interpretacja przepisów AI koliduje z innymi ustawami, pierwszeństwo ma zasada promowania nowych technologii. Warunkiem jest zgodność z fundamentalnymi zasadami z art. 4, który wyznacza zasady, jakimi rząd ma kierować się przy promowaniu AI i które stanowią nieprzekraczalne ramy dla wszelkich kolejnych regulacji sektorowych dotyczących systemów AI: zrównoważony rozwój i dobrobyt, autonomia człowieka, ochrona prywatności i zarządzanie danymi, cyberbezpieczeństwo, przejrzystość i wyjaśnialność, sprawiedliwość i niedyskryminacja, rozliczalność. Jest to rozwiązanie bez precedensu w europejskim systemie regulacyjnym – ustawodawca wprost nakazuje interpretatorom prawa preferować wykładnię wspierającą innowację.

Tajwan, jako gospodarka głęboko zakorzeniona w globalnym łańcuchu wartości technologicznych, traktuje ustawę o AI jako instrument polityki narodowej, nie jako akt prawny regulujący zachowanie podmiotów prywatnych.

4.3. Japonia – promocja bez sankcji

Japoński Act on Promotion of Research and Development, and Utilization of AI-Related Technology, uchwalony 28 maja 2025 r. i obowiązujący od 1 września 2025 r.[16], wyróżnia się spośród wszystkich omawianych aktów tym, że już jego tytuł wyraża filozofię regulacyjną. Nie ma tu mowy o regulacji, jest promocja, nie ma zakazów,

[15] Artificial Intelligence Basic Act, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=H0160093, dostęp 7.06.2026 r.

[16] Act on Promotion of Research and Development, and Utilization of AI-Related Technology, https://www.kojimalaw.jp/wp/wp-content/uploads/2025/09/Japan-AI-Promotion-Act-KOJIMA-LAW-OFFICES-jp-en-reference-translation.pdf, dostęp 7.06.2026 r.

klasyfikacji ryzyka ani sankcji finansowych, ale jest za to kompleksowy program wsparcia dla podmiotów rozwijających i stosujących AI.

Adekwatnie dla tak wyznaczonego kierunku, art. 1 wprost określa AI jako fundament rozwoju społeczno-gospodarczego i podstawę dobrobytu, zaś art. 3 wyznacza główne kierunki, w ramach których Japonia ma wspierać rozwój i wykorzystanie AI, jako technologii wzmacniającej wydajność, innowacyjność i bezpieczeństwo narodowe. Kraj chce działać kompleksowo, przejrzyście i bezpiecznie, zapobiegając nadużyciom oraz aktywnie współpracować międzynarodowo – celem jest globalne przywództwo. Zgodnie z art. 7 Podmioty stosujące AI mają dążyć do efektywności operacyjnej i tworzenia nowych gałęzi przemysłu, a zarazem wpisywać się w politykę rządu. Na szczeblu krajowym, stosownie do art. 18-19 ustaw, powstaje *AI Strategic Headquarters* z Premierem na czele, w skład którego wchodzą wszyscy ministrowie. Budżet na AI w roku 2026 wynosi 502,7 mld jenów (ok. 3,5 mld USD), z czego aż 90% przeznaczono na wzmocnienie zdolności AI.

4.4. Stany Zjednoczone – model konkurencyjności i dominacji

20 marca 2026 r. Biały Dom opublikował dokument *National Policy Framework for Artificial Intelligence: Legislative Recommendations*[17], skierowany do Kongresu USA. Dokument ten nie jest ustawą, lecz zestawem rekomendacji legislacyjnych, który wyraźnie sygnalizuje kierunek polityki AI administracji Prezydenta Donalda Trumpa. Jego filozofia jest diametralnie różna od podejścia europejskiego, zamiast klasyfikacji ryzyka, ex-ante compliance i ocen skutków, priorytetem jest innowacyjność, dominacja technologiczna USA i eliminowanie barier regulacyjnych.

Framework identyfikuje siedem obszarów priorytetowych dla legislacji AI: (1) Ochrona dzieci i wzmocnienie roli rodziców, (2) Ochrona i wzmacnianie amerykańskich społeczności, (3) Poszanowanie własności intelektualnej i wspieranie twórców, (4) Zapobieganie cenzurze i ochrona wolności słowa, (5) Wspieranie innowacji i zapewnienie dominacji USA w dziedzinie AI, (6) Edukacja Amerykanów i budowa siły roboczej gotowej do pracy z AI, (7) Ustanowienie federalnych ram polityki AI i ograniczenie nadmiernie rozproszonych regulacji stanowych.

Szczególnie akcentowany jest obszar infrastruktury obliczeniowej i energetyki. Framework zakłada generację energii bezpośrednio przy centrach obliczeniowych oraz

[17] The White House, National Policy Framework for Artificial Intelligence: Legislative Recommendations, https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf, dostęp 8.06.2026 r.

eliminację barier regulacyjnych dla inwestycji w infrastrukturę AI. Innymi słowy USA chcą zdecydowanie dążyć do rozbudowy wielkoskalowej infrastruktury obliczeniowej.

Kontrast z Europą jest uderzający. Żadnej klasyfikacji ryzyka AI, żadnego wymogu ex-ante oceny zgodności, żadnego obowiązku rejestracji. Priorytet jest jeden: „wygrać wyścig AI". Podejście to rodzi pytania o ochronę obywateli i prawa podstawowe, ale jednocześnie tworzy ekosystem, w którym innowacja jest wspierana, a nie hamowana biurokratycznymi procedurami.

Szczególnie istotny z perspektywy polskiej jest element energetyczny, w którym administracja Donalda Trumpa wprost wiąże dominację AI z dominacją energetyczną – centra danych mają mieć zapewniony dostęp do energii on-site, procedury zezwoleń mają być radykalnie skrócone, a sieci energetyczne rozbudowane priorytetowo. To podejście jest diametralnie różne od europejskiego, gdzie rozbudowa sieci energetycznej podlega wieloletnim procedurom środowiskowym i administracyjnym. Efektem jest nie tylko różnica regulacyjna, ale różnica infrastrukturalna, fundamentalna dla AI, która jest technologią niezwykle energochłonną.

5. Porównanie modeli i ich główne implikacje dla konkurencyjności

Krótkie zarysowanie kilku charakterystycznych modeli regulacyjnych pozwala na sformułowanie wniosków dotyczących relacji między otoczeniem prawnym a innowacyjnością.

Pierwsza i najważniejsza obserwacja wynikająca z porównania modeli to głęboka asymetria regulacyjna. Firma europejska rozwijająca system AI wysokiego ryzyka musi przejść ocenę zgodności, sporządzić dokumentację techniczną, wdrożyć system zarządzania ryzykiem, zapewnić nadzór człowieka i zarejestrować się w europejskiej bazie danych, a wszystko to zanim produkt trafi na rynek. Jej amerykański lub odpowiednik mierzy się z ułamkiem tych wymagań. Ta asymetria jest asymetrią kosztów, czasu i zasobów, bezpośrednio przekładającą się na zdolność do szybkiego skalowania i zdobywania rynku.

Koszty compliance stają się dla europejskich przedsiębiorców barierą wejścia na rynek. Globalne korporacje dysponują zasobami pozwalającymi na ponoszenie kosztów regulacyjnych, lecz startup rozwijający np. innowacyjne narzędzie AI dla sektora opieki zdrowotnej, nie ma zasobów na zewnętrzne audyty prawne, certyfikację systemów zarządzania i dokumentację techniczną spełniającą wszystkie

wymogi AI Act. W praktyce oznacza to, że europejskie startupy AI albo unikają zastosowań wysokiego ryzyka (tracąc rynki), albo naruszają przepisy (ponosząc ryzyko sankcyjne), albo przenoszą działalność poza UE (tracąc ekosystem unijny).

Warto jeszcze generalnie zauważyć, że model chiński, którego nie omawiam w tym krótkim tekście szczegółowo, pokazuje z kolei, że regulacja AI może służyć celom jeszcze diametralnie innym – nie ochronie praw obywateli, lecz wzmocnieniu kontroli państwa nad treściami cyfrowymi. Model amerykański demonstruje, że można zdecydować się na niemal całkowity brak regulacji na poziomie federalnym, z naciskiem na konkurencyjność. Obie te opcje są dla Unii Europejskiej nieakceptowalne z przyczyn aksjologicznych i politycznych, ale stanowią ważny punkt odniesienia przy ocenie europejskiej pozycji konkurencyjnej.

Interesującym paradoksem jest fakt, że zarówno USA, jak i Chiny, stosując diametralnie różne modele regulacyjne, osiągają ten sam efekt – szybkość wdrożeń. USA dzięki deregulacji i priorytetowi dla innowacji, Chiny dzięki centralizacji decyzji i eliminacji biurokratycznych przeszkód dla podmiotów zbliżonych do państwa. Europa, ze swoim rozproszonym, wielopoziomowym modelem regulacyjnym, płaci za to cenę w postaci wolniejszego tempa zmian.

Hipoteza Brukseli, że AI Act stanie się globalnym standardem, tak jak GDPR, ma istotne ograniczenia. GDPR rzeczywiście stało się punktem odniesienia dla wielu krajowych regulacji dotyczących ochrony danych, jednak AI jest technologią znacznie bardziej heterogeniczną i AI Act może nie stać się globalnym standardem w tak samo bezpośredni sposób. Systemy dominujące na globalnym rynku AI nie są europejskie. Ich twórcy dostosują się do wymogów AI Act w zakresie niezbędnym do działania w UE, ale europejski model regulacyjny nie stanie się przez to globalnym standardem.

Istnieje wreszcie ryzyko przenoszenia firm i talentów tam, gdzie regulacja jest łagodniejsza. Ryzyko to jest tym większe, im wyższe są bariery regulacyjne i im mniejsze wsparcie dla innowatorów w jurysdykcji bazowej. Polska, jako kraj aspirujący do roli centrum technologicznego, ale pozbawiony dotąd aktywnej technologicznej polityki przemysłowej, jest szczególnie narażona na ten scenariusz.

6. Rekomendacje strategiczne

Pytanie nie brzmi dziś – regulować AI czy nie? AI Act obowiązuje bezpośrednio we wszystkich państwach UE i nie ma możliwości jego uniknięcia. Pytanie brzmi

inaczej – jak zbudować polską politykę przemysłową AI, która wyrówna szanse polskich firm w globalnej rywalizacji, pomimo regulacyjnych obciążeń wynikających z prawa unijnego? Poniżej przedstawiam pięć obszarów rekomendacji, uwzględniających nowe wyzwania zidentyfikowane w niniejszej analizie.

6.1. Infrastruktura obliczeniowa i energetyczna – luka strukturalna Europy

Wielkoskalowe inwestycje w infrastrukturę AI (centra danych, moc obliczeniowa) koncentrują się w USA i Azji. W 2025 r. McKinsey szacował, że „do 2030 roku przedsiębiorstwa zainwestują na całym świecie prawie 7 bilionów dolarów w infrastrukturę centrów danych. Ponad 4 biliony dolarów z tej kwoty zostanie przeznaczone na hardware, a pozostała część na takie obszary, jak nieruchomości i infrastruktura energetyczna. Ponad 40% tych wydatków zostanie zainwestowanych w Stanach Zjednoczonych".[18] Analitycy wskazują również, że „Globalne zapotrzebowanie na moc obliczeniową centrów danych może wzrosnąć trzykrotnie do 2030 roku. Około 70% tego wzrostu będzie wynikało z obciążeń związanych ze sztuczną inteligencją. Goldman Sachs przewiduje, że zużycie energii w centrach danych wzrośnie o 165% w latach 2023–2030".[19] Europa, choć posiada ponad 1000 centrów danych w EU27+UK o łącznym obciążeniu 9,4 GW (2024) i planuje 2,5-krotne zwiększenie do 2030[20], mierzy się z problemem dostępności taniej, stabilnej i skalowalnej energii. To bariera strukturalna, która czyni europejski wyścig infrastrukturalny z USA i Azją niemal niemożliwym do wygrania. Podczas gdy USA deklarują budowę nowej infrastruktury obliczeniowej w tempie wyrażonym w miesiącach, Europa mierzy te procesy w dekadach. Europejska polityka klimatyczna dramatycznie utrudnia więc globalną cyfrową konkurencję. Polityka energetyczna i technologiczna są ze sobą nierozerwanie splecione, więc realny udział w wyścigu technologicznym, wymaga

[18] McKinsey & Company, The data-center balance: How US states can navigate the opportunities and challenges, https://www.mckinsey.com/industries/public-sector/our-insights/the-data-center-balance-how-us-states-can-navigate-the-opportunities-and-challenges, dostęp 9.06.2026 r.

[19] Avid Solutions Inc., 13 Data Center Growth Projections That Will Shape 2026–2030, https://avidsolutionsinc.com/13-data-center-growth-projections-that-will-shape-2026-2030/, dostęp 9.06.2026 r.

[20] Eurelectric, AI and Energy, https://www.eurelectric.org/in-detail/ai-and-energy/, dostęp 9.06.2026 r.

w Polsce i Europie w pierwszej kolejności rozwiązania problemów związanych ze źródłami energii. Jak pokazują nawet ostatnie wydarzenia na Bliskim Wchodzie, centra przetwarzania danych to kluczowa infrastruktura krytyczna współczesnego świata[21], trudno więc mówić o udziale w cyfrowej rewolucji, bez zapewnienia stosownej infrastruktury.

6.2. Prymat inteligentnej adopcji AI zamiast shadow AI

Nawet jednak wobec obiektywnych trudności na polu infrastrukturalnym, możliwe jest osiąganie sukcesów przy odpowiednim ustaleniu priorytetów. Można bowiem skoncentrować się na polu, w którym pozycja lidera zależy w dużej mierze od kreatywności, sprawności organizacyjnej i regulacyjnego otoczenia, a więc – inteligentnej, zaufanej i bezpiecznej implementacji AI w kluczowych sektorach.

Pierwszym i zasadniczym wyzwaniem jest tu uporządkowane wdrażanie AI, zamiast udawania, że jeszcze jej w organizacji nie ma. To drugie podejście oznacza brak świadomości zjawiska *shadow AI*, czyli niekontrolowanego używania narzędzi AI poza oficjalnymi procedurami organizacyjnymi.

Dane empiryczne wskazują jednoznacznie, że adopcja AI już się wydarzyła, najczęściej nieformalnie. Przywoływane już badanie NASK na szerokiej próbie polskich urzędów potwierdza, że 46% urzędników korzysta z generatywnej AI w pracy zawodowej. Urzędnicy wykorzystują AI bardzo praktycznie, przede wszystkim do: wyszukiwanie faktów i informacji – 59% oraz tworzenie i redagowanie dokumentów – 46%[22]. Badanie Fundacji SET i firmy LOGIT wykazało natomiast, że 85% polskich prawników znajduje się w orbicie AI – korzysta z tej technologii, wdraża ją lub planuje wdrożenie w ciągu najbliższych 12 miesięcy. Jednocześnie 53,6% z nich korzysta z rozwiązań otwartych i darmowych, które nie gwarantują spełnienia deklarowanych standardów bezpieczeństwa, zaś 36,3% nie zna żadnych zaawansowanych systemów AI dedykowanych prawnikom[23].

Shadow AI jest więc systemowym zagrożeniem. Urzędnicy, prawnicy i pracownicy innych branż, działający w dobrej wierze, używają publicznie dostępnych narzędzi

[21] Jadczak Adam, Iran celowo atakuje centra danych amerykańskich BigTech'ów, https://itwiz.pl/iran-celowo-atakuje-centra-danych-amerykanskich-bigtechow/, dostęp 9.06.2026 r.

[22] NASK, AI w e-administracji publicznej..., op.cit., s. 8

[23] Czy AI zastąpi prawników? – prezentacja raportu Fundacji SET, https://set.org.pl/czy-ai-zastapi-prawnikow-prezentacja-raportu-fundacji-set/, dostęp 9.06.2026 r.

bez świadomości ryzyk związanych z wyciekiem danych poufnych, halucynacjami modeli językowych, naruszeniami RODO. W kontekście równoczesnego obowiązywania GDPR, NIS2 i AI Act każdy taki incydent może uruchomić kaskadę obowiązków notyfikacyjnych wobec wielu organów jednocześnie.

Rozwiązaniem nie jest ani zakaz używania AI, ani udawanie, że tej technologii nie ma, to nieskuteczne i kontrproduktywne. Rozwiązaniem jest stworzenie klarownych ram, które *shadow AI* zastąpią modelami zaufanej adopcji. W bezpiecznej, uporządkowanej i kreatywnej implementacji AI możemy być liderem, to z pewnością jest w naszym zasięgu.

6.3. *Dual-use* AI i reżim regulacyjny

Jednym ze strategicznie istotnych problemów europejskiej regulacji AI jest kwestia systemów *dual-use*, czyli technologii rozwijanych jednocześnie z myślą o zastosowaniach cywilnych, jak i wojskowych. AI Act wyłącza spod swojego zakresu zastosowania systemy AI, które wprowadzono do obrotu, oddano do użytku lub są one wykorzystywane, wyłącznie do celów wojskowych, obronnych lub do celów bezpieczeństwa narodowego (art. 2 ust 3 AI Act). Jednak firmy rozwijające produkty AI na rynku cywilnym, które chciałyby równolegle rozwijać zastosowania militarne, napotykają istotną barierę. Systemy AI wysokiego ryzyka na rynku cywilnym wymagają bowiem pełnej dokumentacji technicznej, oceny zgodności i rejestracji w europejskiej bazie danych. Są to procedury kosztowne, czasochłonne i transparentne – informacje o systemie trafiają do publicznej bazy danych. Firma, która chce równolegle rozwijać zastosowanie militarne, musi spełniać wymogi dla wersji cywilnej, co jest trudne do pogodzenia z wymogami wojskowej tajności lub innymi ograniczeniami obowiązującymi w sektorze obronnym. Efektem jest strukturalne utrudnienie tworzenia i implementacji technologii *dual-use*, czyli tradycyjnie silnego akceleratora innowacji.

Polska jako zwornik wschodniej flanki NATO, doświadczający bezpośrednio konsekwencji rosyjskiej agresji na Ukrainę, powinna szczególnie mocno artykułować potrzebę stworzenia regulacyjnej ścieżki ułatwiającej *dual-use* AI. Niezbędne jest też zaangażowanie się Sił Zbrojnych RP oraz innych podmiotów systemu bezpieczeństwa narodowego w aktywne poszukiwanie i inspirowanie polskich innowacyjnych przedsiębiorców do profilowania na wczesnym etapie obiecujących z perspektywy bezpieczeństwa projektów, w kierunku celów wojskowych, obronnych i bezpieczeństwa narodowego, co umożliwi skorzystanie z wyłączenia z AI Act.

6.4. Wsparcie startupów AI – certyfikacja, sandbox i zaufanie

Brak krajowego programu wsparcia certyfikacji jest jedną z najbardziej dotkliwych luk w polskiej polityce AI. Jak już pisałam, trzy kluczowe standardy, czyli ISO/IEC 27001:2022 (zarządzanie bezpieczeństwem informacji), ISO/IEC 27701:2019 (zarządzanie prywatnością) oraz ISO/IEC 42001:2023 (zarządzanie AI), pokrywają łącznie ok. 80% wymagań wynikających z unijnych norm AI Act, GDPR i NIS2[24]. To zatem rozpoznawalna i ustandaryzowana ścieżka do osiągniecia potwierdzonej międzynarodowo zgodności regulacyjnej, zwiększającej bezpieczeństwo zarówno przedsiębiorcy, jak też jego klientów. Jednak koszt implementacji i certyfikacji tych trzech standardów dla małej firmy technologicznej lub startupu może wynosić dziesiątki tysięcy euro, a więc stanowić kwotę zaporową dla większości innowatorów.

Polska potrzebuje programu certyfikacyjnego obejmującego:

- dotacje certyfikacyjne dla startupów i MŚP rozwijających systemy AI wysokiego ryzyka,
- uproszczoną ścieżkę certyfikacji etapowej (pre-assessment przed pełnym audytem),
- integrację trzech reżimów (AI Act + GDPR + NIS2) w jeden zintegrowany system zarządzania zamiast trzech odrębnych procesów certyfikacyjnych;
- bezpłatne konsultacje pre-assessment.

Piaskownice regulacyjne przewidziane w rządowym projekcie ustawy są krokiem we właściwym kierunku, ale ich uruchomienie jest spóźnione. W tym czasie polskie startupy AI znalazły się w gorszej pozycji konkurencyjnej niż ich odpowiednicy z krajów, gdzie takie rozwiązania działają już od lat. Każdy miesiąc opóźnienia oznacza, że innowatorzy nie mają bezpiecznego środowiska do testowania rozwiązań, co spycha ich ku jurysdykcjom z bardziej przyjaznymi ramami regulacyjnymi.

W obszarze sektora publicznego kluczowe jest natomiast stworzenie standaryzowanej listy kontrolnej oceny narzędzi AI, która pozwoliłaby urzędnikom na świadome i bezpieczne wdrażanie AI bez konieczności angażowania zewnętrznych ekspertów prawnych przy każdym zakupie. Uzupełnieniem powinna być matryca kompetencji nadzorczych, czyli precyzyjne przypisanie, kto odpowiada za jakie naruszenia i jakie

[24] Grenda K., From Regulation to Readiness: Operational Gaps..., op.cit., s.27

obowiązki notyfikacyjne obowiązują przy nakładaniu się reżimów GDPR/ NIS2 / AI Act. Chaos notyfikacyjny przy incydentach naruszających jednocześnie te trzy regulacje jest dziś jednym z głównych źródeł niepewności prawnej.

6.5. Polska w NATO – militarne zastosowania AI

Na koniec kwestia strategicznego pozycjonowania Polski w globalnym ekosystemie AI. Polska ma unikalne, niemożliwe do skopiowania aktywa strategiczne i jako filar wschodniej flanki NATO, z bezpośrednim dostępem do informacji i doświadczeń z zastosowań AI w konflikcie zbrojnym toczącym się za wschodnią granicą, może i powinna odgrywać kluczową rolę w obszarze militarnych zastosowań AI i bezpieczeństwa technologicznego w Sojuszu. To nie jest ambicja przerastająca nasze możliwości, ale obowiązek wynikający z pozycji geopolitycznej, zasobów intelektualnych i ambicji rozwojowych. To wątek, który będzie przedmiotem odrębnej analizy.

Zakończenie: Ambitna Polska w erze sztucznej inteligencji

Odpowiedź na pytanie czy zmierzamy w kierunku osiągniecia pozycji w gronie państw – liderów technologicznych, czy też cyfrowych peryferii nie leży oczywiście w treści przepisów, lecz uwzględniając polskie zasoby – raczej w woli politycznej i instytucjonalnej zdolności do ich wdrożenia.

Regulacja AI jest jednak wyborem strategicznym, nie tylko prawnym. Europa wybrała model ochrony praw i zarządzania ryzykiem, model z wielu perspektyw wartościowy, ale generujący koszty, które europejskie firmy muszą ponosić w globalnej rywalizacji. Azja wybrała model strategicznego wsparcia innowacji, zaś deklarowanym wprost celem USA, znajdującym odzwierciedlenie w działania regulacyjnych, jest globalna dominacja technologiczna. Polska, jak każde państwo UE, nie ma swobody wyboru między tymi modelami w zakresie regulacji unijnej. Ma jednak swobodę decyzji o tym, jak uzupełnić AI Act o własną politykę przemysłową, infrastrukturalną i bezpieczeństwa.

Polska ma przy tym istotne zasoby – inżynierów, matematyków, infrastrukturę akademicką i rosnące inwestycje w sektor technologiczny. Brakuje spójnej strategii, która połączy regulację z polityką przemysłową, compliance z innowacją, a ambicje z adekwatnym pozycjonowaniem Polski w globalnym ekosystemie AI.

Polska ambitna w dolinie cieni

Piotr Guział

Abstrakt:

Artykuł łączy perspektywę praktyczną przedsiębiorcy-twórcy platformy AI z refleksją strategiczną o warunkach budowania polskiej i europejskiej suwerenności cyfrowej. Autor odwołuje się do koncepcji Cyfrowego Okręgu Przemysłowego jako adaptacji idei Centralnego Okręgu Przemysłowego i proponuje postulaty: koalicyjny model językowy (LLM), krajową infrastrukturę obliczeniową, wartości jako fundament architektury cyfrowej. Inspirując się europejskimi sukcesami kooperacji (Airbus, Eurofighter), formułuje wizję cyfrowej Doliny Krzemowej.

Słowa kluczowe: Cyfrowy Okręg Przemysłowy, suwerenność cyfrowa, LLM, AI, infrastruktura obliczeniowa, koalicja europejska, startup, innowacje

Dolina Krzemowa to dziś synonim technologicznej potęgi, innowacji i globalnej dominacji. Ale jej historia zaczęła się skromnie, od garażu, od uczelni, od kilku naukowców, którzy postanowili zamienić wiedzę w produkt i wkrótce udało im się opracować dużo lepsze niż dotychczasowe tranzystory krzemowe i stworzyć pierwszy komercyjny układ scalony. Z tego ziarna wyrosły Intel, AMD, Nvidia i cały ekosystem, który zmienił świat.

W rozumieniu geografii ekonomicznej Dolina Krzemowa to okręg przemysłowy oparty na silnej sieci powiązań między przedsiębiorstwami i inwestorami, najbardziej rozpoznawalny na świecie symbol zaawansowanej technologicznie działalności gospodarczej oraz ścisłych związków między sferą nauki i produkcji. Za sukcesem Doliny Krzemowej stoi koncentracja w jednym miejscu nowoczesnych przedsiębiorstw, najlepszych uczelni oraz wielkich funduszy inwestycyjnych. To jest właśnie model, o którym powinniśmy myśleć, gdy mówimy o cyfrowym okręgu przemysłowym. Nie o jednej firmie, nie o jednej uczelni, a nawet nie o jednym państwie, lecz o ekosystemie, który łączy naukę, kapitał i przemysł w jedną, spójną całość, zdolną konkurować na globalnym rynku.

W tym kontekście jednym z najważniejszych pytań naszych czasów jest: czy Europa zbuduje swój cyfrowy okręg przemysłowy, czy też, nieświadomie, podryfuje

w przestrzeń, którą można nazwać Doliną Cieni? Przestrzeń, w której cyfrowe narzędzia istnieją, lecz nie służą wspólnocie, w której dane krążą, lecz nie wiadomo gdzie, w której sztuczna inteligencja pracuje, lecz nikt nie wie, dla kogo i na czyją korzyść.

To nie jest pytanie retoryczne. To pytanie o strategię kontynentu, o bezpieczeństwo instytucji, o przyszłość europejskiej administracji, europejskiego prawa i europejskiej gospodarki. I, co chcę podkreślić od samego początku, to pytanie, na które nie ma odpowiedzi w skali pojedynczego państwa narodowego. Nawet tak dużego jak Polska.

I. Okręg przemysłowy jako idea

Pojęcie okręgu przemysłowego ma w Polsce szczególny ciężar historyczny. Centralny Okręg Przemysłowy, budowany w latach 1936-1939 z inicjatywy wicepremiera Eugeniusza Kwiatkowskiego, był projektem nie tylko ekonomicznym, lecz przede wszystkim strategicznym. Chodziło o stworzenie rdzenia przemysłowego w widłach Wisły i Sanu, z dala od granic, trudnego do zniszczenia w przypadku agresji. Chodziło o suwerenność. O zdolność do samodzielnego działania w obliczu zagrożenia.

Dziś, gdy mówimy o cyfrowym okręgu przemysłowym, powinniśmy myśleć podobnymi kategoriami, ale ze świadomością, że skala wyzwania radykalnie przekracza możliwości jednego państwa. Infrastruktura cyfrowa jest infrastrukturą krytyczną. Modele językowe, serwery, systemy przetwarzania danych, to zasoby strategiczne nie mniej ważne niż stal czy węgiel w czasach Kwiatkowskiego. A pytanie o to, gdzie te zasoby są zlokalizowane, kto je kontroluje i na jakich zasadach, jest pytaniem o suwerenność w najgłębszym sensie tego słowa.

Ale tu pojawia się pierwsza, fundamentalna trudność. Wyścig o dominację technologiczną nad światem już się rozpoczął. I jest to wyścig, w którym stawką jest nie tylko przewaga gospodarcza, lecz zdolność do kształtowania rzeczywistości: informacyjnej, prawnej, militarnej. Dwie potęgi, Stany Zjednoczone i Chiny, zainwestowały w ten wyścig zasoby, których żadne europejskie państwo, nawet najsilniejsze gospodarczo, nie jest w stanie samodzielnie zrównoważyć.

II. Błąd, który łatwo popełnić

W debacie o cyfrowej suwerenności bardzo łatwo wpaść w pułapkę myślenia narodowego. Logika jest pozornie prosta: nasze dane powinny być na naszych serwerach,

nasze modele AI powinny być trenowane przez nasze instytucje, nasza infrastruktura powinna być pod kontrolą naszego państwa. Brzmi rozsądnie. Brzmi patriotycznie. Jest jednak, w obecnych realiach geopolitycznych, intelektualnie nieuczciwe.

Żadne europejskie państwo nie jest w stanie samodzielnie wygrać wyścigu technologicznego ze Stanami Zjednoczonymi ani z Chinami. To nie jest pesymizm. To jest trzeźwa ocena proporcji. Polska podjęła próbę stworzenia własnego modelu językowego. PLLuM, czyli Polish Large Language Universal Model, to rodzina dużych polskich modeli językowych, umożliwiających generowanie tekstu oraz przetwarzanie języka naturalnego. To osiągnięcie godne uznania i dobrze, że powstało. Ale trzeba powiedzieć wprost: twórcy projektu nie stworzyli od zera nowego modelu LLM, który byłby alternatywą dla zagranicznych. Budżet projektu nie był na to wystarczający. W efekcie badacze w ramach projektu PLLuM postanowili zaadaptować istniejące modele do języka polskiego, tak aby lepiej mówiły po polsku, lepiej orientowały się w polskich realiach i lepiej odpowiadały na potrzeby polskich użytkowników. Innymi słowy: polska wersja modelu językowego to w istocie nakładka na modele stworzone przez amerykańską Metę i francuski Mistral, a nie samodzielna budowla od fundamentów.

To nie jest zarzut pod adresem polskich naukowców, czy polityków. To jest opis strukturalnego ograniczenia, które dotyczy każdego europejskiego państwa z osobna. Porównanie jest tu brutalne, ale uczciwe: to tak jakby zestawiać niegdysiejszą produkcję Fabryki Samochodów Osobowych na warszawskim Żeraniu z zakładami General Motors. Oba przedsięwzięcia to produkcja samochodów, ale skala, złożoność, jakość, osiągi i liczba modeli są nieporównywalne. Nie dlatego, że polscy inżynierowie byli gorsi od amerykańskich. Dlatego, że skala zainwestowanego kapitału i infrastruktury była nieporównywalna. Dokładnie ta sama logika obowiązuje w wyścigu o prymat w świecie przetwarzania danych i sztucznej inteligencji.

Polska jest tu przykładem szczególnie wymownym, i to niezależnie od tego, kto aktualnie sprawuje władzę. Uzależnienie polskiej administracji publicznej od oprogramowania dostarczanego przez globalnych gigantów jest faktem strukturalnym, nie politycznym. Twórcy analizy Fundacji Instrat przebadali 71 zamówień z okresu 11 miesięcy, udostępnionych w Biuletynie Zamówień Publicznych. Raport wskazał, że aż 99 procent przypadków wykluczało rozwiązania polskich producentów, a wymagania przedstawione w zamówieniach brały pod uwagę jedynie oferty, które miały unikalne cechy produktów i aplikacji Microsoftu. Taka dominacja oznacza nie tylko możliwość dyktowania warunków cenowych, ale w przypadku awarii lub jednostronnej decyzji biznesowej po stronie dostawcy, może dojść do paraliżu działalności całych instytucji państwowych.

Co więcej, dane wskazują, że usługi chmurowe upowszechniają się również w administracji publicznej: ponad 70 procent ankietowanych jednostek korzysta z usług chmurowych, a najważniejszym kryterium wyboru dostawcy są już istniejące umowy licencyjne, według wskazań ponad połowy korzystających z chmury. Innymi słowy: polska administracja wybiera dostawcę nie dlatego, że jest najlepszy pod względem bezpieczeństwa czy suwerenności danych, lecz dlatego, że już wcześniej wybrała tego samego dostawcę. To jest definicja uzależnienia.

Tymczasem inne kraje europejskie wyciągają wnioski. Francja zapowiedziała rezygnację z Windowsa na rzecz Linuxa w administracji centralnej. Niemcy w landzie Szlezwik-Holsztyn przeniosły na Linuxa 30 tysięcy stacji roboczych, oszczędzając na samych licencjach 15 milionów euro. Polska w tym zestawieniu jest nieobecna. I nie jest to kwestia jednej opcji politycznej, jednego rządu czy jednej kadencji. To jest systemowy, wieloletni dryf w stronę zależności, który trwa niezależnie od tego, kto zasiada przy sterach.

III. Garażowy startup w cyfrowej Polsce

Piszę o tym z perspektywy praktycznej, nie akademickiej. LOGiT FLOW, platforma AI dla profesjonalistów, którą buduję od podstaw, jest małym polskim dowodem na to, że suwerenność cyfrowa zaczyna się właśnie tak: od decyzji, by nie czekać na gotowe rozwiązanie z zewnątrz, lecz zbudować własne. Ale ta sama droga, przebyta od środka, pozwala mi z pełną odpowiedzialnością powiedzieć, co w Polsce działa, co działa gorzej, a czego nie ma w wystarczającej skali.

Co działa dobrze: Polska ma wybitnych programistów i inżynierów. Kompetencje techniczne polskich specjalistów są na poziomie światowym, a koszty operacyjne wciąż pozostają konkurencyjne w porównaniu z Europą Zachodnią. Rynek rośnie, świadomość cyfrowa przedsiębiorstw i instytucji zwiększa się z roku na rok. Polskie startupy AI przyciągnęły w ostatnich latach setki milionów euro finansowania, plasując Polskę na czele regionu Europy Środkowej i Wschodniej pod względem inwestycji w tę branżę. W Polsce powstają dziś narzędzia, które z powodzeniem konkurują z zachodnimi odpowiednikami pod względem jakości i bezpieczeństwa.

Co działa gorzej: budowanie zaufania wśród klientów instytucjonalnych, w szczególności w sektorze publicznym, to proces wielokrotnie dłuższy i bardziej kosztowny niż w przypadku podmiotów zagranicznych, które wchodzą na rynek z gotową marką.

Zetknąłem się osobiście z sytuacją, w której instytucja samorządowa zadała nam blisko sto szczegółowych pytań dotyczących bezpieczeństwa danych i ochrony informacji, podczas gdy tych samych pytań nie zadała Microsoftowi ani Google, bo tamte, jak usłyszałem, "są już uznane". Inna instytucja chwaliła się, że u nich już działa sztuczna inteligencja, ale z nami mają problem, bo jesteśmy startupem. Nie problem z jakością, funkcjonalnością, ceną, tylko z faktem, że nie jesteśmy powszechnie znani. Zatem nie chodzi o brak zrozumienia technologii. Chodziło o coś innego: o to, że nieznana marka krajowego dostawcy jest domyślnie traktowana jako ryzyko, którego nie warto podejmować, podczas gdy znana marka zagranicznego giganta jest domyślnie traktowana jako bezpieczna. Ten mechanizm niszczy każdy krajowy startup w zalążku.

Czego nie ma w wystarczającej skali: mechanizmy wsparcia w Polsce istnieją. PARP, NCBR, PFR Ventures dysponują programami dla startupów i firm innowacyjnych. Nowe instrumenty, takie jak STEP z alokacją sięgającą ponad 900 milionów euro na technologie cyfrowe i deep-tech, wskazują, że kierunek jest właściwy. Polska planuje też powołanie Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, w ramach której mają powstać bezpłatne piaskownice regulacyjne dla małych i średnich firm testujących systemy AI. Problem jednak nie leży w braku przepisów, lecz w strukturze i skali tego wsparcia. Polskie programy są w ogromnym stopniu uzależnione od środków unijnych, a nie od krajowego, prywatnego kapitału ryzyka. Kiedy jeden program się kończy, a kolejny nie wystartował, cały rynek zwalnia. Pomoc de minimis, najpowszechniejszy instrument publiczny, nie może przekroczyć 300 tysięcy euro na firmę w ciągu trzech lat. To jest kwota absolutnie niewystarczająca do zbudowania infrastruktury AI zdolnej konkurować z podmiotami dysponującymi setkami milionów dolarów prywatnego kapitału. Brakuje też systemowych preferencji dla krajowych dostawców technologii w zamówieniach publicznych, podobnych do tych, które stosują Stany Zjednoczone wobec własnych firm w ramach polityki Buy American. I brakuje przede wszystkim praktycznej kultury instytucjonalnej, która zamiast pytać "ale to jest startup, czy to jest bezpieczne?", pytałaby: "czy ten podmiot spełnia wymagania, które postawiłbym każdemu innemu dostawcy?".

IV. Europa potrafi: lekcja z Airbusa, Eurofightera, Sap i Spotify

Zanim jednak popadniemy w pesymizm, warto przypomnieć sobie, że Europa już stawała przed podobnymi wyzwaniami i wygrywała. Nie dlatego, że jedno państwo

okazało się wystarczająco silne. I, co równie ważne, nie dlatego, że powierzono projekt unijnej biurokracji. Dlatego, że kilka suwerennych państw zdecydowało się dobrowolnie połączyć swoje potencjały wokół konkretnego celu.

To rozróżnienie jest fundamentalne i warto je wypowiedzieć wprost. Gdyby projekt Airbusa miał przejść przez standardowe procedury unijne, z komisjami, dyrektywami, sporami o to, w którym kraju ma być wytwarzany każdy podzespół, z debatami o parytetach zatrudnienia i łańcuchach ekologicznych, projekt nigdy by nie powstał. Albo powstałby z wieloletnim opóźnieniem, w ułamku pierwotnych parametrów i kilkukrotnie wyższym budżecie. Airbus nie jest sukcesem Unii Europejskiej jako instytucji. Jest sukcesem Francji, Niemiec, Wielkiej Brytanii i Hiszpanii, które postanowiły działać razem, zachowując własne interesy, własne kompetencje i własne decyzje, ale w ramach wspólnej architektury projektu. Historia przyznała im rację: Airbus kontroluje dziś ponad 60 procent globalnego rynku lotnictwa komercyjnego, wyprzedzając Boeinga. Projekt, który zaczynał jako polityczna ambicja kilku rządów, stał się globalnym liderem branży.

Eurofighter potwierdza tę samą logikę. Niemcy, Wielka Brytania, Włochy i Hiszpania stworzyły największy program międzynarodowej współpracy obronnej w Europie. Ponad 600 zamówionych samolotów, praca 100 tys. ludzi. Nie powołano do tego celu żadnej unijnej agencji z rozbudowanym mandatem i własnym budżetem administracyjnym. Powołano konsorcjum suwerennych państw z jasno podzielonymi rolami i jasno zdefiniowanym celem.

W obszarze technologii cywilnej europejskie sukcesy globalnego formatu można policzyć na palcach jednej ręki. SAP: założony przez siedmiu inżynierów w Niemczech w 1972 roku, dziś trzeci co do wielkości producent oprogramowania na świecie i największa spółka technologiczna w Europie pod względem kapitalizacji rynkowej. Spotify: szwedzki startup, który zdominował globalny rynek streamingu i zmusił Apple oraz Amazon do defensywnej odpowiedzi. Bolt: estoński startup, który zbudował platformę mobilności działającą w kilkudziesięciu krajach i stał się jednym z symboli bałtyckiego ekosystemu technologicznego. To są europejskie sukcesy na miarę światową. I właśnie dlatego, że można je wymienić jednym tchem, bez potrzeby sięgania po drugą rękę, widać wyraźnie, że są wyjątkami, a nie systemową regułą.

Co więcej, nawet te wyjątki wymagają pewnej uczciwości w ocenie. SAP jest dziś potęgą, ale w obszarze infrastruktury AI nie jest w stanie samodzielnie zrównoważyć inwestycji OpenAI, Google czy Microsoftu, które operują budżetami rzędu dziesiątek miliardów dolarów rocznie. Spotify odniosło sukces na rynku treści, ale jego

infrastruktura obliczeniowa opiera się na chmurze Google. Bolt zbudował doskonały produkt, lecz w rywalizacji z Uberem, który ma dostęp do amerykańskiego kapitału w skali nieporównywalnej z europejskim rynkiem venture capital, walczy z ciągłą asymetrią zasobów. Innymi słowy: Europa potrafi tworzyć wyjątkowych założycieli i wyjątkowe produkty. Ale nie zbudowała jeszcze ekosystemu, który produkuje takie firmy seryjnie, tak jak robi to Dolina Krzemowa. I zapewne nie zbuduje go przez powołanie kolejnej unijnej agencji z siedzibą w Brukseli. Zbuduje go wtedy, gdy suwerenne państwa zdecydują się połączyć swoje zasoby i swoje rynki wokół konkretnych celów, tak jak zrobiły to przy Airbusie i przy Eurofighterze: bez oddawania suwerenności, z zachowaniem własnych interesów i z jasno podzielonymi rolami.

V. Stan obecny: uczciwa diagnoza

Zanim przejdziemy do wizji przyszłości, należy uczciwie opisać stan obecny. I ta uczciwość wymaga przyznania rzeczy, o której w debacie publicznej mówi się zbyt rzadko.

Dziś europejska infrastruktura AI po prostu nie istnieje w skali, która pozwalałaby na rezygnację z narzędzi dostarczanych przez podmioty spoza Unii Europejskiej. Europejczycy, którzy chcą korzystać z dobrodziejstw nowoczesnych technologii, w tym z zaawansowanych modeli językowych, systemów analizy dokumentów czy narzędzi automatyzacji pracy, są w praktyce zmuszeni korzystać z rozwiązań, których infrastruktura zlokalizowana jest poza europejskim obszarem gospodarczym, przede wszystkim w Stanach Zjednoczonych. Na globalnym rynku chmury obliczeniowej Amazon Web Services kontroluje blisko 38 procent rynku, Microsoft Azure około 24 procent, a Google Cloud około 9 procent. Łącznie trzy amerykańskie podmioty kontrolują ponad 70 procent globalnej infrastruktury chmurowej, na której opiera się funkcjonowanie instytucji publicznych i prywatnych na całym świecie, w tym w Europie.

Czy jest to zgodne z prawem? Na dziś, tak. Europejskie RODO dopuszcza możliwość przetwarzania danych poza Europejskim Obszarem Gospodarczym w kilku ściśle określonych przypadkach. Pierwszym z nich jest obowiązywanie decyzji Komisji Europejskiej o adekwatności ochrony danych w danym państwie trzecim. Takie decyzje obowiązują między innymi w odniesieniu do Stanów Zjednoczonych w ramach mechanizmu EU-US Data Privacy Framework, a także wobec Japonii, Kanady, Singapuru czy Wielkiej Brytanii. Drugim mechanizmem są standardowe klauzule umowne, czyli SCC, które mogą być inkorporowane do warunków użytkowania danej

usługi, zapewniając formalną zgodność z wymogami RODO nawet przy transferze danych poza EOG.

Innymi słowy: korzystanie z amerykańskich narzędzi AI, przy odpowiednio skonstruowanych warunkach użytkowania, jest dziś prawnie dopuszczalne. Co więcej, wiodący dostawcy rozwiązań oferują dla klientów instytucjonalnych taki wybór warunków, które nie dopuszczają trenowania modeli na danych użytkownika, gwarantują bezpieczne przechowywanie danych oraz zapewniają tak zwane zero retention, czyli brak przechowywania danych po zakończeniu sesji. Dlatego tak ważne w organizacjach są wdrożenia systemowe, a nie zgoda na indywidualne korzystanie z obszaru shadow AI, które nie daje żadnych gwarancji bezpieczeństwa w zakresie obchodzenia się z danymi.

Ale pytanie nie brzmi: czy jest to zgodne z prawem? Pytanie brzmi: czy jest to model, w którym chcemy funkcjonować na stałe? Czy chcemy, by nasza cyfrowa infrastruktura, nasze dane, nasze modele AI, były zlokalizowane poza naszą kontrolą, w państwach, które mogą jednostronnie zmieniać warunki dostępu, które podlegają własnym regulacjom prawnym, które mogą, w określonych okolicznościach geopolitycznych, ograniczyć lub zablokować dostęp do usług?

Odpowiedź brzmi: nie. Nie dlatego, że Stany Zjednoczone są wrogiem. Nie dlatego, że obecna współpraca transatlantycka jest zła. Ale dlatego, że suwerenność, w tym suwerenność cyfrowa, polega właśnie na tym, by nie być zależnym od dobrej woli innych, nawet sojuszników. Suwerenność to zdolność do samodzielnego działania, gdy okoliczności tego wymagają.

VI. Sztuczna inteligencja: narzędzie czy władca?

Nie można pisać o cyfrowym okręgu przemysłowym bez refleksji nad sztuczną inteligencją. AI stała się słowem-kluczem, zaklęciem, które otwiera drzwi do finansowania, uwagi mediów i politycznej przychylności. Ale za tym słowem kryją się bardzo konkretne pytania, na które polityka publiczna wciąż nie udzieliła wystarczająco precyzyjnych odpowiedzi.

Pierwsze pytanie brzmi: czyja sztuczna inteligencja? Większość narzędzi AI, z których korzystają dziś europejskie instytucje publiczne, pochodzi od podmiotów, których centra decyzyjne i infrastruktura obliczeniowa zlokalizowane są poza Europą. Dane wprowadzane do tych systemów trafiają na serwery, nad którymi europejskie

instytucje nie mają bezpośredniej kontroli. Modele językowe są trenowane na tych danych, chyba że warunki użytkowania wyraźnie to wykluczają. To nie jest zarzut pod adresem konkretnych firm. To jest opis strukturalnej zależności, którą każde poważne państwo musi świadomie zaadresować.

Drugie pytanie brzmi: kto odpowiada za decyzje podejmowane z pomocą AI? To pytanie prawne, etyczne i organizacyjne zarazem. Sztuczna inteligencja jest narzędziem, które potrafi generować przekonująco brzmiące, lecz błędne odpowiedzi. Potrafi cytować nieistniejące przepisy, przywoływać zmyślone orzeczenia, konstruować logicznie spójne, lecz merytorycznie fałszywe argumenty. Zjawisko to, znane jako halucynacje AI, jest szczególnie niebezpieczne w środowiskach, gdzie precyzja ma znaczenie prawne: w administracji publicznej, w wymiarze sprawiedliwości, w sektorze finansowym.

Właśnie dlatego korzystanie bezpośrednio z surowych modeli językowych, bez żadnej warstwy pośredniej, jest szczególnie ryzykowne w zastosowaniach profesjonalnych. Model językowy sam w sobie nie wie, że jest prawnikiem, lekarzem czy urzędnikiem. Odpowiada na pytania w sposób statystycznie prawdopodobny, nie merytorycznie zweryfikowany. Nie ma żadnego sita, przez które przechodzą pytania i odpowiedzi. Stąd rosnący na świecie trend, który warto dostrzec i docenić: zamiast korzystać bezpośrednio z ogólnych modeli językowych, instytucje sięgają po wyspecjalizowane platformy branżowe, prawne, medyczne, administracyjne, które co prawda korzystają z tych samych dużych modeli językowych jako silnika, ale poprzez własne oprogramowanie tworzą precyzyjne sito. Sito, które dostosowuje wyniki do charakteru pracy odbiorcy, eliminuje odpowiedzi spoza zakresu merytorycznego, redukuje ryzyko halucynacji i zapewnia, że AI działa jak doświadczony asystent w konkretnej dziedzinie, a nie jak encyklopedia odpowiadająca na wszystko. To jest dokładnie model, który realizuje LOGiT FLOW: platforma AI dla profesjonalistów, zbudowana tak, by sztuczna inteligencja pracowała precyzyjnie w realiach polskiego prawa, polskiej administracji i polskiego rynku.

Tacy dostawcy wyspecjalizowanych platform powinni spełniać dodatkowe warunki, by zasługiwać na zaufanie instytucji publicznych i prywatnych. Przede wszystkim powinni posiadać certyfikaty bezpieczeństwa, takie jak np. ISO 27001 w zakresie zarządzania bezpieczeństwem informacji oraz ISO 27701 w zakresie ochrony danych osobowych, lub inne równoważne certyfikaty potwierdzające dojrzałość procesów bezpieczeństwa. Powinni regularnie przeprowadzać audyty bezpieczeństwa, w tym testy penetracyjne, które weryfikują odporność systemu na ataki

z zewnątrz. Powinni oferować nie tylko serwis techniczny i określony czas reakcji na zgłoszenia, lecz przede wszystkim kompleksowe wsparcie wdrożeniowe, obejmujące szkolenia nie tylko z obsługi narzędzia, lecz także z budowania kompetencji cyfrowych w organizacji. To ostatnie jest szczególnie ważne w sektorze publicznym: samo wdrożenie narzędzia bez zbudowania kultury jego odpowiedzialnego używania jest jak zakup samochodu bez posiadania prawa jazdy.

Zasada nadrzędna pozostaje jednak niezmieniona: AI jest narzędziem wspierającym człowieka, nie zastępującym go. Odpowiedzialność za decyzje i dokumenty zawsze ponosi człowiek. Technologia może przyspieszać, porządkować, analizować. Ale decydować musi człowiek. Ta zasada powinna stać się fundamentem polityki AI, a zarazem odpowiedzią na pytanie o granice automatyzacji w sferze publicznej.

VII. Droga do cyfrowego okręgu przemysłowego

Co zatem należy zrobić? Pozwolę sobie zaproponować kilka postulatów, które uważam za kluczowe.

Postulat pierwszy: koalicyjny duży model językowy (LLM), jako projekt strategiczny. Polska i jej partnerzy regionalni potrzebują wspólnego dużego modelu językowego, zdolnego realnie konkurować z rozwiązaniami amerykańskimi i chińskimi. Nie jest to projekt, który może zrealizować jedno państwo. Wymaga połączenia kompetencji naukowych, zasobów obliczeniowych i finansowania z obszaru grupy państw gotowych działać wspólnie. Wymaga przełamania narodowych partykularyzmów na rzecz wspólnego celu i odwagi politycznej do długoterminowego myślenia strategicznego. Ale jest wykonalny, o czym świadczy historia Airbusa, Eurofightera i CERN (europejskie centrum badań nad fizyką cząstek elementarnych). Żaden z tych projektów nie czekał na zgodę wszystkich dwudziestu siedmiu państw. Każdy zaczął się od grupy państw z jasną wolą działania.

Postulat drugi: krajowa i koalicyjna infrastruktura obliczeniowa. Serwery, centra danych, infrastruktura obliczeniowa niezbędna do trenowania i uruchamiania zaawansowanych modeli AI, to zasoby strategiczne. Polska potrzebuje własnej infrastruktury tego rodzaju, zlokalizowanej na własnym terytorium, podlegającej własnemu prawu i własnemu nadzorowi. Ale zamykanie się tylko w granicach państwa narodowego do w globalnym świecie ślepa uliczka. Sukces w tym obszarze można osiągnąć tylko poprzez współdziałanie z innymi państwami europejskimi.

Serwerownie mogą być rozproszone, tak jak produkcja Airbusa jest rozproszona między kilka krajów, lecz powinny tworzyć jeden spójny, suwerenny system.

Postulat trzeci: wartości jako fundament architektury cyfrowej. Architektura cyfrowa, którą zbudujemy, powinna odzwierciedlać wartości, które chcemy chronić: ochronę prywatności, przejrzystość, odpowiedzialność, poszanowanie praw podstawowych, zgodę na różnorodność przekonań, a nie odgórnie narzucone wzorce. RODO, AI Act, NIS2, to nie muszą być biurokratyczne przeszkody. To są wyrazy cywilizacyjnej tożsamości w przestrzeni cyfrowej. Infrastruktura, którą budujemy, powinna być z tymi wartościami spójna.

Postulat czwarty: uczciwa ocena stanu przejściowego. Dopóki własna infrastruktura AI nie powstanie w wystarczającej skali, będziemy zmuszeni korzystać z narzędzi dostarczanych przez podmioty zewnętrzne. To jest fakt, który należy przyjąć z otwartymi oczami, a nie wypierać. Zadaniem polityków i urzędników nie jest straszenie i polityka zakazów, lecz, do czasu gdy nie powstanie alternatywna infrastruktura, zapewnienie w oficjalnych kanałach komunikacji, że korzystanie z obecnych narzędzi AI i infrastruktury chmurowej jest dopuszczalne i zgodne z prawem, jeśli odbywa się na warunkach maksymalnie bezpiecznych: z odpowiednimi klauzulami umownymi spełniającymi warunki RODO, z zakazem trenowania modeli na danych instytucji publicznych, z gwarancjami zero retention tam, gdzie jest to możliwe, a dostawcy takich usług potrafią wykazać środki, jakie podjęli, by stać się zaufanym i bezpiecznym partnerem.

Postulat piąty: inwestycja w krajowe kompetencje i krajowych dostawców. Infrastruktura to nie tylko serwery i modele. To przede wszystkim ludzie i firmy. Polska ma wybitnych programistów, inżynierów i specjalistów w dziedzinie AI. Zbyt wielu z nich pracuje dla firm spoza Polski, przyciągniętych wyższymi wynagrodzeniami i lepszą infrastrukturą badawczą. Równocześnie polskie instytucje publiczne systematycznie pomijają krajowych dostawców technologii na rzecz zagranicznych gigantów, nawet wtedy, gdy krajowe rozwiązania oferują nie gorszy poziom bezpieczeństwa, lepsze dostosowanie do polskiego prawa i realną możliwość budowania długoterminowej relacji partnerskiej, a nie wyłącznie relacji licencyjnej z odległą korporacją.

VIII. Czas na decyzję

Znaleźliśmy się w punkcie, w którym decyzje podejmowane dziś będą miały konsekwencje przez następne dekady. Wyścig technologiczny między Stanami

Zjednoczonymi a Chinami już trwa w najlepsze. Polska i Europa nie mogą w nim nie uczestniczyć, bo nieobecność jest też wyborem, i to wyborem o bardzo konkretnych konsekwencjach: technologicznej zależności, utraty konkurencyjności gospodarczej i w perspektywie długoterminowej, ograniczenia zdolności do samodzielnego kształtowania własnej przyszłości.

Ale suwerenność cyfrowa nie jest projektem, który zrealizuje jedno państwo, choćby najsprawniejsze i najbardziej ambitne. Historia pokazuje, że wygrywają koalicje: państw, które łączą kompetencje, kapitał i wolę polityczną wokół wspólnych celów. Może w tym pomóc Unia Europejska, jako instytucja, ale historia już wielokrotnie pokazała, że eurokracja nie jest obecnie najszybszą i najbardziej efektywną formą podejmowania decyzji. Może to być również współpraca regionalna, bilateralna, w formacie Trójmorza, grupy V4, w formacie Trójkąta Weimarskiego czy innych dobrowolnych koalicji państw, które rozumieją, że stawką jest coś więcej niż gospodarcza konkurencyjność. Stawką jest zdolność do decydowania naszej części świata o własnej przyszłości.

Kluczowe jest jedno: żaden z tych formatów nie zadziała, jeśli każde z państw będzie budowało własną, narodową odpowiedź na wyzwanie o kontynentalnej skali, osobno, bez koordynacji, bez wspólnych standardów i bez gotowości do dzielenia się zasobami. To droga do Doliny Cieni: fragmentacji, nieefektywności i pogłębiającej się zależności od dostawców zewnętrznych, wobec których nikt z osobna nie ma wystarczającej siły negocjacyjnej.

Airbus pokazał, że połączone potencjały suwerennych państw europejskich mogą pokonać globalnego lidera, gdy działają jak konsorcjum, a nie jak komitet. SAP pokazał, że europejska firma może stać się największą firmą technologiczną kontynentu i rywalizować z amerykańskimi gigantami na ich własnym podwórku. Eurofighter pokazał, że zaawansowane systemy obronne można budować w koalicji, bez rezygnowania z narodowych interesów i narodowych kompetencji. Historia Doliny Krzemowej pokazuje z kolei, że ekosystem innowacji rodzi się tam, gdzie nauka, kapitał i przemysł spotykają się w jednym miejscu, z jedną wspólną ambicją, bez czekania na zgodę centralnej biurokracji.

Centralny Okręg Przemysłowy lat trzydziestych ubiegłego wieku był projektem odważnym, dalekowzrocznym i strategicznym. Jego twórcy rozumieli, że suwerenność gospodarcza jest warunkiem suwerenności politycznej. Dziś, w erze cyfrowej, ta sama logika obowiązuje, ale w innej skali. Suwerenność cyfrowa jest warunkiem suwerenności w każdym innym wymiarze. I jest to suwerenność, którą możemy osiągnąć tylko wspólnie, w koalicji państw, które rozumieją, co jest stawką.

Dolina Krzemowa czy Dolina Cieni? Kwiatkowski w 1936 roku nie pytał, czy Polska jest gotowa na budowę COP-u. Pytał, co się stanie, jeśli go nie zbuduje. My dziś stoimy przed tym samym pytaniem, tyle że zamiast stali i węgla chodzi o serwery, modele językowe i nasze dane. Zamiast wideł Wisły i Sanu chodzi o przestrzeń cyfrową, która nie ma granic, ale ma właścicieli. I tak jak wtedy odpowiedź zależała od woli kilku ludzi przy stole decyzyjnym, tak i dziś zależy. Historia nie pyta, czy mamy czas. Pyta tylko, czy mamy wizję, odwagę i determinację.

Cyberbezpieczeństwo ma narodowość. Dlaczego Polska potrzebuje własnego cyberpancerza

Jan Kostrzewa

Abstrakt:

Artykuł postuluje wprowadzenia preferowania narodowego "local content" w cywilnych przetargach obejmujących rozwiązania cyberbezpieczeństwa. Autor wskazuje, że narzędzia takie jak EDR, XDR, VPN, DLP, rejestracja sesji zdalnej czy systemy backupu działają w najbardziej wrażliwych obszarach infrastruktury cyfrowej, dlatego zaufanie do ich producentów ma wymiar strategiczny. Tekst omawia przykłady oraz regulacje dotyczące dostawców wysokiego ryzyka, pokazując, że cyberbezpieczeństwo jest nierozerwalnie związane z jurysdykcją, geopolityką i odpornością państwa. W zakończeniu postuluje stworzenie listy polskich rozwiązań cyberbezpieczeństwa "Dostawcy Niskiego Ryzyka", która umożliwi preferowanie w przetargach krajowych dostawców.

Słowa kluczowe: cyberbezpieczeństwo, suwerenność technologiczna, cyberpancerz, dostawca wysokiego ryzyka, local content, dostawca niskiego ryzyka

Polska potrafi tworzyć produkty cyfrowe klasy światowej. Branża gier komputerowych jest tego najlepszym przykładem: według raportu PARP 97% gier tworzonych w Polsce trafia na rynki globalne, a Polska należy do czołowych producentów gier w Europie. Ze wszystkim miast całej Unii Europejskiej to właśnie w Warszawie. Dlaczego? Ponieważ w tym sektorze, liczy się jakość, kreatywność i skalowalność, a nie miejsce pochodzenia studia. Gracz kupujący grę o zombie, postapokalipsie czy świecie fantasy zwykle nie pyta, czy zespół

pracował w Warszawie, Wrocławiu, Londynie czy Seulu – pyta, czy produkt jest dobry. W tym sensie gamedev jest branżą globalną, gdzie narodowość producenta ma znaczenie drugorzędne wobec jakości dzieła. *Cyberpunk 2077, Dying Light* czy *Frostpunk* to polskie produkty rozpoznawalne globalnie, ale Polska nie sprzedaje w tym obszarze „polskości", tylko jakość, klimat, technologię i wyobraźnię

W cyberbezpieczeństwie logika obowiązuje jednak inna. Tu produkt jest elementem infrastruktury zaufania, narzędziem dostępu do danych, mechanizmem egzekwowania polityk i często strażnikiem najbardziej wrażliwych informacji. Oprogramowanie bezpieczeństwa działa w najbardziej uprzywilejowanym miejscu systemu, ma wgląd w pliki, pamięć, procesy, konfigurację i ruch sieciowy. Z tego powodu zaufanie do producenta nie jest abstrakcyjną preferencją zakupową, lecz jednym z podstawowych kryteriów bezpieczeństwa państwa, biznesu i obywatela.

Dlaczego zaufanie ma znaczenie

Antywirus, EDR, platforma XDR, VPN, system DLP czy narzędzie do analizy sieci nie są neutralne w tym samym sensie co gra komputerowa. Ich zadaniem jest widzieć więcej niż zwykły użytkownik, reagować szybciej niż człowiek i mieć dostęp tam, gdzie inne aplikacje nie sięgają. Jeśli taki system jest źle zaprojektowany, podatny na kompromitację albo kontrolowany przez podmiot podporządkowany obcej władzy, może stać się nie tarczą, lecz kanałem wycieku informacji. Dlatego w cyberbezpieczeństwie pochodzenie producenta i jego jurysdykcja naprawdę mają znaczenie.

Przypadek Kaspersky'ego stał się jednym z najczęściej cytowanych przykładów tego problemu. Reuters opisywał decyzje władz USA i Wielkiej Brytanii o ograniczaniu użycia produktów tej firmy w systemach rządowych z powodu obaw o wpływ Kremla i ryzyko dla bezpieczeństwa narodowego. Uzasadnienie nie sprowadzało się do technicznej oceny jednego programu, lecz do szerszego pytania: czy podmiot działający w obcej jurysdykcji, powiązanej z aparatem państwowym, może zostać zmuszony do współpracy z własnym państwem? Właśnie tu ujawnia się różnica między „dobrym produktem" a „produktem, któremu można powierzyć strategiczny dostęp".

Inny słynny przykład Telegram, który startował jako „niezależny" komunikator stworzony przez Pawła Durowa, który po konflikcie z rosyjskimi władzami w czasach

VKontakte budował wizerunek produktu odpornego na naciski Kremla i bezpiecznego dla opozycji oraz aktywistów. Z tego powodu przez lata uchodził za jedno z głównych narzędzi komunikacji dla środowisk antykremlowskich, ukraińskich, białoruskich czy szerzej – opozycji w regionie.

Dziennikarze niezależnych portali i mediów ustalili, że już wcześniej – w latach 2015–2021 – Durow odwiedzał Rosję regularnie, ponad 50 razy, głównie Moskwę i Petersburg, choć publicznie deklarował, że „nie ma drogi powrotnej" i nie planuje powrotu do kraju. Ostatnie potwierdzone wizyty miały miejsce jesienią 2021 r., kiedy w Rosji trwała kampania wyborcza, a na Telegramie blokowano boty i kanały opozycji.

Po latach budowania wizerunku „niezależnego" twórcy Telegrama Paweł Durow stał się bezpośrednim celem organów ścigania w Unii Europejskiej. W sierpniu 2024 r. został zatrzymany na paryskim lotnisku Le Bourget na podstawie nakazu wydanego przez francuską prokuraturę, w ramach śledztwa dotyczącego roli Telegrama w przestępczości zorganizowanej i braku współpracy z organami ścigania. Durow – posiadający obywatelstwo francuskie i ZEA – został oskarżony i objęty nadzorem sądowym, z zakazem opuszczania Francji po wpłaceniu wysokiej kaucji.

Francja postawiła mu zarzuty związane nie tyle z pojedynczym incydentem, co z systemową tolerancją przestępczości na platformie. Według komunikatów paryskiej prokuratury i relacji mediów, Durow usłyszał m.in. zarzuty współudziału w administrowaniu platformą internetową w celu umożliwienia nielegalnych transakcji w ramach zorganizowanej grupy przestępczej, odmowy współpracy z organami ścigania, współudziału w rozpowszechnianiu pornografii dziecięcej, ułatwiania handlu narkotykami, oszustw, prania brudnych pieniędzy oraz przestępczego spisku. U sedna była teza, że brak moderacji treści i odmowa przekazywania danych użytkowników w praktyce czyni go współodpowiedzialnym za działalność przestępczą na Telegramie.

Dla Unii Europejskiej i Francji ten przypadek stał się również narzędziem wymuszenia współpracy. Po zatrzymaniu Durowa przedstawiciele Telegrama deklarowali, że platforma przestrzega prawa UE, a firma zaczęła komunikować gotowość do większego dostosowania się do europejskich regulacji, w tym wymogów dotyczących przeciwdziałania praniu pieniędzy, moderacji treści i współpracy z organami ścigania. De facto oznacza to przejście z modelu „kompletnie niezależnego" komunikatora do modelu, w którym właściciel platformy i sama usługa podlegają rosnącej presji prawnej i politycznej.

Geopolityka w kodzie

Współczesne cyberbezpieczeństwo nie ogranicza się do skuteczności algorytmów detekcji. Coraz częściej obejmuje ocenę łańcucha dostaw, ryzyka przejęcia firmy, potencjalnego wpływu regulacji kraju pochodzenia oraz możliwości wymuszenia współpracy przez tamtejsze służby. W praktyce oznacza to, że organizacja nie kupuje wyłącznie licencji. Kupuje także model odpowiedzialności, model prawny, model własności, model dostępu do danych i model odporności na nacisk polityczny. Jeśli producent oprogramowania bezpieczeństwa podlega obcej jurysdykcji, to należy zadać pytania o przejrzystość własności, miejsce przechowywania telemetrii, kanały aktualizacji, procedury reagowania na incydenty i możliwość zdalnego wymuszania zmian. W przypadku narzędzia, które działa z najwyższymi uprawnieniami, nawet mało prawdopodobne scenariusze mają wysoką wagę skutków.

Dzisiaj to nie jest dyskusja „czy" tylko „jak" ograniczać wpływ obcych państw na cyberbezpieczeństwo

W nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC 2.0, implementującej NIS2) zostało wprowadzone pojęcie „Dostawca Wysokiego Ryzyka" (DWR) to producent sprzętu lub oprogramowania ICT, którego produkty mogą poważnie zagrażać bezpieczeństwu państwa, obronności, porządkowi publicznemu lub życiu i zdrowiu ludzi. Po formalnym uznaniu dostawcy za DWR, podmioty kluczowe i ważne (wg KSC) nie mogą kupować wskazanych produktów/usług, a te już wdrożone muszą zostać wycofane w określonym czasie (4–7 lat, zależnie od sektora). Ustawowo przewidziano też dotkliwe kary za brak wycofania – sięgające nawet dziesiątek milionów złotych / procent obrotu, w szczególności dla podmiotów kluczowych.

Formalnie status DWR nie zależy automatycznie od kraju pochodzenia, choć w praktyce jednym z kryteriów jest wpływ państwa macierzystego na dostawcę (np. możliwość wymuszenia współpracy przez służby, brak niezależnego sądownictwa, regulacje nakazujące współpracę z wywiadem itp.). Procedura ma charakter administracyjny: decyzję wydaje Minister Cyfryzacji po zasięgnięciu opinii Kolegium ds. Cyberbezpieczeństwa, w oparciu o ocenę techniczną (podatności, architektura, łańcuch dostaw) i nietechniczną (własność, jurysdykcja, powiązania polityczne).

W praktyce projekt od początku był politycznie „gorący", bo oznacza realne narzędzie do wykluczania konkretnych firm np. domyślnie wskazywano chińskich dostawców infrastruktury 5G, takich jak Huawei i ZTE.

Nawet sojusznicy mają własne interesy

Problem nie kończy się na państwach jawnie wrogich. Prawdziwa dojrzałość strategiczna polega na zrozumieniu, że nawet sojusznicy posiadają własne interesy narodowe. Dziś Polska funkcjonuje w silnych strukturach sojuszniczych – NATO, Unii Europejskiej i szeroko rozumianego Zachodu. To jednak nie oznacza automatycznej zgodności interesów w każdej sytuacji. Co jeśli strategiczne interesy dużego państwa sojuszniczego zaczną rozmijać się z interesami Polski? Co jeśli dla partnera geopolitycznego priorytetem stanie się szybkie zakończenie konfliktu na wschodzie – nawet kosztem bezpieczeństwa Polski lub Europy Środkowo-Wschodniej?

Technologia nie jest neutralna wobec takich napięć.

Cyberpancerz – lista polskich rozwiązań cyberbezpieczeństwa

Cyberbezpieczeństwo instytucji czy organizacji można podzielić na obszary bezpieczeństwa np.: end-point-ów (laptopów, smartphonów), serwerów, kopii zapasowych, ruchu sieciowego, rejestracji sesji zdalnych, proxy, zgodności polityk, systemu edukacji pracowników, bezpieczeństwo konfiguracji usług chmurowych itd.

Każdy z tych obszarów można porównać do pojedynczej „płyty" pancerza.

I tak jak w porządnej zbroi płytowej możemy wyróżnić fragmenty, które chronią niezwykle newralgiczne fragmenty ciała tak i tutaj możemy płyty pancerza (narzędzia cyberbezpieczeństwa) podzielić na krytyczne i wspomagające

Narzędzia krytyczne to takie, które mają bezpośredni dostęp do danych wrażliwych (konfiguracje, pliki, metadane, ruch, klucze szyfrujące, logi, sesje). Przejęcie lub kompromitacja prowadzi do krytycznego incydentu (np. łamanie szyfrów, wyciek danych, sabotaż, manipulacja logami, zablokowanie backupów). Działają z najwyższymi uprawnieniami (administrator, system, kernel, root).

Obszary krytyczne:

Obszar	Przykładowe narzędzia
Endpoint & Network Protection	EDR, XDR, NDR, antywirusy korporacyjne
Komunikacja i tożsamość	Komunikatorów korporacyjny (szyfrowany), systemy PKI, MFA, SSO
Monitorowanie i rejestracja	Systemy rejestracji sesji zdalnych (RDP/SSH/VNC), SIEM, DLP
Backup i odporność	Systemy backupu, archiwizacja
Zarządzanie infrastrukturą	BMC, IPMI, systemy zarządzania siecią, orchestracja chmury
Chmura i API	Systemy zarządzania dostępem do chmury, API gateways

Narzędzia wspomagające to takie, które nie przetwarzają danych wrażliwych w sposób bezpośredni. Biorą udział w procesie cyberbezpieczeństwa, ale nie mają pełnego dostępu do plików, sesji, konfiguracji. Polsce powinno zależeć, aby być liderem w tych dziedzinach, ponieważ wysoka jakość produktu wiąże się z wysokim poziomiem cyberbezpieczeństwa polskich firm i instytucji. Równocześnie kompromitacja tego typu rozwiązania to ryzyko operacyjne, ale nie krytyczny incident.

Obszary wspomagające:

Obszar	Przykładowe narzędzia
Edukacja i świadomość	Platformy „edukuj i sprawdzaj", symulacje phishingu, testy wiedzy
Dokumentacja i zgodność	Systemy wspierające zgodność z NIS2, KSC 2.0, CRA, CRI
Audyt i testy	Narzędzia do audytów, testów penetracyjnych (niezależne od środowiska)
Analiza zagrożeń	Platformy threat intelligence (konsultacyjne, nie zintegrowane)

Wnioski dla Polski

Powinna powstać formalna lista polskich rozwiązań cyberbezpieczeństwa wraz z rozwiązaniem prawnym w Prawie Zamówień Publicznych umożliwiającym preferowanie produktów z tej listy, ze względu na bezpieczeństwo państwa. W końcu po szczycie NATO w 2016 roku cyberprzestrzeń została wpisana jako pełnoprawna domen prowadzenia działań wojennych. Polskie instytucje powinna mieć możliwość zaopatrzyć się pełen cyber pancerz od polskich komercyjnych dostawców, którzy odnoszą sukces nie tylko na rodzinnym obszarze, ale przede wszystkim w eksporcie. W końcu brak eksportu budzi uzasadnione obawy o jakość produktu, a nie można zapominać, że Polska w swoim geostrategicznym położeniu musi kłaść nacisk nie tylko na wspieranie gospodarki, ale również i najlepsze jakościowo rozwiązania na świecie. Warto zauważyć, że już teraz Polska posiada olbrzymie portfolia firm cyberbezpieczeństwa, które odniosły globalny sukces. **Co w przypadku, gdy polski przemysł nie wytworzył odpowiedniego jakościowego rozwiązania w danym obszarze?**

W takim przypadku powinna być możliwość zaopatrzenia się w produkt z kraju Trójmorza lub „on premise" t.j. oprogramowanie lub infrastruktura IT, która chociaż pochodzi z dalekiego państwa (np.: Turcja), to działa na lokalnym serwerze firmy lub instytucji, a więc w przypadku geopolitycznych napięć istnieje możliwość odłączenie jej od centrali.

Polska podpisem Prezydenta RP – Karola Nawrockiego pod ustawą KSC 2.0. w dniu 19 lutego 2026 formalnie stwierdziła, że **cyberbezpieczeństwo ma narodowość.** Czas tą myśl wprowadzić w życie. Lista firm w postacie cyberpancerza wraz z preferencyjnymi regulacjami w PZP jest odpowiedzią na polityczno-technologiczne wyzwania naszych czasów.

Czy Polskę stać na Narodowy Program budowy Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa?

ppłk rez. dr inż. Robert Kośla

Abstrakt

Artykuł przedstawia założenia Narodowego Programu Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa jako strategicznej inicjatywy wzmacniającej suwerenność technologiczną, bezpieczeństwo narodowe i konkurencyjność gospodarczą Polski. Autor wskazuje na potrzebę budowy zintegrowanego ekosystemu innowacji, opartego na współpracy sektora publicznego, przemysłu, środowiska akademickiego i inwestorów, ze szczególnym uwzględnieniem sztucznej inteligencji, chmury obliczeniowej, technologii kwantowych, kryptografii oraz rozwiązań podwójnego zastosowania. Program ma wykorzystać istniejące kompetencje Polski w zakresie cyberbezpieczeństwa i certyfikacji, tworząc podstawy dla rozwoju krajowego klastra technologicznego zdolnego do konkurowania na rynku europejskim i globalnym.

Słowa kluczowe: cyberbezpieczeństwo; suwerenność cyfrowa; Cyfrowy Okręg Przemysłowy; sztuczna inteligencja; technologie kwantowe; chmura obliczeniowa; kryptografia; innowacje; bezpieczeństwo narodowe; partnerstwo publiczno-prywatne.

Uzasadnienie strategiczne

Polska znajduje się na strategicznym rozdrożu w globalnym wyścigu o przywództwo technologiczne, szczególnie w zakresie nowych przełomowych technologii, takich jak sztuczna inteligencja (AI), przetwarzanie w chmurze i technologie kwantowe.

Wizją strategiczną powinna być budowa Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa – ekosystemu innowacji w Polsce podobnego do kalifornijskiej Doliny Krzemowej – który wykorzysta istniejące atuty kraju w zakresie cyberbezpieczeństwa i kryptografii oraz wyniesie go na czołową pozycję w cyfrowej przyszłości Europy.

Niniejszy artykuł przedstawia zarys Narodowego Programu Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa (NPCOPCyber), równoważącego bezpieczeństwo narodowe z wolnością innowacji oraz angażującego sektor publiczny (w tym agencje rządowe), przemysł prywatny, inwestorów i środowisko akademickie w program współpracy.

Imperatywy strategiczne

Polskie władze uznają konieczność zapewnienia suwerenności technologicznej i odporności. Program opiera się na trzech podstawowych imperatywach:

- **Bezpieczeństwo narodowe i suwerenność cyfrowa** – jako jeden z krajów w Europie najczęściej atakowanych w cyberprzestrzeni, Polska musi opracować własne bezpieczne technologie cyfrowe, aby zmniejszyć zależność od zagranicznych dostawców i chronić dane krytyczne. Program strategiczny wykorzystuje te atuty, aby wzmocnić bezpieczeństwo narodowe i zmniejszyć zależność od technologii zewnętrznych.
- **Wzrost gospodarczy i wiodąca rola w dziedzinie innowacji** – tworząc Cyfrowy Okręg Przemysłowy w obszarze cyberbezpieczeństwa (COPCyber jako krajowe centrum technologiczne na wzór Doliny Krzemowej, Polska może zdobyć większy udział w gospodarce cyfrowej i branżach o wysokiej wartości. gospodarka cyfrowa będzie stanowić około 9% polskiego PKB (około 123 mld USD). Jako lider regionalny Polska może przyciągać talenty i kapitał oraz służyć jako centrum dla aspiracji technologicznych Europy Środkowej i Wschodniej oraz Państw Bałtyckich.
- **Europejska i globalna konkurencja technologiczna** – program powinien wpisywać Polskę w szersze dążenia Europy do konkurencyjności technologicznej, czerpiąc jednocześnie z najlepszych światowych praktyk. Tworząc COPCyber, Polska może uzupełniać inicjatywy UE (takie jak unijna ustawa

o chipach dotycząca półprzewodników oraz cele Dekady Cyfrowej) i wyrobić sobie niszę jako europejskie centrum innowacji cyfrowych w obszarze cyberbezpieczeństwa. Oznacza to, że polski program powinien być częścią globalnego ruchu mającego na celu dostosowanie innowacji technologicznych do strategicznych celów narodowych i musi być realizowany z równie ambitnym nastawieniem.

Wizja programu – proponowany przeze mnie Narodowy Program Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa to kompleksowy, wieloaspektowy plan budowy prężnego klastra technologicznego skupionego na technologiach sztucznej inteligencji typu, chmurze obliczeniowej i technologiach kwantowych w Polsce, oparty na światowej klasy wiedzy specjalistycznej w zakresie matematyki, fizyki, bezpieczeństwa i kryptografii.

Istniejące możliwości Polski i dziedzictwo w zakresie technologii cyberbezpieczeństwa

Uważam, że ambicje Polski dotycząca budowy Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa powinny opierać się na wieloletnim doświadczeniu w zakresie kryptoanalizy, kryptografii, projektowania urządzeń do bezpiecznej komunikacji oraz kompetencji w zakresie badań i certyfikacji cyberbezpieczeństwa:

- **Doświadczenie instytucjonalne (UOP/ABW oraz SKW)** – Urząd Ochrony Państwa (UOP) – historycznie ukształtował wczesne możliwości Polski w zakresie oceny i certyfikacji narzędzi kryptograficznych służących do ochrony informacji niejawnych. Od 2002 r. Ten solidny ekosystem oceny i certyfikacji gwarantuje, że rozwiązania polskiej produkcji spełniają rygorystyczne wymagania bezpieczeństwa – co jest kluczowym czynnikiem umożliwiającym realizację inicjatywy COPCyber.
- **Sprawdzone technologie krajowe** – w Polsce działa kilka firm i ośrodków badawczo-rozwojowych, które mogą pochwalić się znaczącymi osiągnięciami w dziedzinie bezpiecznych technologii cyfrowych. Krajowe produkty i innowacje pokazują dotychczasowe atuty Polski w dziedzinie kryptografii, bezpiecznej komunikacji i cyberbezpieczeństwa – zapewniając platformę

zaufania i know-how do budowy nowej doliny innowacji cyfrowych. Programy certyfikacyjne ABW i SKW potwierdziły jakość wielu z tych produktów, podkreślając wiarygodne osiągnięcia Polski w dziedzinie technologii o wysokim poziomie bezpieczeństwa.

- **Ważne kamienie milowe** – oprócz dotychczas certyfikowanych produktów polskie instytuty badawcze i sektor obronny osiągnęły znaczące przełomy w obszarach które powinny być objęte nowym programem COPCyber. Takie kamienie milowe wzmacniają strategiczne uzasadnienie dla inwestowania w krajowy klaster technologiczny: Polska może stać się liderem w dziedzinie bezpiecznych innowacji cyfrowych, pod warunkiem odpowiedniej organizacji i wsparcia.

Ramy programu: budowa Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa (COPCyber)

Aby zrealizować tę wizję, polski Narodowy Program Bezpiecznej Cyfrowej Doliny Przemysłowej w obszarze cyberbezpieczeństwa powinien zostać oparty na podstawowych filarach i mechanizmach współpracy między zainteresowanymi stronami.

Zarządzanie i model organizacyjny

Partnerstwo publiczno-prywatne (PPP) i koordynacja

Skuteczny ekosystem innowacji wymaga ścisłej koordynacji działań rządu, przemysłu i środowiska akademickiego. W ramach programu należy powołać radę zarządzającą lub biuro programowe w formie partnerstwa publiczno-prywatnego (PPP), w skład którego wejdą kluczowe ministerstwa

Rada ta wyznaczałaby kierunki strategiczne, ustalała priorytety projektów (np. Model PPP zapewnia wspólną odpowiedzialność: sektor publiczny kieruje celami strategicznymi i finansowaniem, podczas gdy sektor prywatny i środowisko akademickie wnoszą potencjał innowacyjny oraz perspektywę rynkową.)

Strategii Sztucznej Inteligencji, któremu przewodniczy prezydent, skupia ministrów, ekspertów technologicznych, a nawet Narodową Służbę Wywiadowczą w celu

kierowania polityką w zakresie sztucznej inteligencji i cyfryzacji. Stany Zjednoczone, choć bardziej zdecentralizowane, wykorzystują sieć krajowych agencji innowacyjnych i partnerstw przemysłowych (takich jak współpraca DARPA z firmami z Doliny Krzemowej) w celu zharmonizowania rozwoju technologii obronnych i komercyjnych.

Krajowi liderzy i integracja MŚP

Program powinien wykorzystywać firmy będące „krajowymi liderami" – uznane polskie firmy technologiczne i wykonawców z sektora cyberbezpieczeństwa o sprawdzonych możliwościach (takie jak WB Group, Asseco, Comarch, Enigma, ComCERT). Jednocześnie polityka będzie zachęcać MŚP i start-upy do udziału poprzez inkubatory, akceleratory i wyzwania innowacyjne, zapewniając, że mniejsze innowacyjne firmy staną się integralnymi uczestnikami klastra.

Synergia cywilno-wojskowa

Odzwierciedlając potencjał nowych technologii podwójnego zastosowania, program NPCOPCyber będzie wspierał współpracę między sektorem cywilnym a obronnym. Zarządzanie klastrem powinno uwzględniać wkład agencji obronnych

W Stanach Zjednoczonych agencje takie jak DARPA, wyraźnie dążą do przeniesienia innowacji „z laboratorium do rzeczywistego świata" w celu osiągnięcia korzyści zarówno dla bezpieczeństwa narodowego, jak i gospodarczego, a Japonia poszerza swoją bazę przemysłowo-obronną, traktując sektor obronny jako priorytetowy obszar wzrostu i łagodząc przepisy dotyczące eksportu technologii związanych z obronnością.

Ramy regulacyjne i prawne

Regulacje oparte na zasadach i sprzyjające innowacjom

Kluczowym czynnikiem sukcesu jest otoczenie regulacyjne, które wspiera innowacje, a nie je hamuje. Polska powinna przyjąć podejście oparte na zasadach w zakresie regulacji nowych technologii: skupiając się na ogólnych zabezpieczeniach i efektach, a nie na nadmiernie szczegółowych przepisach. Należy wykorzystywać regulacyjne

piaskownice (dla sztucznej inteligencji, fintech-u, systemów autonomicznych), aby umożliwić firmom testowanie nowych technologii pod nadzorem organów regulacyjnych bez przedwczesnego wprowadzania pełnych regulacji. Co istotne, unijne przepisy ramowe dla sztucznej inteligencji wyłączają zastosowania związane z obronnością z cywilnych regulacji dotyczących sztucznej inteligencji, uznając potrzebę odrębnego traktowania technologii wojskowych – jest to niuans, który Polska może wziąć pod uwagę przy równoważeniu innowacji i nadzoru bezpieczeństwa.

Konkretne zmiany prawne w Polsce

Aby stworzyć sprzyjające środowisko, w założeniach dla programu NPCOPCyber proponuję konkretne zmiany w aktualnych polskich przepisach.

1. **Zachęty do badań, rozwoju i innowacji** – należy opierać się na istniejących w Polsce przepisach sprzyjających innowacjom, takich jak ustawa o wspieraniu działalności innowacyjnej (2017 r. Należy zmienić tę ustawę, aby jeszcze bardziej wzmocnić zachęty do stosowanych badań i rozwoju oraz projektów pilotażowych, a nie tylko badań laboratoryjnych. Jedną z opcji jest odliczenie z tytułu „rozwoju i wdrożenia", pozwalające firmom odliczyć część kosztów związanych z skalowaniem prototypów lub wdrażaniem innowacji (nie tylko w fazie badawczej).)
2. **Zmiany w prawie zamówień publicznych** – należy znowelizować Prawo zamówień publicznych w celu lepszego wspierania innowacyjnych i zaawansowanych technologicznie rozwiązań. Wprowadzenie do polskiego prawa wytycznych dotyczących zamówień przedkomercyjnych (zgodnych z ramami UE) zapewniłoby innowacyjnym polskim MŚP możliwość wczesnego wdrażania rozwiązań w sektorze publicznym.
3. **Kontrola eksportu i produkty podwójnego zastosowania** – należy zmienić krajowe procedury kontroli eksportu w Polsce w odniesieniu do technologii podwójnego zastosowania (zaawansowane szyfrowanie, sztuczna inteligencja itp. Należy dostosować się do przepisów UE (ramy rozporządzenia UE w sprawie produktów podwójnego zastosowania 2021/821), jednocześnie usprawniając procesy licencyjne w kraju.), która kładzie nacisk na zabezpieczenie kluczowych technologii, jednocześnie ostrożnie ułatwiając handel z sojusznikami w celu utrzymania konkurencyjności rynkowej.

4. **Przepisy dotyczące zarządzania danymi i cyberbezpieczeństwa** – należy zadbać o to, by przepisy dotyczące ochrony danych i cyberbezpieczeństwa (np. wdrożenie w Polsce dyrektywy UE NIS2 oraz ustawy o sztucznej inteligencji) były egzekwowane w sposób zapewniający ochronę obywateli i infrastruktury, nie hamując przy tym innowacji.

Reasumując, zmiany te mają na celu stworzenie zmodernizowanego ekosystemu prawnego, który zachęca do eksploracji, testowania i skalowania najnowocześniejszych technologii w Polsce – podobnie do dynamicznego, proinnowacyjnego klimatu, któremu przypisuje się sukces amerykańskiej Doliny Krzemowej (gdzie łagodne regulacje i silna ochrona własności intelektualnej przyciągnęły innowatorów).

Rezultatem powinny być inteligentne regulacje, które chronią interesy publiczne (bezpieczeństwo, ochronę, prywatność), jednocześnie usuwając przestarzałe lub nadmierne bariery dla innowacji.

Instrumenty gospodarcze i finansowe

Ulgi podatkowe i kredyty na badania, rozwój i wdrażanie – Polska już teraz zapewnia ulgi podatkowe na badania i rozwój (odliczenie w wysokości 100-200% kwalifikowanych wydatków na badania i rozwój). Konkretne środki powinny obejmować: zwiększenie stawek odliczeń na badania i rozwój w obszarach priorytetowych (sztuczna inteligencja, technologia kwantowa, cyberbezpieczeństwo), zwłaszcza dla MŚP; oferowanie zwrotnych ulg podatkowych dla start-upów niepodlegających opodatkowaniu (tak, aby nawet innowatorzy, którzy jeszcze nie osiągają zysków, otrzymywali zwrot gotówki – podejście stosowane przez Koreę Południową i inne kraje w celu wspierania młodych firm); oraz dodanie ulgi podatkowej z tytułu „pierwszego wdrożenia", o którą firmy mogą się ubiegać, gdy projekt badawczo-rozwojowy zaowocuje wprowadzeniem na rynek lub wykorzystaniem w Polsce produktu nadającego się do sprzedaży.

Środki takie zachęcają nie tylko do wynalazczości, ale także do komercyjnego wdrażania nowych technologii.

Finansowanie publiczne i dotacje – polski rząd powinien przeznaczyć specjalne środki na konkurencyjne dotacje i zaproszenia do składania wniosków w ramach „wielkich wyzwań" w dziedzinie nowych technologii. ogólnokrajowy konkurs

na opracowanie kolejnych polskich modeli sztucznej inteligencji lub na zbudowanie do 2030 r. prototypu platformy komunikacyjnej zabezpieczonej kwantowo.

Tam, gdzie to możliwe, należy wykorzystać fundusze unijne (Horyzont Europa, Cyfrowa Europa – w ramach Europejskiego Centrum Kompetencji Cyberbezpieczeństwa – ECCC) w połączeniu z krajowym współfinansowaniem. Na przykład należy utworzyć Polski Fundusz Bezpiecznych Technologii (podobny w duchu do DARPA lub unijnego EIC Accelerator), który finansuje projekty o wysokim ryzyku i wysokich zyskach, łączące środowisko akademickie i start-upy, zwłaszcza w zakresie technologii podwójnego zastosowania.

Polska musi w podobny sposób przeznaczyć znaczne środki publiczne na pobudzenie rozwoju tej branży.

Wsparcie dla innowacji o podwójnym zastosowaniu i w zakresie bezpieczeństwa – biorąc pod uwagę nacisk na zapewnienie bezpieczeństwa, szczególne wsparcie powinno trafić do innowacji o podwójnym zastosowaniu (posiadających potencjał zarówno cywilny, jak i obronny) – często niedofinansowanych przez inwestorów prywatnych z powodu niepewności rynkowej.

Mechanizmy mogłyby obejmować fundusze dopasowujące (rząd dopasowuje prywatne inwestycje VC w start-upy zajmujące się technologiami bezpieczeństwa) lub gwarantowane zakupy początkowe przez agencje obronne/publiczne, jeśli prototypy spełniają wymagania (jako forma zachęty rynkowej).

Zmniejsza to ryzyko związane z rozwojem technologii takich jak bezpieczne urządzenia komunikacyjne, narzędzia AI do wywiadu lub systemy szyfrowania kwantowego, zapewniając ich wczesne wdrożenie. Program polski może sformalizować takie inicjatywy inkubacyjne (być może na wzór wewnętrznego podejścia „polskiej DARPA" w przypadku kluczowych projektów).

Strefy przedsiębiorczości i infrastruktura – program NPCOPCyber będzie miał wymiar fizyczny. Jako centrum COPCyber można wyznaczyć specjalną strefę ekonomiczną lub park innowacji (np. w pobliżu dużego ośrodka akademickiego, takiego jak Warszawa, Kraków czy Wrocław). Strefa ta oferowałaby firmom z klastra ulgi podatkowe, uproszczenia regulacyjne oraz najnowocześniejszą infrastrukturę (taką jak suwerenne centra danych w chmurze, sieci testowe 5G/kwantowe oraz wspólne laboratoria prototypowe).

Dzięki skupieniu w jednym miejscu firm, liderów kierunkowych i ośrodków badawczych polski COPCyber wygeneruje efekt klastrowy (przenoszenie wiedzy, gromadzenie talentów), który ma kluczowe znaczenie dla przyspieszenia innowacji.

Integracja bezpieczeństwa narodowego i promocja eksportu

Integracja bezpieczeństwa i standardy – cechą charakterystyczną COPCyber powinno być uwzględnienie kwestii bezpieczeństwa od samego początku. Polski program NPCPCyber zapewni udział podmiotów bezpieczeństwa narodowego

Odzwierciedla to koordynację międzyagencyjną obserwowaną za granicą: Korea Południowa uruchomiła niedawno Krajową Grupę Konsultacyjną ds.

Tymczasem Japonia uczyniła bezpieczeństwo gospodarcze (łańcuchy dostaw technologii, technologie krytyczne) formalnym filarem swojej strategii bezpieczeństwa narodowego, podkreślając, że rozwój zaawansowanych technologii ma kluczowe znaczenie dla obronności.

Polski program NPCOPCyber powinien podobnie traktować zaawansowanie technologiczne jako nieodłączny element obrony narodowej, przy czym ABW, SKW i NASK powinny wykorzystać swoje role certyfikacyjne (rozszerzając je na przykład o certyfikaty w zakresie sztucznej inteligencji i bezpieczeństwa w chmurze), aby nadać technologiom „Made in Poland" znak zaufania zarówno w kraju, jak i na arenie międzynarodowej.

Wsparcie eksportu i partnerstwa międzynarodowe – program wykorzysta potencjał polskiego Ministerstwa Spraw Zagranicznych (MSZ) i jego sieci polskich przedstawicielstw do aktywnego promowania polskich rozwiązań w zakresie bezpiecznych technologii za granicą. MSZ powinno koordynować działania z PAIH (Polską Agencją Inwestycji i Handlu) w celu identyfikacji rynków docelowych (sojusznicy z NATO, sąsiedzi z UE itp.) dla polskiego eksportu bezpiecznych technologii.

Polski program NPCOPCyber może również obejmować zachęty dla podmiotów zagranicznych.

Równowaga między bezpieczeństwem a otwartością – ze względu na wrażliwy charakter niektórych nowych technologii Polska będzie utrzymywać rozważną kontrolę eksportu (jak wspomniałem wcześniej), aby zapewnić, że kluczowe technologie nie trafią w ręce przeciwników. Jednak skupiając się na rynkach eksportowych opartych na zaufaniu (NATO/UE oraz partnerzy tacy jak Korea Południowa czy sama Japonia), Polska może stać się globalnym dostawcą zaufanych, bezpiecznych technologii.

Umowy o współpracy międzyrządowej, powinny stanowić podstawę tych działań.

Współpraca z uczelniami i rozwój talentów

Wspólne badania i rozwój oraz konsorcja przemysłowo-akademickie – program NPCOPCyber powinien sformalizować instrumenty współpracy między przemysłem a środowiskiem akademickim poprzez wspólne projekty badawcze oraz wspólne zaplecze badawcze.

Zagraniczne analogie stanowią ośrodki amerykańskiej Narodowej Fundacji Naukowej (NSF) oraz granty badawcze dla uczelni, które dostarczają przemysłowi talenty i pomysły; japoński program „Moonshot R&D", który często łączy przedsiębiorstwa i środowisko akademickie w dążeniu do ambitnych celów; oraz południowokoreański KAIST (Korea Advanced Institute of Science & Tech), współpracujący ramię w ramię z przemysłem i sektorem obronnym

Polska może w podobny sposób wykorzystać swoje uczelnie techniczne i instytuty (np. NASK, Sieć Łukasiewicz) jako siłę napędową innowacji w klastrze.

Rozwój i zatrzymywanie talentów – ludzie są siłą napędową każdego centrum technologicznego. Program NPCOPCyber wzmocni edukację w zakresie STEM (Science Technology Engineering Mathematics) oraz szkolenia z zakresu zaawansowanych umiejętności dostosowanych do potrzeb przemysłu.

Dodatkowo należy włączyć staże technologiczne dla studentów studiów licencjackich oraz programy stypendialne dla polskich studentów umożliwiające szkolenie w czołowych światowych laboratoriach (z zobowiązaniem do powrotu).

Zagraniczne najlepsze praktyki w tym obszarze to trwały sukces Korei Południowej w zakresie badań i rozwoju wynika częściowo z wysoko wykształconej siły roboczej i ukierunkowanych programów szkoleniowych (ich nowy plan działania w zakresie sztucznej inteligencji kładzie nacisk na talenty i strategię „społeczeństwa opartego na sztucznej inteligencji").

Zarządzanie akademicko-przemysłowe – aby w pełni zintegrować środowisko akademickie, Biuro Programowe COPCyber może powołać Radę Naukową złożoną z czołowych polskich i międzynarodowych naukowców, którzy będą udzielać wskazówek dotyczących trendów naukowych i pomagać w ocenie wniosków projektowych.

Zapewni to, że rozwój COPCyber będzie oparty na najnowszej wiedzy – będzie to również sygnał dla środowiska akademickiego, że ma ono swoje miejsce przy stole.

Podobne struktury istnieją w Stanach Zjednoczonych (Prezydencka Rada Doradców ds. Nauki, Technologii), które koordynują politykę naukową na wysokim szczeblu z celami gospodarczymi.

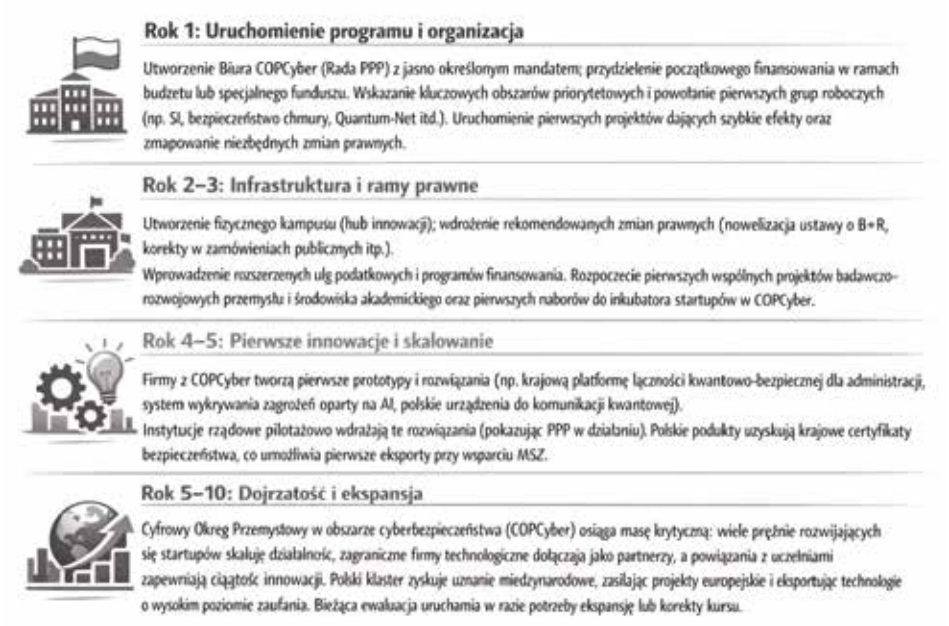
Ryzyko i środki ograniczające

Chociaż potencjalne korzyści są znaczące, muszę też zwrócić szczególną uwagę na zarządzanie ryzykiem i wyzwaniami.

- **Przeszkody biurokratyczne** – jeśli program NPCOPCyber nie zostanie wdrożony w sposób dynamiczny, może utknąć w biurokracji. Środki ograniczające ryzyko: należy przyjąć model lean governance z jasnymi wskaźnikami wydajności dla Biura Programowego COPCyber oraz regularnymi przeglądami postępów przez komitet sterujący.
- **Niepewność regulacyjna** – regulacje dotyczące technologii przełomowych (AI, chmury obliczeniowe, przetwarzanie kwantowe) ewoluują na poziomie UE, co może powodować niepewność wśród przedsiębiorstw. Środki ograniczające ryzyko: Polska powinna aktywnie kształtować regulacje UE (wykorzystując krajową wiedzę specjalistyczną w zakresie bezpieczeństwa i AI) oraz zapewnić wytyczne dla lokalnego przemysłu.
- **Talenty i drenaż mózgów** – przyciąganie i zatrzymywanie najlepszych specjalistów w dziedzinie sztucznej inteligencji, chmury obliczeniowej i technologii kwantowych stanowi wyzwanie w obliczu globalnej konkurencji. Środki ograniczające ryzyko: należy oferować konkurencyjne zachęty (opcje na akcje, granty, uznanie) oraz podkreślać wyjątkową misję (bezpieczeństwo Polski i suwerenność technologiczna), aby przyciągnąć talenty o patriotycznych przekonaniach i nastawione na wywieranie wpływu.
- **Konkurencja rynkowa** – konkurencję będą stanowić światowi giganci technologiczni oraz zagraniczne start-upy. Polskie innowacje mogą mieć trudności, o ile nie będą się wyraźnie wyróżniać. Ponadto należy zachęcać do nawiązywania strategicznych partnerstw z przyjaznymi zagranicznymi firmami technologicznymi (tak jak robi to Japonia, zapraszając do globalnej współpracy w zakresie badań i rozwoju), aby uniknąć izolacji i przyspieszyć proces uczenia się.

Plan wdrożenia (orientacyjne etapy)

Poniżej przedstawiłem proponowany harmonogram realizacji Narodowego Programu Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa.



Rysunek 1: Proponowany harmonogram realizacji Narodowego Programu Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa

Wnioski

Polski Narodowy Program Cyfrowego Okręgu Przemysłowego w obszarze cyberbezpieczeństwa to śmiała inicjatywa łącząca politykę technologiczną, bezpieczeństwa i gospodarczą kraju w jeden transformacyjny program.

Poprzez integrację solidnych fundamentów cyberbezpieczeństwa (polskiego przemysłu kryptograficznego, oprogramowania i kompetencji certyfikacyjnych) z przyszłościowymi inwestycjami w sztuczną inteligencję, technologie chmur obliczeniowych oraz technologie kwantowe, program ma na celu wyniesienie Polski do czołówki krajów wprowadzających cyfrowe innowacje w obszarze cyberbezpieczeństwa.

W tym artykule (bazującym na szerszym dokumencie koncepcyjnym) wskazałem, w jaki sposób można stworzyć i rozwijać Bezpieczną Cyfrową Dolinę Przemysłową: od uzasadnienia strategicznego po konkretne ramy programowe, które obejmują interesariuszy od rządu (np. Ostatecznym rezultatem będzie Polska będąca eksporterem netto zaawansowanych bezpiecznych technologii cyfrowych, liderem innowacji w Europie oraz krajem, który z powodzeniem równoważy bezpieczeństwo i dobrobyt w erze cyfrowej).

Dlaczego polski COP 2.0 zaczyna się w szkole, a nie na politechnice, i jak zbudować nasz ekosystem innowacji bez grantozy?

dr Daniel Milewski

Abstrakt

Artykuł przedstawia filary budowy polskiej suwerenności technologicznej. Autor podkreśla, że podstawą takiego modelu muszą być długofalowe inwestycje w edukację, kompetencje cyfrowe, kulturę eksperymentu i akceptację ryzyka. Tekst krytykuje „grantozę" jako główną patologię polskiej polityki innowacyjnej i wskazuje alternatywne mechanizmy, takie jak: państwo jako pierwszy klient, fundusze funduszy, kapitał cierpliwy, infrastrukturę badawczo-obliczeniową, ulgi podatkowe i wsparcie talentów. Nowy Cyfrowy Okręg Przemysłowy to więc projekt łączący edukację, przemysł, administrację, bezpieczeństwo i kapitał prywatny.

Słowa kluczowe: COP 2.0, Cyfrowy Okręg Przemysłowy, innowacje, edukacja technologiczna, kapitał ludzki, grantoza, deep-tech, suwerenność technologiczna, ekosystem innowacji

Wprowadzenie

Debata o nowoczesnym państwie zbyt często zaczyna się w Polsce od pytania, jak sfinansować laboratoria, startupy i wielkie projekty technologiczne. Tymczasem prawdziwy początek leży wcześniej: w szkole podstawowej, w jakości kształcenia

matematycznego, informatycznego i technicznego, w kulturze rozwiązywania problemów oraz w społecznej zgodzie na eksperyment, który nie zawsze kończy się sukcesem. Jeżeli państwo chce budować własne technologie, nie może zaczynać od końca łańcucha, czyli od pieniędzy dla już ukształtowanych zespołów. Musi zacząć od kapitału ludzkiego, a dopiero potem budować kapitał finansowy i instytucjonalny.

Ta perspektywa dobrze wpisuje się w kontekst Kongresu Fundacji SET „Polska ambitna. Jak wzmacniać państwo w niestabilnym świecie?". Postawiono tam pytania o odporność państwa rozumianą szerzej niż wyłącznie w kategoriach wojskowych. W dyskusjach kongresowych mocno wybrzmiała teza, że bezpieczeństwo państwa obejmuje również gospodarkę, energetykę i technologie, a Polska nie powinna ograniczać się do implementowania cudzych rozwiązań, lecz powinna współtworzyć i eksportować własne technologie.

W tym sensie idea „COP 2.0 – Cyfrowego Okręgu Przemysłowego" (hasło na wzór budowanego w II Rzeczypospolitej Centralnego Okręgu Przemysłowego i postulat podobnego „zastrzyku nowoczesności", jednak już bez geograficznych barier) nie jest wyłącznie projektem gospodarczym. Jest propozycją nowego modelu państwa rozwojowego: takiego, które potrafi łączyć edukację, badania, przemysł, wojsko, administrację i kapitał prywatny. Taki model nie może jednak opierać się na prostym rozdawnictwie środków publicznych. Jeśli ogromny strumień pieniędzy zostanie wpuszczony w tradycyjny system grantowy bez zmiany reguł gry, rezultatem będzie przede wszystkim wzrost liczby podmiotów wyspecjalizowanych w pozyskiwaniu finansowania, a nie w budowaniu produktów, kompetencji i przewag technologicznych.

Punkt wyjścia: edukacja zamiast iluzji skrótu

Najważniejszy program rozwoju technologicznego nie zaczyna się na politechnice, lecz w pierwszych latach edukacji. Państwo, które chce uczestniczyć w globalnym wyścigu technologicznym, musi znacznie podnieść poziom kompetencji cyfrowych dzieci i młodzieży: od logiki, matematyki i programowania, po pracę projektową, rozumienie danych, podstawy automatyki oraz świadome korzystanie z narzędzi sztucznej inteligencji. Bez tego nawet najlepiej zaprojektowane instrumenty finansowe będą działały na zbyt wąskiej bazie talentów.

W praktyce oznacza to potrzebę przejścia od nauczania odtwórczego do nauczania twórczego. Szkoła powinna uczyć nie tylko poprawnych odpowiedzi,

lecz także stawiania hipotez, testowania rozwiązań, pracy w zespole i odpowiedzialności za rezultat. W krajach, które odniosły sukces innowacyjny, przewaga nie bierze się wyłącznie z liczby absolwentów kierunków technicznych. Bierze się z tego, że znaczna część społeczeństwa rozumie technologię nie jako magiczne narzędzie, ale jako obszar, który można współtworzyć.

To prowadzi do zmiany zasadniczej: innowacja nie jest wydarzeniem, lecz kulturą. Jeżeli młody człowiek przez kilkanaście lat funkcjonuje w systemie, w którym liczy się wyłącznie bezbłędne odtworzenie materiału, to później trudno oczekiwać, że jako badacz, przedsiębiorca czy urzędnik będzie skłonny podejmować ryzyko intelektualne. A bez tej skłonności nie ma ani startupów, ani przełomowych technologii, ani ambitnego przemysłu.

Kultura ryzyka: państwo musi zaakceptować porażkę

Jedną z największych barier rozwojowych w Polsce jest publiczna filozofia rozliczania projektów. W wielu obszarach nadal dominuje przekonanie, że projekt badawczy finansowany ze środków publicznych „musi się udać", a jeśli nie doprowadzi do oczekiwanego wyniku, to oznacza błąd, niegospodarność albo nienależyte wykonanie zadania. Taka logika może sprawdzać się przy budowie drogi lub zakupie sprzętu biurowego, ale jest zabójcza dla innowacji.

W świecie nowych technologii porażka nie jest anomalią, lecz elementem procesu selekcji. Znaczna część przedsięwzięć badawczych i startupowych kończy się niepowodzeniem nie dlatego, że były źle prowadzone, lecz dlatego, że eksplorowały obszar realnej niepewności. Jeżeli państwo chce mieć choć kilka wielkich sukcesów technologicznych, musi stworzyć takie ramy prawne i instytucjonalne, w których część projektów może zakończyć się fiaskiem bez automatycznego uruchamiania logiki represyjnej.

To nie oznacza zgody na marnotrawstwo. Oznacza zmianę sposobu oceny: z kontroli samego wyniku na ocenę jakości procesu, kompetencji zespołu, przejrzystości decyzji i wartości zdobytej wiedzy. W innowacji należy rozliczać uczciwość, rzetelność i uczenie się, a nie wyłącznie końcowy triumf. Państwo, które nie potrafi odróżnić nieudanego eksperymentu od nadużycia, samo skazuje się na technologiczny konformizm.

Jak inwestować, a nie rozdawać

W dyskusji o wielkich środkach publicznych kluczowe jest rozróżnienie między wydawaniem a inwestowaniem. Sam rozmiar puli niczego nie gwarantuje. Można wydać setki miliardów złotych i otrzymać tysiące prezentacji, konferencji, raportów i prototypów, które nigdy nie trafią na rynek. Można też użyć podobnych środków do uruchomienia trwałego ekosystemu, w którym publiczny pieniądz przyciąga kapitał prywatny, wzmacnia zdolność komercjalizacji i obniża bariery wejścia dla ambitnych zespołów.

Dlatego główną zasadą powinno być przesunięcie ciężaru z klasycznych grantów na instrumenty wymuszające kontakt z rynkiem. Dotacja przyznana tylko za obietnicę projektu zbyt łatwo staje się celem samym w sobie. Natomiast pieniądz publiczny powiązany z realnym wdrożeniem, zakupem, współinwestowaniem albo stworzeniem infrastruktury dużo lepiej porządkuje bodźce. W takim modelu nie wygrywa ten, kto najsprawniej napisze wniosek, lecz ten, kto potrafi zbudować technologię, znaleźć klienta, dostarczyć produkt i rozwijać firmę.

Warto przy tym pamiętać, że nawet organizatorzy i uczestnicy kongresowych debat podkreślali potrzebę inwestowania w technologie nie milionów, lecz miliardów złotych, przy jednoczesnym budowaniu własnych zdolności technologicznych zamiast biernego korzystania z rozwiązań zagranicznych. Pytanie nie brzmi więc, czy inwestować dużo, lecz jak inwestować mądrze.

Państwo jako pierwszy klient

Najsilniejszym impulsem dla rozwoju technologii bywa nie dotacja, lecz zamówienie. Jeżeli resort obrony, zdrowia, cyfryzacji lub infrastruktury ogłasza, że kupi określoną liczbę sztuk systemu spełniającego jasno opisane parametry, wówczas zmienia się cała dynamika rynku. Przedsiębiorca widzi potencjalny popyt, inwestor widzi szansę na kontrakt, a zespół technologiczny wie, że pracuje nad rozwiązaniem, które może rzeczywiście wejść do użycia.

Mechanizm „*First Buyer*", czyli państwa jako pierwszego klienta, jest szczególnie ważny w sektorach *dual-use* i *deep-tech*, gdzie bariera wejścia jest wysoka, a pierwszy odbiorca ma znaczenie strategiczne. Zamiast finansować sam prototyp, państwo może finansować rynek dla prototypu, a to uruchamia prywatne pieniądze znacznie skuteczniej niż klasyczny grant. W ten sposób administracja przestaje być

biernym rozdawcą środków, a staje się aktywnym kreatorem popytu na technologie ważne z punktu widzenia bezpieczeństwa i konkurencyjności kraju.

Takie podejście dobrze współgra z szerszą kongresową diagnozą, zgodnie z którą odporność państwa wymaga interoperacyjności między służbami, gospodarką i szeroko rozumianą przestrzenią bezpieczeństwa. Zamówienia na technologie publiczne mogą więc działać jednocześnie jako narzędzie rozwojowe, przemysłowe i strategiczne.

Fundusze funduszy i rola prywatnego kapitału

Drugi filar powinien stanowić model, w którym państwo nie wybiera bezpośrednio zwycięzców, lecz wzmacnia profesjonalnych pośredników inwestycyjnych. W praktyce oznacza to rozwój funduszy funduszy oraz współpracy z prywatnymi funduszami *venture capital*. Państwo może występować jako partner cichy, dostarczający część kapitału i poprawiający profil ryzyka, ale nie powinno zastępować rynku w codziennych decyzjach inwestycyjnych.

To rozwiązanie ma silne precedensy. Izraelski program Yozma 2.0 został zaprojektowany tak, aby zwiększać dostępność kapitału dla sektora *high-tech*, wzmacniać stabilność lokalnego rynku VC, zwiększać udział inwestorów instytucjonalnych oraz promować specjalizację funduszy, zwłaszcza w *deep-tech*. Program ma działać bez bezpośredniej ingerencji władz publicznych w decyzje inwestycyjne instytucji i zarządzających funduszami, a państwo oferuje współfinansowanie oraz preferencyjne warunki wykupu swojego udziału.

Szczególnie istotny jest sam mechanizm bodźców. Według informacji Israel Innovation Authority program przewiduje około 160 mln dolarów środków państwowych, które mają uruchomić co najmniej 700 mln dolarów inwestycji inwestorów instytucjonalnych, przy czym państwo dokłada 30 centów do każdego dolara inwestycji i ogranicza własną ingerencję w proces alokacji kapitału. To cenna lekcja: skuteczne państwo innowacyjne nie polega na tym, że urzędnik wie lepiej, która technologia wygra, lecz na tym, że potrafi tak ustawić reguły, by rynek chętniej brał udział w finansowaniu ryzyka.

Infrastruktura zamiast samej gotówki

W przypadku sztucznej inteligencji, zaawansowanych symulacji, fotoniki czy nowych materiałów problemem nie zawsze jest brak pomysłów. Często problemem jest brak

dostępu do bardzo drogiej infrastruktury: mocy obliczeniowej, laboratoriów, aparatury pomiarowej, środowisk testowych i zasobów danych. Dlatego część wsparcia powinna mieć charakter majątkowy, a nie wyłącznie gotówkowy.

Państwo może budować klastry superkomputerowe, centra testowania technologii, wspólne laboratoria i bezpieczne zasoby obliczeniowe, a następnie udostępniać je w formie voucherów infrastrukturalnych. Taki instrument ma kilka zalet. Po pierwsze, ogranicza ryzyko czysto konsumpcyjnego wykorzystania środków. Po drugie, obniża próg wejścia dla małych zespołów. Po trzecie, tworzy wspólną bazę technologiczną, która zostaje w kraju i może służyć kolejnym projektom.

To szczególnie ważne w obszarach, w których światowy wyścig opiera się na skali. Polski startup nie wygra tylko dzięki entuzjazmowi, jeśli jego konkurent ma wielokrotnie lepszy dostęp do obliczeń, danych i zaplecza eksperymentalnego. Publiczna infrastruktura nie zastąpi rynku, ale może wyrównać warunki startu i zwiększyć szanse na komercjalizację.

Ulgi podatkowe i specjalne warunki dla talentów

Trzeci obszar to otoczenie podatkowe i regulacyjne. Nawet najlepsze programy inwestycyjne nie zadziałają, jeżeli innowacyjna firma będzie jednocześnie obciążona wysoką niepewnością podatkową, skomplikowanym raportowaniem i słabą przewidywalnością prawa. Ekosystem technologiczny potrzebuje nie tyle doraźnych wyjątków, ile spójnego pakietu bodźców wspierających reinwestowanie zysków, działalność badawczo-rozwojową i zatrudnianie najlepszych specjalistów.

Dlatego rozsądne wydaje się skokowe rozszerzenie ulgi B+R oraz IP Box, a także upowszechnienie modelu zbliżonego do estońskiego CIT dla podmiotów uczestniczących w strategicznych strukturach rozwojowych. Brak opodatkowania zysku do momentu jego wypłaty wzmacnia zdolność firmy do akumulacji kapitału, inwestowania w zespół i skalowania działalności. W sektorach technologicznych, gdzie wzrost wymaga wieloletniego reinwestowania, ma to znaczenie fundamentalne.

Osobnego namysłu wymaga również polityka wobec talentów. W wybranych projektach strategicznych można rozważyć preferencje podatkowe dla najwyższej klasy inżynierów, badaczy i menedżerów technologicznych. Nie chodzi o tworzenie przywileju dla wąskiej grupy, lecz o świadome uznanie, że globalna konkurencja o talenty jest dziś równie ważna jak konkurencja o kapitał.

Deep-tech, czyli kapitał cierpliwy

Nie wszystkie innowacje dają się finansować klasycznym modelem venture capital. Część projektów *deep-tech* dojrzewa długo, wymaga kosztownych badań, certyfikacji, testów przemysłowych i bardzo wysokiej tolerancji na niepewność. W takich obszarach jak fotonika, półprzewodniki, materiały zaawansowane, technologie kosmiczne czy zaawansowana biotechnologia prywatny rynek często uznaje ryzyko za zbyt duże albo horyzont zwrotu za zbyt odległy.

Właśnie tutaj potrzebne są państwowe wejścia kapitałowe o długim horyzoncie, realizowane przez wyspecjalizowany fundusz celowy. Taki fundusz powinien działać według zasad inwestora portfelowego: akceptować, że część przedsięwzięć upadnie, ale kilka może przynieść ogromny zwrot gospodarczy i strategiczny. Kluczowe jest jednak to, by zarządzanie takim kapitałem było profesjonalne, autonomiczne i odporne na logikę politycznego cyklu.

Gdzie zostawić klasyczne granty

Nie oznacza to, że klasyczne bezzwrotne granty należy zlikwidować. Powinny jednak zostać przesunięte tam, gdzie są naprawdę uzasadnione: do badań podstawowych i bardzo wczesnych etapów rozwoju technologii, czyli tam, gdzie rynek z definicji nie jest jeszcze w stanie wycenić potencjału projektu. Uczelnie, instytuty badawcze i zespoły pracujące na poziomach TRL 1-3 nadal potrzebują finansowania, które nie wymaga natychmiastowej komercjalizacji.

To właśnie tam powstaje początek lejka innowacji. Problem zaczyna się wtedy, gdy tę samą logikę grantową próbuje się przenieść na etapy, na których produkt powinien już spotkać się z użytkownikiem, inwestorem albo zamówieniem publicznym. Państwo nie powinno więc rezygnować z grantów całkowicie, lecz precyzyjnie zawęzić ich funkcję: mają zasilać przyszłe przełomy, a nie zastępować rynek tam, gdzie rynek powinien już testować jakość rozwiązania.

COP 2.0 – Cyfrowy Okręg Przemysłowy jako projekt państwowy

Jeżeli idea Cyfrowego Okręgu Przemysłowego ma być czymś więcej niż hasłem, musi zostać oparta na czterech połączonych filarach. Pierwszy to edukacja i kapitał

ludzki, zaczynające się od szkoły. Drugi to kultura instytucjonalna dopuszczająca ryzyko i porażkę jako naturalny element procesu innowacji. Trzeci to inteligentna architektura finansowania: zamówienia publiczne, fundusze funduszy, kapitał udziałowy, vouchery infrastrukturalne i ukierunkowane ulgi podatkowe. Czwarty to państwo zdolne do współpracy międzyresortowej, które umie połączyć politykę technologiczną z bezpieczeństwem, przemysłem i rozwojem regionalnym.

W szerszym sensie jest to odpowiedź na diagnozę sformułowaną podczas kongresu: bezpieczeństwo i odporność państwa nie kończą się na obronności, lecz obejmują także finanse publiczne, przewidywalność podatków, zdolności przemysłowe i kompetencje technologiczne. Polska potrzebuje więc nie tylko większych pieniędzy, ale przede wszystkim nowej filozofii ich używania.

Zakończenie

Najbardziej ambitne państwa nie wygrywają dlatego, że mają najlepsze hasła o innowacjach. Wygrywają dlatego, że konsekwentnie budują łańcuch od edukacji do komercjalizacji, od szkolnej ciekawości do przemysłowej skali, od publicznej infrastruktury do prywatnego kapitału, od odwagi badawczej do dojrzałego rynku. Polska może taki model stworzyć, ale tylko pod warunkiem, że przestanie utożsamiać politykę innowacyjną z dystrybucją grantów.

Stawką nie jest kolejny program wsparcia. Stawką jest zdolność państwa do wytwarzania własnych technologii, zatrzymywania talentów i budowania trwałej suwerenności gospodarczej. COP 2.0 – Cyfrowy Okręg Przemysłowy będzie doliną krzemową tylko wtedy, gdy najpierw stanie się doliną kompetencji, odwagi i dobrze zaprojektowanych instytucji.

Od Centralnego Okręgu Przemysłowego do Cyfrowego Okręgu Przemysłowego – transformacja potencjału strategicznego państwa

Marcin Stachowski, Paweł Turowski

Abstrakt

Artykuł analizuje możliwość wykorzystania doświadczeń Centralnego Okręgu Przemysłowego (COP) jako inspiracji dla budowy współczesnego modelu wzmacniania potencjału państwa określanego mianem ***Cyfrowego Okręgu Przemysłowego***. Punktem wyjścia jest założenie, że źródła potęgi państw ulegają obecnie głębokiej transformacji pod wpływem rozwoju technologii cyfrowych, sztucznej inteligencji, cyberbezpieczeństwa oraz infrastruktury danych. W opracowaniu zastosowano analizę literatury, dokumentów strategicznych oraz danych dotyczących kapitalizacji rynkowej przedsiębiorstw sektora obronnego i technologicznego.

Przeprowadzone badania wskazują, że podobnie jak COP w latach trzydziestych XX wieku koncentrował zasoby państwa wokół strategicznych gałęzi przemysłu, tak współcześnie kluczowe znaczenie dla bezpieczeństwa i rozwoju gospodarczego uzyskują technologie cyfrowe oraz technologie podwójnego zastosowania. Analiza kapitalizacji największych przedsiębiorstw światowego sektora obronnego i sztucznej inteligencji potwierdza przesunięcie głównych obszarów koncentracji kapitału, innowacji i przewag konkurencyjnych w kierunku sektorów opartych na danych, algorytmach i zaawansowanych technologiach.

W artykule wykazano, że zdolność do tworzenia, rozwijania i ochrony kluczowych technologii staje się jednym z podstawowych wyznaczników bezpieczeństwa narodowego, odporności

państwa oraz jego pozycji międzynarodowej. W konsekwencji *Cyfrowy Okręg Przemysłowy* należy postrzegać jako instrument budowy suwerenności technologicznej oraz wzmacniania potencjału strategicznego Polski w warunkach gospodarki cyfrowej i wielodomenowego środowiska bezpieczeństwa XXI wieku.
Słowa kluczowe: Cyfrowy Okręg Przemysłowy, bezpieczeństwo państwa, suwerenność technologiczna, sztuczna inteligencja, technologie przełomowe, odporność państwa.

Wprowadzenie

Współczesne środowisko bezpieczeństwa podlega dynamicznym przeobrażeniom wynikającym zarówno z postępu technologicznego, jak i zmian zachodzących w globalnym układzie sił. W XXI wieku państwa rywalizują nie tylko o przewagę militarną, lecz również o kontrolę nad technologiami, danymi, infrastrukturą cyfrową oraz zdolnością do generowania innowacji. Coraz wyraźniej widoczny staje się proces przesuwania źródeł bogactwa i potęgi państw z tradycyjnych sektorów przemysłowych do obszaru technologii cyfrowych, sztucznej inteligencji, systemów autonomicznych, technologii kosmicznych oraz zaawansowanych usług opartych na przetwarzaniu danych.

Zmiana ta ma charakter strukturalny i wpływa zarówno na rozwój gospodarczy, jak i sposób kształtowania bezpieczeństwa narodowego. O ile w epoce industrialnej o sile państw decydowały przede wszystkim zasoby surowcowe, potencjał przemysłowy, zdolności produkcyjne i możliwości mobilizacji gospodarki na potrzeby wojny przemysłowej, o tyle współcześnie coraz większe znaczenie zyskuje zdolność do tworzenia, pozyskiwania i wykorzystywania technologii przełomowych. W rezultacie technologia staje się nie tylko źródłem wzrostu gospodarczego, lecz również jednym z podstawowych czynników determinujących pozycję państwa w środowisku międzynarodowym oraz jego odporność na zagrożenia militarne, niemilitarne i hybrydowe.

Proces ten jest szczególnie widoczny w polityce największych światowych aktorów. Stany Zjednoczone realizują szeroko zakrojone programy wspierające rozwój półprzewodników, sztucznej inteligencji oraz technologii podwójnego zastosowania. Chiny konsekwentnie budują własny ekosystem technologiczny, traktując niezależność technologiczną jako jeden z filarów bezpieczeństwa państwa. Z kolei Unia Europejska rozwija koncepcję strategicznej autonomii technologicznej, dążąc do ograniczenia zależności od zewnętrznych dostawców kluczowych technologii. Dodatkowo doświadczenia wojny rosyjsko-ukraińskiej potwierdziły rosnące znaczenie

systemów bezzałogowych, cyberprzestrzeni, rozpoznania satelitarnego oraz analityki danych dla prowadzenia współczesnych działań wojennych.

W tym kontekście szczególnego znaczenia nabierają doświadczenia związane z budową Centralnego Okręgu Przemysłowego (COP), jednego z najambitniejszych przedsięwzięć modernizacyjnych II Rzeczypospolitej. Projekt ten miał na celu nie tylko zwiększenie potencjału przemysłowego i obronnego państwa, lecz również stworzenie fundamentów długookresowego rozwoju gospodarczego poprzez koncentrację inwestycji w sektorach uznawanych wówczas za najbardziej nowoczesne i strategiczne. COP stanowił przykład świadomej polityki państwa ukierunkowanej na budowę przewag technologicznych, wzmacnianie odporności gospodarki oraz rozwój zdolności niezbędnych dla zapewnienia bezpieczeństwa narodowego. Współcześnie można dostrzec analogię pomiędzy historyczną logiką budowy COP a potrzebą tworzenia nowoczesnego ekosystemu technologicznego, określanego w niniejszym opracowaniu mianem *Cyfrowego Okręgu Przemysłowego*.

Powstaje zatem zasadniczy problem badawczy dotyczący wpływu transformacji technologicznej na współczesne źródła siły państwa oraz ich znaczenie dla bezpieczeństwa narodowego i rozwoju gospodarczego. Szczególnego znaczenia nabiera pytanie, czy technologie cyfrowe i zdolności technologiczne stają się obecnie strategicznym zasobem państwa porównywalnym do roli, jaką w epoce industrialnej odgrywały przemysł ciężki, infrastruktura produkcyjna oraz potencjał zbrojeniowy.

Analiza została skoncentrowana wokół następujących pytań badawczych:

- czy technologie cyfrowe stają się jednym z głównych źródeł przewagi strategicznej państw;
- jakie znaczenie dla bezpieczeństwa narodowego ma kontrola nad kluczowymi technologiami, danymi i infrastrukturą cyfrową;
- w jakim stopniu krajowy potencjał technologiczny i przemysłowy wpływa na zdolność państwa do zapewnienia bezpieczeństwa oraz odporności na zagrożenia;
- czy Polska rozwija kompetencje technologiczne niezbędne do utrzymania suwerenności technologicznej w warunkach rosnącej konkurencji międzynarodowej.

Celem artykułu jest analiza transformacji potencjału strategicznego państwa poprzez porównanie historycznej koncepcji COP z ideą *Cyfrowego Okręgu Przemysłowego*. Przedmiotem rozważań jest identyfikacja współczesnych źródeł przewagi

strategicznej oraz ocena znaczenia technologii dla bezpieczeństwa narodowego, odporności państwa i rozwoju społeczno-gospodarczego.

Badania przeprowadzono z wykorzystaniem analizy literatury przedmiotu, dokumentów strategicznych, materiałów źródłowych oraz danych dotyczących rozwoju współczesnych sektorów technologicznych. Zastosowano metodę analizy porównawczej oraz podejście indukcyjno-dedukcyjne, umożliwiające identyfikację długoterminowych trendów rozwojowych i ocenę ich znaczenia dla bezpieczeństwa państwa.

W artykule przyjęto tezę, że w warunkach narastającej rywalizacji technologicznej zdolność do tworzenia, rozwijania i ochrony kluczowych technologii staje się jednym z podstawowych wyznaczników pozycji państwa w środowisku międzynarodowym. W konsekwencji *Cyfrowy Okręg Przemysłowy* należy postrzegać nie wyłącznie jako projekt rozwojowy, lecz jako instrument wzmacniania bezpieczeństwa narodowego, odporności strategicznej oraz długookresowej konkurencyjności państwa.

Centralny Okręg Przemysłowy jako instrument budowy potencjału strategicznego państwa

Idea budowy nowego okręgu przemysłowego nie narodziła się dopiero w drugiej połowie lat trzydziestych XX wieku. Jej źródeł należy poszukiwać już w pierwszych latach istnienia odrodzonego państwa polskiego. Doświadczenia wojny polsko-bolszewickiej z lat 1919-1921 oraz analiza położenia geostrategicznego II Rzeczypospolitej doprowadziły do wniosku, że kluczowe zakłady przemysłowe i zbrojeniowe nie powinny znajdować się w bezpośredniej bliskości granic państwa. W przypadku konfliktu zbrojnego mogłyby bowiem zostać szybko zniszczone lub zajęte przez przeciwnika.

W odpowiedzi na te zagrożenia w środowiskach wojskowych opracowano koncepcję tzw. *trójkąta bezpieczeństwa*, obejmującego obszar pomiędzy Wisłą, Sanem i Karpatami. Region ten uznawano za najbardziej odpowiedni do lokalizacji strategicznych inwestycji przemysłowych ze względu na znaczną odległość od granic z Niemcami i Związkiem Sowieckim, korzystne warunki terenowe oraz możliwości rozwoju infrastruktury transportowej i energetycznej[1].

[1] W. Duch, *Centralny Okręg Przemysłowy (COP) – geneza, realizacja i znaczenie największego programu inwestycyjnego II RP*, https://historia.org.pl/2025/03/01/centralny-okreg-przemyslowy-cop-geneza-realizacja-i-znaczenie-najwiekszego-programu-inwestycyjnego-ii-rp/?utm_source=chatgpt.com [dostęp: 06.06.2025].

Do realizacji tej koncepcji powrócono w połowie lat trzydziestych, gdy pogarszająca się sytuacja międzynarodowa, rosnące zagrożenie ze strony III Rzeszy i Związku Sowieckiego oraz konieczność modernizacji Sił Zbrojnych RP wymusiły podjęcie zdecydowanych działań inwestycyjnych. Istotnym czynnikiem były również skutki wielkiego kryzysu gospodarczego, które skłaniały państwo do poszukiwania instrumentów pobudzenia rozwoju gospodarczego i ograniczenia bezrobocia.

Najważniejszym impulsem do realizacji projektu były względy bezpieczeństwa państwa. W drugiej połowie lat trzydziestych kierownictwo polityczne i wojskowe coraz wyraźniej dostrzegało pogarszające się położenie międzynarodowe Polski. Jednocześnie analizy prowadzone przez Ministerstwo Spraw Wojskowych oraz Sztab Główny Wojska Polskiego wskazywały na znaczne zapóźnienie techniczne polskich sił zbrojnych w stosunku do armii największych państw europejskich. W odpowiedzi opracowano program modernizacji i rozbudowy Wojska Polskiego, określany jako sześciolatka modernizacyjna. W latach 1936-1941 planowano przeznaczyć na modernizację uzbrojenia i wyposażenia około 6 mld zł. Realizacja tak ambitnego programu wymagała jednak stworzenia nowoczesnego zaplecza przemysłowego zdolnego do produkcji uzbrojenia, amunicji, sprzętu wojskowego oraz wyposażenia technicznego[2].

Drugą grupę przesłanek stanowiły czynniki gospodarcze. Polska nadal odczuwała skutki światowego kryzysu gospodarczego z lat 1929-1933, który doprowadził do spadku produkcji przemysłowej, ograniczenia inwestycji oraz wzrostu bezrobocia. Władze państwowe poszukiwały instrumentów umożliwiających pobudzenie gospodarki oraz przyspieszenie procesów modernizacyjnych. COP miał stać się motorem industrializacji kraju. Zakładano rozwój nowoczesnych gałęzi przemysłu, w tym przemysłu metalurgicznego, maszynowego, chemicznego, elektrotechnicznego oraz zbrojeniowego. Inwestycje miały zwiększyć potencjał produkcyjny państwa, pobudzić rozwój infrastruktury transportowej i energetycznej oraz stworzyć nowe impulsy rozwojowe dla całej gospodarki[3].

Projekt wpisywał się jednocześnie w szerszy trend aktywnej polityki gospodarczej państwa, obserwowany w wielu krajach świata w okresie międzywojennym. Podobnie jak amerykański *New Deal*, opierał się na założeniu, że duże inwestycje

[2] G. Ostasz, *Centralny Okręg Przemysłowy – idea i realizacja*, „Biuletyn Instytutu Pamięci Narodowej" 2024, nr 11, s. 31–43.

[3] Ibidem.

publiczne mogą jednocześnie pobudzać wzrost gospodarczy, ograniczać bezrobocie i wzmacniać potencjał strategiczny państwa[4].

Istotne znaczenie miały również uwarunkowania społeczne. II Rzeczpospolita pozostawała państwem o dominującym charakterze rolniczym. Szczególnie w centralnej i południowo-wschodniej części kraju występowało zjawisko przeludnienia agrarnego, prowadzące do ukrytego bezrobocia, niskiej wydajności gospodarstw rolnych oraz ograniczonych możliwości awansu społecznego. Budowa COP miała stworzyć nowe miejsca pracy poza rolnictwem oraz umożliwić przepływ ludności do rozwijających się ośrodków przemysłowych. Dzięki temu projekt pełnił funkcję nie tylko gospodarczą, ale również społeczną, przyczyniając się do poprawy warunków życia ludności oraz ograniczania napięć społecznych[5].

Jednocześnie inwestycje realizowane w ramach COP miały sprzyjać wyrównywaniu różnic rozwojowych pomiędzy bardziej uprzemysłowionymi regionami zachodnimi a słabiej rozwiniętymi obszarami centralnej i południowo-wschodniej Polski, stając się narzędziem polityki regionalnej i budowy spójności społeczno-gospodarczej państwa.

Realizacja tak ambitnego przedsięwzięcia przekraczała możliwości finansowe państwa. W związku z tym rząd podjął działania mające na celu pozyskanie zagranicznych źródeł finansowania, przede wszystkim we Francji. We wrześniu 1936 roku podpisano polsko-francuską umowę kredytową, na mocy której Polska uzyskała pożyczkę zbrojeniową w wysokości około 2,25 mld franków, co odpowiadało około 480 mln zł. Kredyt miał charakter zarówno finansowy, jak i materiałowy, umożliwiając zakup nowoczesnych maszyn, urządzeń i technologii niezbędnych do rozbudowy przemysłu obronnego. W 1939 roku Polska uzyskała kolejną pożyczkę francuską w wysokości około 430 mln franków[6].

Kluczową rolę w uruchomieniu projektu odegrał wicepremier i minister skarbu Eugeniusz Kwiatkowski, który przedstawił program intensywnej industrializacji państwa oparty na dużych inwestycjach publicznych. Formalną decyzję o budowie COP podjęto 4 lutego 1937 roku. Realizację przedsięwzięcia rozpoczęto jeszcze w tym samym roku na obszarze około 60 tys. km² obejmującym części województw: kieleckiego, krakowskiego, lubelskiego i lwowskiego.

---

4 Ibidem.

5 B. Kaczmar, *Centralny Okręg Przemysłowy 1937-1939*, https:/www.bu.kul.pl/centralny-okreg-przemyslowy-1937-1939-krotka-historia%2Cart_11274.html?utm_source=chatgpt.com [dostęp:06.06.2026].

6 Ibidem.

COP był największym przedsięwzięciem gospodarczym II Rzeczypospolitej oraz jednym z najważniejszych programów strategicznych okresu międzywojennego. Łączył cele gospodarcze i społeczne, przyczyniając się do rozwoju przemysłu, ograniczania bezrobocia, rozbudowy infrastruktury oraz wzmacniania potencjału państwa. Projekt zwiększał również zdolność państwa do funkcjonowania w warunkach kryzysu i wojny poprzez rozbudowę krajowego potencjału produkcyjnego, dywersyfikację bazy przemysłowej oraz lokowanie kluczowych inwestycji w obszarze uznawanym za bezpieczniejszy z punktu widzenia obronności.

W tym znaczeniu COP można postrzegać jako jeden z pierwszych w historii Polski programów wzmacniania odporności państwa, choć pojęcie to nie było wówczas jeszcze stosowane. Rozwój przemysłu, infrastruktury transportowej i energetycznej oraz zwiększanie samowystarczalności gospodarczej miały służyć nie tylko przyspieszeniu modernizacji kraju, lecz również zwiększeniu zdolności państwa do utrzymania ciągłości funkcjonowania w warunkach zagrożenia.

Pomimo że wybuch II wojny światowej uniemożliwił pełną realizację wszystkich założeń programu, COP pozostaje jednym z najbardziej udanych przykładów strategicznej polityki państwa w historii Polski. Projekt ten pokazał, że budowa potencjału narodowego wymaga koncentracji zasobów w sektorach uznawanych za kluczowe dla bezpieczeństwa, rozwoju gospodarczego i modernizacji kraju. Z perspektywy XXI wieku rodzi to pytanie, które obszary gospodarki pełnią obecnie rolę analogiczną do przemysłu ciężkiego, chemicznego i zbrojeniowego rozwijanego w ramach COP.

Transformacja technologiczna i ewolucja źródeł potęgi państw

Analiza doświadczeń COP prowadzi do szerszej refleksji nad zmianą źródeł potęgi państw w XXI wieku. Podobnie jak w latach trzydziestych XX wieku COP koncentrował najbardziej perspektywiczne i strategicznie istotne gałęzie gospodarki II Rzeczypospolitej, tak współcześnie funkcję tę przejmują sektory oparte na wiedzy, danych oraz technologiach cyfrowych.

W pierwszej połowie XX wieku o potencjale gospodarczym i militarnym państwa decydowały przede wszystkim zdolności produkcyjne przemysłu ciężkiego, hutniczego, chemicznego, energetycznego i zbrojeniowego. To właśnie te sektory stanowiły fundament industrializacji, modernizacji sił zbrojnych oraz budowy przewag

strategicznych. Państwo dysponujące rozwiniętym przemysłem mogło skuteczniej prowadzić działania wojenne, szybciej odbudowywać straty oraz zapewniać sobie większą niezależność gospodarczą.

Współcześnie obserwowany jest jednak proces głębokiej transformacji technologicznej, który prowadzi do zmiany struktury światowej gospodarki. Coraz większe znaczenie uzyskują technologie cyfrowe, sztuczna inteligencja, cyberbezpieczeństwo, technologie kosmiczne, systemy autonomiczne, analiza wielkich zbiorów danych oraz infrastruktura przetwarzania informacji. To właśnie w tych sektorach koncentrują się obecnie najważniejsze procesy innowacyjne, przepływy kapitału oraz źródła przewagi konkurencyjnej.

Zmiana ta wynika nie tylko z postępu technologicznego, lecz również z transformacji środowiska bezpieczeństwa. Globalizacja, cyfryzacja oraz rozwój technologii informacyjnych doprowadziły do rozszerzenia przestrzeni rywalizacji strategicznej poza tradycyjne domeny lądową, morską i powietrzną. Coraz większego znaczenia nabierają cyberprzestrzeń, przestrzeń informacyjna oraz infrastruktura danych. W rezultacie współczesne konflikty obejmują nie tylko działania militarne, lecz również operacje informacyjne, cyberataki, presję gospodarczą, działania technologiczne oraz oddziaływanie na infrastrukturę krytyczną państw.

W konsekwencji zmianie ulega również sposób postrzegania potencjału strategicznego państwa. O jego sile decydują dziś nie tylko zasoby materialne i zdolności militarne, lecz także poziom rozwoju technologicznego, zdolność do generowania innowacji, dostęp do danych, kompetencje cyfrowe społeczeństwa oraz odporność infrastruktury teleinformatycznej. Coraz większego znaczenia nabiera także zdolność państwa do zachowania suwerenności technologicznej w obszarach kluczowych dla bezpieczeństwa i rozwoju gospodarczego.

Porównanie historycznego COP z koncepcją *Cyfrowego Okręgu Przemysłowego* pozwala dostrzec fundamentalną zmianę sposobu rozumienia potencjału państwa.

Centralny Okręg Przemysłowy	**Cyfrowy Okręg Przemysłowy**
przemysł ciężki	technologie cyfrowe
infrastruktura fizyczna	infrastruktura danych
produkcja militarna	technologie dual-use

fabryki i zakłady przemysłowe	centra danych i infrastruktura cyfrowa
mobilizacja przemysłowa	mobilizacja cyfrowa
surowce strategiczne	dane i technologie
odporność wojny przemysłowej	odporność wojny informacyjnej
produkcja materiałowa	przetwarzanie informacji

Opracowanie własne

W epoce przemysłowej kluczowe znaczenie miały zdolności produkcyjne, dostęp do surowców oraz infrastruktura materialna. Współcześnie równie istotnym zasobem strategicznym stają się dane, algorytmy, zdolności obliczeniowe oraz infrastruktura cyfrowa. Państwo może utracić zdolność skutecznego funkcjonowania nie tylko wskutek zniszczenia zakładów przemysłowych lub sieci energetycznych, lecz również w wyniku paraliżu systemów teleinformatycznych, utraty dostępu do danych lub zakłócenia funkcjonowania infrastruktury cyfrowej.

Oznacza to również zmianę charakteru odporności państwa. Współczesna odporność obejmuje nie tylko zdolność do odtwarzania potencjału militarnego i gospodarczego, lecz także zdolność do zapewnienia ciągłości funkcjonowania systemów informacyjnych, ochrony danych, przeciwdziałania cyberatakom oraz utrzymania sprawności infrastruktury krytycznej. Coraz większego znaczenia nabierają odporność cybernetyczna, odporność informacyjna oraz odporność technologiczna.

Transformacja ta znajduje odzwierciedlenie również w strukturze światowej gospodarki. Tak jak w latach trzydziestych XX wieku najbardziej perspektywiczne i kapitałochłonne były sektory przemysłu ciężkiego, chemicznego, elektrotechnicznego czy zbrojeniowego, tak obecnie rolę tę przejmują technologie cyfrowe, sztuczna inteligencja, technologie kosmiczne oraz infrastruktura danych. To właśnie wokół tych obszarów koncentrują się współcześnie procesy innowacyjne, przepływy kapitału oraz rozwój nowych modeli gospodarczych.

W tym kontekście zasadne staje się pytanie, czy współczesne państwa nie stoją przed wyzwaniem podobnym do tego, przed którym stanęła II Rzeczpospolita w latach trzydziestych XX wieku. Jeżeli wówczas budowa potencjału państwa wymagała koncentracji zasobów wokół przemysłu ciężkiego, energetyki i przemysłu obronnego, to obecnie analogicznej koncentracji wymagają sektory sztucznej inteligencji,

cyberbezpieczeństwa, technologii kosmicznych, infrastruktury danych oraz technologii podwójnego zastosowania. Odpowiedź na to pytanie wymaga analizy współczesnych przepływów kapitału i koncentracji wartości ekonomicznej, które coraz wyraźniej wskazują na dominującą rolę zaawansowanych technologii w budowie potencjału państw XXI wieku.

Kapitalizacja rynkowa jako wskaźnik koncentracji potencjału technologicznego

Przemiany opisane powyżej znajdują odzwierciedlenie nie tylko w zmianach technologicznych i geopolitycznych, lecz również w strukturze światowej gospodarki. Jednym z najbardziej syntetycznych wskaźników pozwalających ocenić kierunki koncentracji kapitału, innowacji oraz oczekiwań inwestorów jest kapitalizacja rynkowa przedsiębiorstw. Choć nie stanowi ona bezpośredniej miary potencjału państwa, pozwala identyfikować sektory gospodarki uznawane za najbardziej perspektywiczne oraz zdolne do generowania przyszłej wartości ekonomicznej.

Analiza globalnych rynków kapitałowych wskazuje, że w ostatnich dekadach nastąpiło wyraźne przesunięcie głównych strumieni kapitału z tradycyjnych gałęzi przemysłu w kierunku sektorów opartych na wiedzy, danych i zaawansowanych technologiach. Proces ten nie oznacza utraty znaczenia przemysłu obronnego czy przemysłu ciężkiego, lecz wskazuje na pojawienie się nowych obszarów generowania przewag konkurencyjnych oraz budowy potencjału strategicznego państw.

Znaczenie przemysłu obronnego dla bezpieczeństwa państw pozostaje bezdyskusyjne. Doświadczenia wojny rosyjsko-ukraińskiej potwierdziły, że zdolności produkcyjne sektora obronnego stanowią jeden z fundamentów prowadzenia długotrwałych działań wojennych oraz utrzymania zdolności odstraszania. Jednocześnie analiza kapitalizacji największych przedsiębiorstw sektora obronnego wskazuje, że pomimo strategicznego znaczenia branży jej wartość rynkowa pozostaje relatywnie niższa od wycen osiąganych przez największe przedsiębiorstwa technologiczne.

Według danych z czerwca 2026 roku łączna kapitalizacja 52 największych przedsiębiorstw światowego sektora obronnego wynosiła około 1,56 bln USD[7].

[7] https://companiesmarketcap.com/defense-contractors/largest-companies-by-market-cap/ [dostęp:06.06.2026].

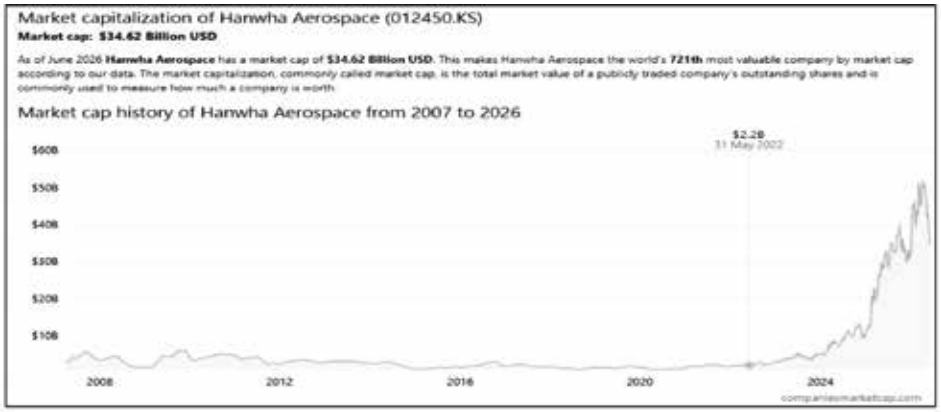
Wśród najwyżej wycenianych podmiotów znajdowały się amerykańskie przedsiębiorstwa *RTX, Honeywell, Lockheed Martin, General Dynamics, Northrop Grumman* i *L3Harris Technologies*, a także europejskie koncerny *Safran, BAE Systems, Rheinmetall, Thales* i *Leonardo*.

Tabela 1. Największe przedsiębiorstwa światowego sektora obronnego

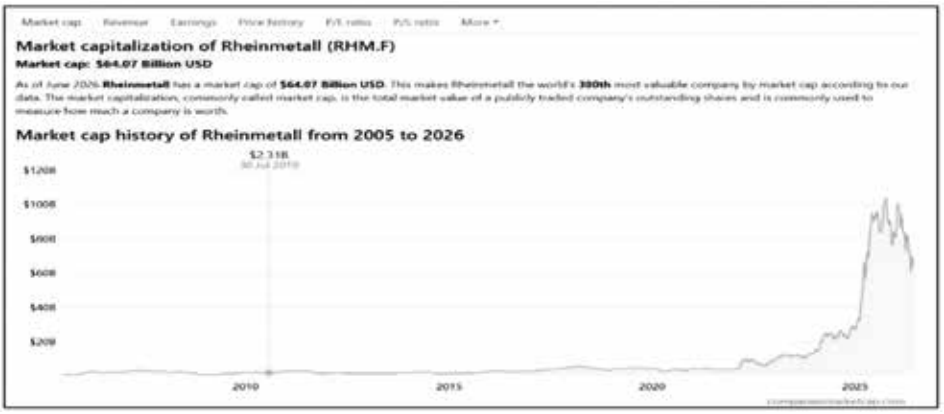
Lp.	Nazwa	Kapitalizacja rynkowa / mld USD	Państwo
1.	RTX	$ 243.73	USA
2.	Safran	$ 135.58	Francja
3.	Honeywell	$ 135, 58	USA
4.	Lockheed Martin	$ 120, 76	USA
5.	General Dynamics	$ 93.68	USA
6.	Northrop Grumman	$ 77.32	USA
7.	BAE Systems	$ 75.56	Wlk. Brytania
8.	Rheinmetall	$ 64,21	Niemcy
9.	L3Harris Technologies	$ 57.34	USA
10.	Thales	$ 55.03	Francja
11.	China State Shipbuilding Corporation (CSSC)	$ 39.99	Chiny
12.	Elbit Systems	$ 38.56	Izrael
13.	Aselsan	$ 35.92	Turcja
14.	Leonardo	$ 34.48	Włochy
15.	Bharat Electronics	$ 31.43	Indie
16.	SAAB AB	$ 30.08	Szwecja
17.	Hindustan Aeronautics	$ 29.70	Indie
18.	Kongsberg Gruppen	$ 28.99	Norwegia
19.	China National Nuclear Power	$ 27.33	Chiny
20.	Dassault Aviation	$ 26.62	Francja
21	CSG N.V. (The Czechoslovak Group)	$ 17.15	Czechy

Opracowanie własne

Pomimo dynamicznego wzrostu wydatków obronnych po 2022 roku kapitalizacja większości przedsiębiorstw sektora zbrojeniowego pozostaje znacząco niższa od wartości osiąganych przez podmioty funkcjonujące w obszarze sztucznej inteligencji, technologii cyfrowych oraz sektora big-tech. Dla przykładu *Lockheed Martin*, producent samolotu wielozadaniowego F-35, osiąga kapitalizację na poziomie około 120 mld USD[8]. Z kolei południowokoreański koncern *Hanwha Aerospace*, producent systemów rakietowych K239 Chunmoo, wykorzystywanych również przez Siły Zbrojne RP, wyceniany jest na około 34,6 mld USD, przy czym jeszcze do niedawna jego wartość rynkowa pozostawała wielokrotnie niższa i nie przekraczała 6 mld USD.



Rys. Kapitalizacja rynkowa *Hanwha Aerospace*, lata 2008-2026[9]



Rys: Kapitalizacja rynkowa *Rheinmetall,* lata 2005-2026[10]

[8] https:/companiesmarketcap.com/defense-contractors/largest-companies-by-market-cap/ [dostęp: 07.06.2026].

[9] https:/companiesmarketcap.com/hanwha-aerospace/marketcap/ [dostęp: 07.06.2026].

[10] https:/companiesmarketcap.com/rheinmetall/marketcap/ [dostęp: 07.06.2026].

Przedstawione dane pokazują, że przedsiębiorstwa sektora obronnego odnotowują obecnie bardzo dynamiczny wzrost wartości rynkowej. Szczególnie widoczne jest to w przypadku *Rheinmetall* oraz *Hanwha Aerospace*, których wyceny wzrosły wielokrotnie w następstwie wojny na Ukrainie oraz zwiększenia wydatków obronnych przez państwa NATO i ich partnerów.

Nie zmienia to jednak faktu, że nawet po uwzględnieniu tej dynamiki kapitalizacja większości przedsiębiorstw zbrojeniowych pozostaje znacząco niższa od wartości osiąganych przez największe podmioty funkcjonujące w sektorze technologii cyfrowych. Oznacza to, że współczesne rynki finansowe dostrzegają największy potencjał wzrostu przede wszystkim w sektorach związanych z technologiami przełomowymi.

Jeszcze wyraźniej tendencja ta widoczna jest w przypadku przedsiębiorstw rozwijających technologie sztucznej inteligencji. Szacuje się, że łączna kapitalizacja 66 największych przedsiębiorstw funkcjonujących w tym sektorze osiągnęła poziom około 21,6 bln USD[11]. Oznacza to, że wartość rynkowa samego sektora sztucznej inteligencji jest blisko czternastokrotnie wyższa od łącznej kapitalizacji światowego przemysłu obronnego notowanego na giełdach papierów wartościowych. Jeżeli do analizy włączone zostałyby również przedsiębiorstwa funkcjonujące w obszarze technologii kosmicznych, półprzewodników, cyberbezpieczeństwa, technologii kwantowych czy infrastruktury chmurowej, skala tej przewagi byłaby jeszcze większa.

Tabela 2. Największe przedsiębiorstwa sektora sztucznej inteligencji

Światowy przemysł sztucznej inteligencji			
Lp.	**Nazwa**	**Kapitalizacja rynkowa / USD**	**Państwo**
1.	NVIDIA	$ 4.967 bln	USA
2.	Apple	$ 4.514 bln	Francja
3.	Alphabet (Google)	$ 4.449 bln	USA
4.	Microsoft	$ 3.095 bln	USA

[11] https:/companiesmarketcap.com/artificial-intelligence/largest-ai-companies-by-marketcap/ [dostęp: 07.06.2026].

5.	Meta Platforms (Facebook)	$ 1.505 bln	USA
6.	Tesla	$ 1.468 bln	USA
7.	Oracle	$ 614.55 mld	Wlk. Brytania
8.	Palantir	$ 324 mld	Niemcy
9.	IBM	$ 267.71 mld	USA
10.	Cambricon Technologies	$ 120.66 mld	Francja
11.	Adobe	$ 101.63 mld	Chiny
12.	CoreWeave	$ 54.76 mld	Izrael
13.	Cerebras Systems	$ 44.14 mld	Turcja
14.	Aurora Innovation	$ 12.37 mld	Włochy
15.	Dynatrace	$ 12.29 mld	Indie
16.	SenseTime	$ 8.58 mld	Szwecja
17.	Tempus AI	$ 8.33 mld	Indie
18.	Mobileye	$ 7.97 mld	Norwegia
19.	UiPath	$ 5.84 mld	Chiny
20.	Presight AI	$ 5.49 mld	Francja

Opracowanie własne

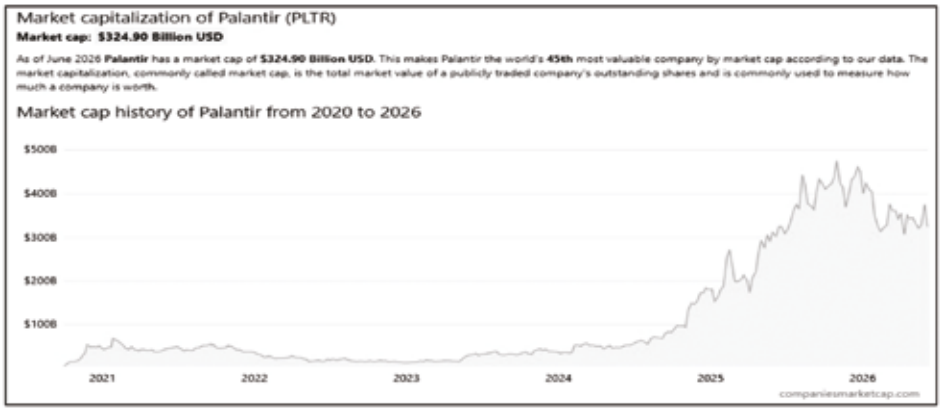
Analiza struktury tego sektora wskazuje jednocześnie na wyraźną dominację Stanów Zjednoczonych. Spośród największych przedsiębiorstw rozwijających technologie sztucznej inteligencji zdecydowana większość należy do podmiotów amerykańskich. Dotyczy to zarówno liczby przedsiębiorstw, jak i ich wartości rynkowej.

Największe podmioty sektora sztucznej inteligencji, takie jak *NVIDIA*, *Apple, Alphabet* czy *Microsoft*, osiągają kapitalizację liczoną w bilionach dolarów. Dla porównania najwyżej sklasyfikowane przedsiębiorstwo chińskie, *Cambricon Technologies*, osiąga kapitalizację około 120 mld USD. Dysproporcja ta pokazuje nie tylko przewagę

technologiczną Stanów Zjednoczonych, lecz również zdolność amerykańskiego systemu gospodarczego do komercjalizacji innowacji, pozyskiwania kapitału oraz tworzenia globalnych ekosystemów technologicznych.

Szczególnie interesującym przykładem ilustrującym zmianę źródeł wartości we współczesnej gospodarce jest porównanie przedsiębiorstw *Palantir Technologies* oraz *Lockheed Martin*.

Palantir Technologies powstał w 2003 roku jako przedsiębiorstwo rozwijające rozwiązania z zakresu analizy danych, sztucznej inteligencji oraz wspomagania procesów decyzyjnych. Wśród klientów firmy znajdują się administracja publiczna, agencje wywiadowcze, siły zbrojne oraz podmioty komercyjne. Kapitalizacja przedsiębiorstwa osiągnęła poziom około 324 mld USD.



Rys. Kapitalizacja rynkowa *Palantir*, lata 2021-2026[12]

Dla porównania Lockheed Martin, przedsiębiorstwo o ponad stuletniej historii, wyceniane jest obecnie na około 120 mld USD.

[12] https:/companiesmarketcap.com/palantir/marketcap/ [dostęp: 07.06.2026].



Rys. Kapitalizacja rynkowa *Lockheed Martin*, lata 1996-2026[13]

Porównanie obu przedsiębiorstw jest interesujące również z perspektywy czasu potrzebnego do budowy ich wartości rynkowej. *Lockheed Martin* wywodzi swoje korzenie z 1912 roku i przez ponad sto lat uczestniczył w tworzeniu przełomowych technologii lotniczych oraz wojskowych. Do dorobku przedsiębiorstwa należą między innymi samoloty P-38 Lightning, U-2, SR-71 Blackbird, F-117 Nighthawk, F-16 oraz F-35[14]. Pomimo ponad stuletniej historii oraz fundamentalnego znaczenia dla bezpieczeństwa narodowego Stanów Zjednoczonych kapitalizacja przedsiębiorstwa pozostaje niemal trzykrotnie niższa od wyceny *Palantira*. Z powyższego wynika, że firma funkcjonująca od niespełna ćwierćwiecza, opierająca swoją działalność przede wszystkim na danych, oprogramowaniu i sztucznej inteligencji, osiągnęła wartość rynkową przewyższającą jednego z największych producentów uzbrojenia na świecie.

Nie identyfikuje to oczywiście spadku znaczenia przemysłu obronnego. Przeciwnie, doświadczenia współczesnych konfliktów zbrojnych potwierdzają jego kluczową rolę dla bezpieczeństwa państw. Porównanie to pokazuje jednak zmianę struktury światowej gospodarki oraz przesunięcie głównych obszarów koncentracji kapitału w kierunku sektorów opartych na wiedzy, danych i technologiach przełomowych.

Przedstawione dane prowadzą do szerszego wniosku dotyczącego ewolucji źródeł potęgi państw. Kapitalizacja przedsiębiorstw stanowi bowiem nie tylko miernik ich wartości ekonomicznej, lecz również pośredni wskaźnik zdolności państwa do tworzenia innowacji, przyciągania inwestycji, rozwijania przełomowych

[13] https:/companiesmarketcap.com/lokheedmartin/marketcap/ [dostęp: 07.06.2026].

[14] R. Aversa, B. Akash, R. Bucinell, A. Apicella, F.I. Petrescu, *Lockheed Martin – A Short Review*, „Journal of Aircraft and Spacecraft Technology", 2017, nr 1, https:/papers.ssrn.com/sol3/papers.cfm?abstract_id=3073975 [dostęp: 07.06.2026].

technologii oraz budowy przewag strategicznych. Współcześnie potencjał państwa coraz częściej determinowany jest nie tylko przez wielkość produkcji przemysłowej, zasoby naturalne czy potencjał militarny, lecz również przez zdolność funkcjonowania w sektorach wysokich technologii. Dane, algorytmy, sztuczna inteligencja, cyberbezpieczeństwo oraz technologie dual-use stają się zasobami strategicznymi porównywalnymi z rolą, jaką w XX wieku odgrywały stal, energia czy zdolności produkcyjne przemysłu ciężkiego.

Powyższe obserwacje znajdują odzwierciedlenie również w strategicznym myśleniu największych mocarstw. Jak podkreśla Jake Sullivan, doradca ds. bezpieczeństwa narodowego prezydenta Stanów Zjednoczonych w latach 2021-2025, kluczowymi technologiami determinującymi pozycję państw w XXI wieku są przede wszystkim sztuczna inteligencja, kwantowe systemy informacyjne, informatyka oraz półprzewodniki[15]. W jego ocenie zdolność do rozwijania i kontrolowania tych obszarów będzie miała zasadniczy wpływ zarówno na bezpieczeństwo narodowe, jak i konkurencyjność gospodarczą państw.

Sullivan wskazuje, że sztuczna inteligencja powinna być wykorzystywana przez Stany Zjednoczone do wzmacniania bezpieczeństwa narodowego, zwiększania dobrobytu gospodarczego oraz utrzymywania przewagi technologicznej nad rywalami strategicznymi. Niezależnie od oceny proponowanych przez niego instrumentów politycznych, sam sposób definiowania technologii jako narzędzia oddziaływania geopolitycznego pokazuje, jak istotną rolę odgrywają one obecnie w kształtowaniu siły państw. Co więcej, Sullivan zwraca uwagę, że rywalizacja technologiczna nie dotyczy wyłącznie aspektów gospodarczych. Istotne znaczenie ma również to, które państwa i które systemy technologiczne staną się dominującymi standardami światowymi. Od tego zależeć będzie nie tylko podział korzyści ekonomicznych, lecz również kształt przyszłego porządku cyfrowego, norm regulacyjnych oraz wartości przenoszonych przez technologie na skalę globalną[16].

Dowodzi to, że współczesna polityka bezpieczeństwa i polityka przemysłowa coraz silniej się przenikają. Państwa zdolne do budowy własnych kompetencji technologicznych uzyskują jednocześnie przewagę gospodarczą, militarną i polityczną.

---

[15] J. Sullivan, *What It Will Take to Gain the Advantage Over China*, „Foreign Affairs", May/June 2026, https://www.foreignaffairs.com/united-states/tech-high-ground-jake-sullivan [dostęp: 06.06.2026].

[16] J. Sullivan, T. Feldman, *Geopolitics in the Age of Artificial Intelligence: Strategy and Power in an Uncertain AI Future*, „Foreign Affairs", 27.01.2026, https://www.foreignaffairs.com/united-states/geopolitics-age-artificial-intelligence [dostęp: 07.06.2026].

W tym sensie obserwowana koncentracja kapitału w sektorach zaawansowanych technologii stanowi nie tylko zjawisko ekonomiczne, lecz również jeden z kluczowych wymiarów współczesnej rywalizacji strategicznej.

Przedstawione tendencje rodzą pytanie o to, w jaki sposób państwo może świadomie budować własny potencjał technologiczny oraz koncentrować zasoby w sektorach uznawanych za newralgiczne dla przyszłego rozwoju i bezpieczeństwa. Odpowiedzią na to wyzwanie może być koncepcja *Cyfrowego Okręgu Przemysłowego*, stanowiąca współczesną adaptację logiki, która legła u podstaw budowy COP w latach trzydziestych XX wieku.

Cyfrowy Okręg Przemysłowy jako nowy model budowy potencjału państwa

Analiza doświadczeń COP oraz współczesnych procesów koncentracji kapitału prowadzi do wniosku, że państwa odnoszące sukces w długiej perspektywie strategicznej potrafią identyfikować i wspierać sektory gospodarki o kluczowym znaczeniu dla przyszłego rozwoju. W epoce COP o sile państwa decydowały przede wszystkim zdolności przemysłowe i produkcyjne. Obecnie coraz większe znaczenie zyskują zdolności technologiczne, obejmujące technologie cyfrowe, sztuczną inteligencję, cyberbezpieczeństwo, technologie kosmiczne oraz rozwiązania dual-use.

Przedstawione wcześniej dane dotyczące kapitalizacji przedsiębiorstw wskazują, że największe procesy akumulacji kapitału, innowacji oraz kompetencji technologicznych zachodzą obecnie właśnie w tych sektorach. Oznacza to, że budowa długoterminowego potencjału gospodarczego i bezpieczeństwa państwa wymaga stworzenia warunków umożliwiających rozwój własnych zdolności technologicznych oraz aktywne uczestnictwo w globalnej rywalizacji innowacyjnej.

W tym kontekście zasadne wydaje się sformułowanie koncepcji *Cyfrowego Okręgu Przemysłowego* jako współczesnej adaptacji logiki, która legła u podstaw budowy COP. Nie oznacza to prostego przeniesienia historycznych rozwiązań do realiów XXI wieku, lecz wykorzystanie tej samej filozofii działania państwa polegającej na koncentracji zasobów w obszarach uznawanych za kluczowe dla bezpieczeństwa, rozwoju gospodarczego oraz budowy przewag strategicznych.

Cyfrowy Okręg Przemysłowy można zdefiniować jako zintegrowany system rozwoju potencjału technologicznego państwa obejmujący infrastrukturę cyfrową,

działalność badawczo-rozwojową, przemysł wysokich technologii, administrację publiczną, środowisko akademickie oraz sektor prywatny. Jego podstawowym celem byłoby stworzenie warunków umożliwiających koncentrację kapitału, wiedzy, kompetencji oraz inwestycji w obszarach uznawanych za strategiczne z punktu widzenia bezpieczeństwa państwa oraz jego konkurencyjności gospodarczej.

W przeciwieństwie do historycznego COP współczesny model nie musiałby posiadać wyłącznie charakteru geograficznego. O ile COP był skoncentrowany na określonym obszarze terytorialnym, o tyle *Cyfrowy Okręg Przemysłowy* może funkcjonować jako rozproszona sieć wzajemnie powiązanych podmiotów tworzących narodowy ekosystem technologiczny. Jego spójność wynikałaby nie ze wspólnej lokalizacji, lecz z integracji infrastrukturalnej, organizacyjnej, badawczej oraz technologicznej.

Podstawę funkcjonowania współczesnej gospodarki cyfrowej stanowi infrastruktura umożliwiająca gromadzenie, przetwarzanie i analizowanie danych. W epoce przemysłowej podobną rolę odgrywały elektrownie, linie kolejowe, sieci transportowe oraz zakłady przemysłowe. W warunkach XXI wieku strategicznego znaczenia nabierają:

- centra danych,
- krajowe zasoby chmury obliczeniowej,
- infrastruktura telekomunikacyjna,
- sieci transmisji danych,
- systemy przetwarzania informacji,
- zasoby wysokowydajnych mocy obliczeniowych.

Posiadanie własnych zdolności w tym zakresie staje się warunkiem zachowania suwerenności technologicznej oraz odporności państwa na zakłócenia zewnętrzne.

Sztuczna inteligencja staje się obecnie jednym z najważniejszych czynników wpływających na rozwój gospodarczy, efektywność administracji publicznej oraz zdolności obronne państw. Jej znaczenie wykracza daleko poza sektor komercyjny. Technologie te znajdują zastosowanie między innymi w:

- analizie danych wywiadowczych,
- systemach dowodzenia i kierowania,
- cyberbezpieczeństwie,
- medycynie,

- logistyce,
- zarządzaniu kryzysowym,
- przemyśle i energetyce.

Państwa zdolne do rozwoju własnych kompetencji w obszarze sztucznej inteligencji uzyskują przewagę nie tylko gospodarczą, lecz również militarną i polityczną.

Jedną z najważniejszych cech współczesnej rewolucji technologicznej jest postępujące zacieranie się granicy pomiędzy technologiami cywilnymi i wojskowymi. Coraz większa liczba rozwiązań posiada charakter podwójnego zastosowania (dual-use), co oznacza możliwość ich wykorzystania zarówno na potrzeby gospodarki, jak i bezpieczeństwa państwa. Dotyczy to przede wszystkim:

- sztucznej inteligencji,
- technologii satelitarnych,
- systemów autonomicznych,
- bezzałogowych platform powietrznych,
- zaawansowanej elektroniki,
- cyberbezpieczeństwa,
- technologii kwantowych,
- analityki danych.

Doświadczenia wojny rosyjsko-ukraińskiej pokazują, że technologie rozwijane pierwotnie na potrzeby rynku cywilnego mogą w krótkim czasie uzyskać kluczowe znaczenie militarne.

Historia rozwoju największych przedsiębiorstw technologicznych pokazuje, że ich sukces nie był wyłącznie rezultatem działalności biznesowej. Kluczową rolę odegrały inwestycje w badania naukowe, edukację oraz rozwój kapitału ludzkiego. W przypadku *Cyfrowego Okręgu Przemysłowego* szczególne znaczenie powinny posiadać:

- uczelnie techniczne,
- instytuty badawcze,
- centra transferu technologii,
- laboratoria badawczo-rozwojowe,
- programy wspierające komercjalizację wyników badań.

To właśnie zdolność przekształcania wiedzy w rozwiązania technologiczne stanowi jeden z głównych czynników decydujących o konkurencyjności współczesnych gospodarek.

Doświadczenia historyczne pokazują, że przełomowe projekty modernizacyjne rzadko powstają wyłącznie w wyniku działania mechanizmów rynkowych. Dotyczyło to zarówno budowy COP, jak i wielu współczesnych technologii stanowiących fundament gospodarki cyfrowej. W obu przypadkach kluczową rolę odgrywało państwo, które identyfikowało strategiczne kierunki rozwoju, mobilizowało zasoby finansowe oraz tworzyło warunki instytucjonalne sprzyjające realizacji długoterminowych przedsięwzięć o wysokim poziomie ryzyka.

Aktualnie również państwa uznawane za zwolenników liberalnego modelu gospodarczego coraz częściej prowadzą aktywną politykę przemysłową i technologiczną. Szczególnie widoczne jest to w Stanach Zjednoczonych, gdzie rozwój sektora sztucznej inteligencji, półprzewodników, technologii kosmicznych czy zaawansowanych systemów cyfrowych opiera się na ścisłej współpracy pomiędzy sektorem prywatnym a państwem. Wsparcie to obejmuje nie tylko finansowanie badań i rozwoju, lecz również działania regulacyjne, polityczne, dyplomatyczne oraz ochronę strategicznych przewag technologicznych. W literaturze przedmiotu coraz częściej podkreśla się, że rezygnacja państwa z aktywnego uczestnictwa w kształtowaniu rozwoju sztucznej inteligencji i technologii cyfrowych oznaczałaby de facto rezygnację z wpływu na jeden z najważniejszych procesów determinujących przyszły układ sił gospodarczych i geopolitycznych. W konsekwencji polityka technologiczna staje się integralnym elementem polityki bezpieczeństwa państwa.

W tym kontekście pojawia się również koncepcja określana mianem „Manhattan Project 2.0". Odwołuje się ona do doświadczeń amerykańskiego programu budowy broni atomowej realizowanego podczas II wojny światowej, który dzięki ścisłej współpracy państwa, środowiska naukowego oraz przedsiębiorstw prywatnych doprowadził do powstania technologii zapewniającej Stanom Zjednoczonym długotrwałą przewagę strategiczną[17].. Współcześnie analogiczne postulaty odnoszone są do rozwoju sztucznej inteligencji, technologii kwantowych, półprzewodników oraz innych technologii przełomowych, uznawanych za kluczowe dla przyszłej pozycji gospodarczej i militarnej państw.

[17] B. Buchanan, T. Collins, *The AI Grand Bargain: What America Needs to Win the Innovation Race*, „Foreign Affairs", 21.11.2025, https://www.foreignaffairs.com/united-states/artificial-intelligence-grand-bargain-buchanan-collins [dostęp: 05.06.2026]. J. Sullivan, T. Feldman, *Geopolitics in the Age of Artificial Intelligence: Strategy and Power in an Uncertain AI Future*, op. cit.

Przykład ten pokazuje, że rywalizacja technologiczna coraz częściej postrzegana jest przez największe mocarstwa w kategoriach strategicznych. Oznacza to odejście od przekonania, że rozwój najbardziej zaawansowanych technologii może być pozostawiony wyłącznie mechanizmom rynkowym. Coraz częściej przyjmuje się bowiem, że budowa przewagi technologicznej wymaga długoterminowego współdziałania państwa, sektora nauki oraz przedsiębiorstw prywatnych. W tym sensie współczesne programy rozwoju sztucznej inteligencji i technologii cyfrowych można traktować jako odpowiednik wielkich projektów przemysłowych XX wieku, których celem było jednoczesne wzmacnianie bezpieczeństwa państwa, potencjału gospodarczego oraz pozycji międzynarodowej.

Nie należy jednak z tego wnioskować, że państwo powinno zastępować mechanizmy rynkowe lub samodzielnie realizować proces rozwoju technologicznego. Doświadczenia państw będących liderami innowacji wskazują, że najskuteczniejsze rezultaty osiągane są wówczas, gdy państwo tworzy warunki sprzyjające rozwojowi przedsiębiorczości, badań naukowych oraz komercjalizacji nowych technologii. Rola państwa powinna koncentrować się przede wszystkim na kształtowaniu stabilnego i przewidywalnego otoczenia regulacyjnego, wspieraniu działalności badawczo-rozwojowej, rozwijaniu infrastruktury cyfrowej oraz tworzeniu warunków sprzyjających współpracy pomiędzy światem nauki, administracją publiczną i sektorem prywatnym. Szczególne znaczenie ma również inicjowanie oraz współfinansowanie strategicznych programów inwestycyjnych w obszarach uznawanych za kluczowe dla bezpieczeństwa i konkurencyjności państwa[18].

W takim modelu państwo nie pełni funkcji głównego producenta technologii, lecz występuje w roli integratora narodowego ekosystemu technologicznego. Jego zadaniem jest identyfikowanie sektorów o strategicznym znaczeniu, koordynowanie działań różnych uczestników rynku, ograniczanie barier rozwojowych oraz tworzenie warunków umożliwiających koncentrację kapitału, wiedzy i kompetencji w obszarach decydujących o przyszłej pozycji gospodarczej i bezpieczeństwie państwa. Taką właśnie funkcję pełnił w latach trzydziestych XX wieku COP. Współcześnie analogiczną rolę mogłaby odgrywać koncepcja *Cyfrowego Okręgu Przemysłowego*, której celem byłoby stworzenie warunków dla rozwoju technologii cyfrowych, sztucznej inteligencji, cyberbezpieczeństwa, infrastruktury danych oraz innych technologii przełomowych stanowiących fundament bezpieczeństwa i rozwoju państwa w XXI wieku.

[18] S. Elbaum, S. Mallaby, *The AI Trilemma: How to Regulate a Revolutionary Technology*, „Foreign Affairs", 13.02.2026, https://www.foreignaffairs.com/united-states/ai-trilemma [dostęp: 04.06.2026].

Cyfrowy Okręg Przemysłowy a bezpieczeństwo państwa

Znaczenie *Cyfrowego Okręgu Przemysłowego* wykracza daleko poza sferę gospodarczą. Współcześnie rozwój technologiczny staje się jednym z podstawowych determinantów bezpieczeństwa narodowego, a zdolność państwa do tworzenia, pozyskiwania i ochrony kluczowych technologii coraz częściej decyduje o jego pozycji międzynarodowej, odporności oraz zdolnościach obronnych.

Państwo zdolne do ochrony własnej infrastruktury cyfrowej, rozwijania krajowych kompetencji technologicznych oraz utrzymania kontroli nad strategicznymi zasobami danych uzyskuje większą zdolność reagowania na zagrożenia militarne, hybrydowe, cybernetyczne i informacyjne. W tym ujęciu *Cyfrowy Okręg Przemysłowy* może pełnić funkcję instrumentu wzmacniania odporności państwa, bezpieczeństwa cybernetycznego, suwerenności technologicznej, zdolności obronnych, konkurencyjności gospodarki oraz potencjału innowacyjnego.

Znaczenie tego procesu będzie prawdopodobnie rosło. Prognozy środowiska naukowego i wojskowego wskazują, że w najbliższych dekadach należy spodziewać się dalszego przyspieszenia rozwoju przełomowych technologii. Wynika to przede wszystkim z dojrzewania istniejących rozwiązań technologicznych oraz powstawania nowych, hybrydowych technologii łączących osiągnięcia wielu dziedzin nauki i techniki.

Już kilka lat temu środowisko eksperckie związane z Siłami Zbrojnymi RP identyfikowało siedem kluczowych technologii przełomowych, które mogą w największym stopniu oddziaływać na przyszłe środowisko bezpieczeństwa. Zaliczono do nich sztuczną inteligencję, dane i zdolności obliczeniowe, autonomię systemów, technologie kwantowe, biotechnologię i udoskonalanie człowieka, technologie hipersoniczne oraz technologie kosmiczne. Zakładano jednocześnie, że największe znaczenie będą miały nie pojedyncze technologie, lecz powstające pomiędzy nimi hybrydy technologiczne generujące nowe zdolności operacyjne i gospodarcze[19].

Mechanizm ten można zobrazować przykładem smartfona. Połączenie telefonu komórkowego, komputera osobistego, dostępu do Internetu, ekranów dotykowych oraz aplikacji cyfrowych doprowadziło do powstania całkowicie nowego ekosystemu gospodarczego, który wywarł wpływ na niemal wszystkie sektory gospodarki. Podobny proces może zachodzić obecnie w odniesieniu do sztucznej inteligencji,

[19] *Rozwój technologii przełomowych*, seminarium w ramach NUP, Centrum Doktryn i Szkolenia Sił Zbrojnych RP, 2022.

technologii kosmicznych, autonomii systemów, cyberbezpieczeństwa czy technologii kwantowych. W rezultacie należy spodziewać się dalszego wzrostu wartości ekonomicznej przedsiębiorstw funkcjonujących w tych obszarach oraz postępującej koncentracji kapitału w sektorze technologii cyfrowych.

Cyfrowa transformacja niesie jednak nie tylko szanse, lecz również nowe zagrożenia. Rozwój technologii cyfrowych może prowadzić do pogłębiania zależności technologicznych oraz ograniczania autonomii strategicznej państw. Jednym z najważniejszych wyzwań pozostaje dominacja globalnych korporacji technologicznych kontrolujących znaczną część infrastruktury cyfrowej wykorzystywanej przez państwa i gospodarki. Wiele krajów europejskich pozostaje uzależnionych od zagranicznych dostawców usług chmurowych, infrastruktury telekomunikacyjnej, systemów operacyjnych, platform cyfrowych oraz technologii sztucznej inteligencji.

Uzależnienie od zewnętrznych podmiotów technologicznych może prowadzić do ograniczenia swobody działania państwa w obszarze ochrony danych, bezpieczeństwa infrastruktury krytycznej, niezależności decyzyjnej oraz odporności systemów teleinformatycznych. W warunkach napięć geopolitycznych lub kryzysów międzynarodowych dostęp do określonych technologii może stać się przedmiotem nacisku politycznego, gospodarczego lub strategicznego.

Dodatkowo infrastruktura cyfrowa staje się współcześnie jednym z podstawowych celów operacji prowadzonych zarówno przez państwa, jak i podmioty niepaństwowe. Ataki na systemy energetyczne, administrację publiczną, sektor finansowy czy sieci telekomunikacyjne mogą prowadzić do poważnej destabilizacji funkcjonowania państwa bez konieczności użycia siły militarnej w jej klasycznym rozumieniu.

Istotnym zagrożeniem pozostaje również wojna informacyjna. Rozwój mediów społecznościowych, narzędzi analitycznych oraz sztucznej inteligencji umożliwia prowadzenie zaawansowanych operacji wpływu obejmujących dezinformację, manipulację społeczną, polaryzację społeczną oraz oddziaływanie na procesy demokratyczne. W tym kontekście *Dolina Cieni* symbolizuje negatywny scenariusz transformacji cyfrowej, w którym państwo traci kontrolę nad strategicznymi technologiami, infrastrukturą i danymi, stając się podatne na presję zewnętrzną.

W odpowiedzi na rosnące zagrożenia coraz większego znaczenia nabiera pojęcie suwerenności technologicznej. W praktyce oznacza to zdolność państwa do kontrolowania kluczowych technologii, ochrony infrastruktury cyfrowej, rozwijania własnych kompetencji technologicznych, zapewnienia bezpieczeństwa danych oraz utrzymania ciągłości działania systemów krytycznych.

Suwerenność technologiczna nie oznacza pełnej samowystarczalności, lecz zdolność do ograniczania strategicznych zależności oraz utrzymania kontroli nad technologiami kluczowymi dla bezpieczeństwa państwa. Znaczenie tego zagadnienia podkreślają zarówno NATO, które uznaje cyberprzestrzeń za pełnoprawną domenę operacyjną, jak i Unia Europejska rozwijająca koncepcję autonomii strategicznej w obszarach półprzewodników, sztucznej inteligencji, cyberbezpieczeństwa i infrastruktury cyfrowej. Coraz wyraźniej dostrzega się bowiem, że bezpieczeństwo państwa jest ściśle powiązane z poziomem jego rozwoju technologicznego.

Dobrym przykładem takiego podejścia jest Wielka Brytania, która traktuje dostęp do kluczowych technologii jako element bezpieczeństwa narodowego. Brytyjska strategia opiera się na trzech filarach: rozwoju krajowych zdolności badawczo-przemysłowych, przyspieszeniu wdrażania nowych technologii w sektorach strategicznych oraz pogłębianiu współpracy z najbliższymi partnerami technologicznymi, przede wszystkim ze Stanami Zjednoczonymi. Szczególne znaczenie przypisuje się sztucznej inteligencji, której rozwój wspierany jest poprzez specjalne programy inwestycyjne i tworzenie dedykowanych stref wzrostu technologicznego[20].

Podsumowanie

Przeprowadzona analiza potwierdza, że współczesna transformacja technologiczna prowadzi do zasadniczej zmiany źródeł potęgi państw. O ile w epoce industrialnej podstawę rozwoju gospodarczego, zdolności obronnych oraz pozycji międzynarodowej stanowiły przemysł ciężki, energetyka i potencjał produkcyjny, o tyle w XXI wieku coraz większego znaczenia nabierają technologie cyfrowe, sztuczna inteligencja, dane, zdolności obliczeniowe, cyberbezpieczeństwo oraz technologie podwójnego zastosowania.

Analiza doświadczeń związanych z budową COP prowadzi do wniosku, że sukces tego przedsięwzięcia wynikał nie tylko z realizacji konkretnych inwestycji przemysłowych, lecz przede wszystkim z trafnej identyfikacji sektorów mających kluczowe znaczenie dla bezpieczeństwa i rozwoju państwa. W latach trzydziestych XX wieku były to przemysł ciężki, chemiczny, energetyczny i zbrojeniowy. Współcześnie

[20] *National Security Strategy 2025. Security for the British People in a Dangerous Worlds*, s.47, https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world [dostęp: 07.06.2026].

analogiczną rolę coraz wyraźniej przejmują technologie cyfrowe oraz szeroko rozumiany sektor przełomowych technologii.

Uzyskane wyniki pozwalają udzielić odpowiedzi na postawione pytania badawcze. Po pierwsze, technologie cyfrowe stają się jednym z głównych źródeł przewagi strategicznej państw. Skala koncentracji kapitału w sektorach sztucznej inteligencji, technologii cyfrowych i usług opartych na danych wskazuje, że właśnie tam lokowane są obecnie największe zasoby finansowe, badawczo-rozwojowe i innowacyjne. Po drugie, kontrola nad kluczowymi technologiami, danymi oraz infrastrukturą cyfrową posiada fundamentalne znaczenie dla bezpieczeństwa narodowego. Cyberprzestrzeń i infrastruktura cyfrowa stają się zarówno strategicznym zasobem państwa, jak i potencjalnym celem działań przeciwnika.

Po trzecie, krajowy potencjał technologiczny wpływa bezpośrednio na zdolność państwa do zapewnienia bezpieczeństwa, odporności i ciągłości funkcjonowania w warunkach kryzysu. Współczesna odporność obejmuje bowiem nie tylko potencjał militarny, lecz również odporność technologiczną, informacyjną i cybernetyczną. Po czwarte, Polska dysponuje potencjałem rozwoju kompetencji technologicznych, jednak utrzymanie suwerenności technologicznej wymaga długofalowej i skoordynowanej polityki państwa obejmującej inwestycje w badania i rozwój, kapitał ludzki, infrastrukturę cyfrową oraz sektor wysokich technologii.

Przeprowadzona analiza pozwala pozytywnie zweryfikować przyjętą tezę badawczą. W warunkach narastającej rywalizacji technologicznej zdolność do tworzenia, rozwijania i ochrony kluczowych technologii staje się jednym z podstawowych wyznaczników bezpieczeństwa i pozycji państwa w środowisku międzynarodowym. W konsekwencji *Cyfrowy Okręg Przemysłowy* należy postrzegać nie tylko jako projekt gospodarczy, lecz przede wszystkim jako instrument budowy potencjału strategicznego państwa. Tak jak COP był symbolem modernizacji II Rzeczypospolitej, tak *Cyfrowy Okręg Przemysłowy* może stać się odpowiedzią na wyzwania epoki cyfrowej, w której o sile państw coraz częściej decydują dane, algorytmy, wiedza i technologie przełomowe.

Bibliografia

Aversa R., Akash B., Bucinell R., Apicella A., Petrescu F.I., *Lockheed Martin – A Short Review*, „Journal of Aircraft and Spacecraft Technology", 2017, nr 1, https:/papers.ssrn.com/sol3/papers.cfm?abstract_id=3073975 [dostęp: 07.06.2026].

Buchanan B., Collins T., *The AI Grand Bargain: What America Needs to Win the Innovation Race*, „Foreign Affairs", 21.11.2025, https:/www.foreignaffairs.com/united-states/artificial--intelligence-grand-bargain-buchanan-collins [dostęp: 05.06.2026].

Duch W., *Centralny Okręg Przemysłowy (COP) – geneza, realizacja i znaczenie największego programu inwestycyjnego II RP*, https:/historia.org.pl/2025/03/01/centralny-okreg-przemyslowy-cop-geneza-realizacja-i-znaczenie-najwiekszego-programu-inwestycyjnego--ii-rp/?utm_source=chatgpt.com [dostęp: 06.06.2025].

Elbaum S., Mallaby S., *The AI Trilemma: How to Regulate a Revolutionary Technology*, „Foreign Affairs", 13.02.2026, https:/www.foreignaffairs.com/united-states/ai-trilemma [dostęp: 04.06.2026].

Kaczmar B., *Centralny Okręg Przemysłowy 1937-1939*, https:/www.bu.kul.pl/centralny-okreg-przemyslowy-1937-1939-krotka-historia%2Cart_11274.html?utm_source=chatgpt.com [dostęp:06.06.2026].

National Security Strategy 2025. Security for the British People in a Dangerous Worlds, s. 47, https:/www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world [dostęp: 07.06.2026].

Ostasz G., *Centralny Okręg Przemysłowy – idea i realizacja*, „Biuletyn Instytutu Pamięci Narodowej" 2024, nr 11.

Sullivan J., Feldman T., *Geopolitics in the Age of Artificial Intelligence: Strategy and Power in an Uncertain AI Future*, „Foreign Affairs", 27.01.2026, https:/www.foreignaffairs.com/united-states/geopolitics-age-artificial-intelligence [dostęp: 07.06.2026].

Sullivan J., *What It Will Take to Gain the Advantage Over China*, „Foreign Affairs", May/June 2026, https:/www.foreignaffairs.com/united-states/tech-high-ground-jake-sullivan [dostęp:06.06.2026].

https:/companiesmarketcap.com/artificial-intelligence/largest-ai-companies-by-marketcap/ [dostęp: 07.06.2026].

https:/companiesmarketcap.com/defense-contractors/largest-companies-by-market-cap/ [dostęp:06.06.2026].

https:/companiesmarketcap.com/hanwha-aerospace/marketcap/ [dostęp: 07.06.2026].

https:/companiesmarketcap.com/lokheedmartin/marketcap/ [dostęp: 07.06.2026].

https:/companiesmarketcap.com/palantir/marketcap/ [dostęp: 07.06.2026].

https:/companiesmarketcap.com/rheinmetall/marketcap/ [dostęp: 07.06.2026].

Cyberpotęga czy cyfrowe peryferia? Strategia dla ambitnej Polski

Dariusz Stefaniuk

Abstrakt

Artykuł analizuje strategiczną alternatywę: cyberpotęga lub cyfrowe peryferia. Autor ocenia Strategię Cyfryzacji Państwa do 2035 roku i stawia pytanie, czy Polska chce być jedynie sprawnym użytkownikiem cudzych technologii, czy aktywnym twórcą własnych. Omawia kluczowe wymiary suwerenności cyfrowej: własne modele językowe, krajową infrastrukturę obliczeniową, bezpieczeństwo danych, regulacje AI i ekosystem polskich firm technologicznych.

Słowa kluczowe: suwerenność cyfrowa, cyberpotęga, strategia cyfrowa, sztuczna inteligencja, cyfryzacja państwa, infrastruktura obliczeniowa

1. Wprowadzenie: cyfrowa suwerenność jako element siły państwa

Pytanie postawione w tytule naszego panelu – „cyberpotęga czy cyfrowe peryferia?" – nie jest publicystyczną przesadą. To realny wybór strategiczny, przed którym stoi Polska.

W XX wieku o sile państwa decydowały przede wszystkim przemysł, armia, energetyka, surowce i infrastruktura transportowa. W XXI wieku do tej listy dochodzą nowe filary: dane, sztuczna inteligencja, cyberbezpieczeństwo, własne kompetencje technologiczne, odporna infrastruktura cyfrowa oraz zdolność państwa do ochrony obywateli w cyberprzestrzeni.

Państwo, które nie kontroluje swoich danych, nie rozumie algorytmów, nie ma własnych kompetencji w cyberbezpieczeństwie i nie inwestuje w infrastrukturę obliczeniową, nie będzie w pełni suwerenne. Może mieć nowoczesne aplikacje, ale pozostanie zależne od cudzych platform, cudzych modeli i cudzych centrów decyzyjnych.

Cyfrowe peryferia to nie kraj bez Internetu. To kraj, który używa technologii, lecz nie potrafi ich tworzyć, kontrolować ani skalować.

2. Strategia Cyfryzacji Państwa: dobry kierunek, ale potrzebna większa ambicja

Strategia Cyfryzacji Państwa do 2035 roku ma wyznaczać wieloletnią perspektywę transformacji cyfrowej i poprawiać jakość życia obywateli. To słuszne założenie. Państwo cyfrowe powinno być prostsze, szybsze i bardziej dostępne.

Kluczowe pytanie brzmi jednak: czy strategia ma uczynić Polskę jedynie sprawnym użytkownikiem cudzych technologii, czy państwem, które rozwija własne zdolności? Sama informatyzacja usług publicznych nie wystarczy. Potrzebujemy także własnej infrastruktury, zasobów danych, ośrodków badawczych, polskich produktów cyfrowych i kapitału zdolnego je skalować.

Polska nie może być wyłącznie rynkiem zbytu dla globalnych gigantów technologicznych. Musi być państwem, które potrafi tworzyć, chronić i wykorzystywać własne zasoby cyfrowe.

2.1. Infrastruktura i cyfrowa solidarność

Rozwój sieci szerokopasmowych, likwidacja białych plam, dostęp do 5G i przygotowania do 6G są warunkiem nowoczesnej gospodarki. Z perspektywy Polski lokalnej szczególnie ważne jest, aby transformacja cyfrowa nie pogłębiała podziału między największymi miastami a mniejszymi miejscowościami.

Skala zmiany jest już widoczna nie tylko w metropoliach. Według danych systemu SIDUSIS na 31 marca 2026 roku w Polsce zidentyfikowano 9 270 432 punkty adresowe, z których 8 001 144 – ponad 86% – znajdowało się w zasięgu stacjonarnego internetu szerokopasmowego. Bez jakiegokolwiek zasięgu pozostawało 1 269 288 punktów adresowych. Technologia światłowodowa odpowiadała za ponad 74% wszystkich raportowanych zasięgów. Oznacza to, że światłowód przestał być

infrastrukturą dostępną wyłącznie w centrach największych miast: dociera dziś do małych miast, gmin i coraz większej liczby wsi.

Postęp nie oznacza jednak zakończenia inwestycji. Na koniec marca 2026 roku wykazywano 2 040 688 tzw. białych plam NGA, czyli adresów bez dostępu do sieci zapewniającej parametry sieci bardzo wysokiej przepustowości. Białe plamy są rozproszone po całym kraju, ale najtrudniejsze do likwidacji pozostają przede wszystkim obszary wiejskie, słabo zaludnione, górskie i położone z dala od istniejących węzłów sieci. Tam koszt doprowadzenia łącza do pojedynczego domu jest znacznie wyższy, a inwestycja często nie jest opłacalna bez wsparcia publicznego.

Dobrym przykładem skoku infrastrukturalnego są programy Polska Cyfrowa, Krajowy Plan Odbudowy oraz Fundusze Europejskie na Rozwój Cyfrowy. Projekty programu Polska Cyfrowa objęły zasięgiem około 2,1 mln gospodarstw domowych znajdujących się wcześniej w białych plamach oraz ponad 13 tys. szkół. Dodatkowo umowy podpisane w ramach kolejnych naborów KPO i FERC mają doprowadzić szybki internet do następnych setek tysięcy adresów. W samym czwartym konkursie KPO zakontraktowano ponad 778 mln zł na objęcie zasięgiem blisko 156 tys. nowych punktów adresowych do końca sierpnia 2026 roku.

To ważna lekcja dla strategii państwa: rynek skutecznie rozwija sieć tam, gdzie istnieje odpowiednia liczba odbiorców, ale ostatnie białe plamy wymagają precyzyjnej interwencji publicznej, uproszczenia procesu inwestycyjnego i współpracy z samorządami. Potrzebujemy aktualnych map zasięgu, sprawnego dostępu do pasa drogowego i infrastruktury technicznej, szybszych uzgodnień oraz instrumentów wspierających przyłączenie najdroższych, najbardziej oddalonych adresów. Cyfrowa solidarność oznacza bowiem, że mieszkaniec wsi lub małego miasteczka powinien mieć dostęp do usług o porównywalnej jakości jak mieszkaniec dużej aglomeracji.

Szybki internet nie jest dziś luksusem. Jest warunkiem edukacji, pracy zdalnej, prowadzenia firmy, korzystania z usług publicznych, telemedycyny oraz bezpieczeństwa. Dlatego cyfryzacja musi mieć wymiar solidarnościowy: dostęp do infrastruktury i usług powinien być możliwie równy w całym kraju.

3. Cyberbezpieczeństwo: nie dział IT, lecz bezpieczeństwo narodowe

Cyberbezpieczeństwo nie może być traktowane jako techniczny dodatek do administracji. Jest dziś elementem bezpieczeństwa narodowego, gospodarczego i społecznego.

Atak na szpital, urząd gminy, wodociągi, system energetyczny, transport, bankowość albo system wyborczy może wywołać skutki porównywalne z klasycznym sabotażem. Dlatego cyberbezpieczeństwo powinno być traktowane równie poważnie jak ochrona granic, infrastruktury krytycznej i bezpieczeństwo energetyczne.

Strategia państwa powinna obejmować stałe finansowanie, minimalne standardy bezpieczeństwa dla instytucji publicznych, rozwój zespołów reagowania, szkolenia kadr, bezpieczne kopie zapasowe, procedury awaryjne oraz regularne testy odporności.

Niezbędny jest również realny audyt: czy samorządy są gotowe na ransomware? Czy szpitale potrafią działać po utracie systemów? Czy administracja zna procedury reagowania? Czy łańcuchy dostaw sprzętu i oprogramowania są bezpieczne?

Cyberpotęga to państwo, które nie tylko reaguje na incydenty, lecz potrafi im zapobiegać i utrzymać ciągłość działania nawet podczas poważnego ataku.

4. Sztuczna inteligencja, dane i moc obliczeniowa

Sztuczna inteligencja zmienia administrację, edukację, ochronę zdrowia, przemysł, rolnictwo, wojsko i media. Polska nie może ograniczyć się do roli odbiorcy gotowych rozwiązań opracowanych poza Europą.

AI bez dostępu do danych i mocy obliczeniowej pozostaje hasłem. Dlatego strategiczne znaczenie mają: bezpieczna chmura państwowa, centra przetwarzania danych, infrastruktura GPU, superkomputery, krajowe modele językowe oraz jasne zasady wykorzystywania danych publicznych.

Dane państwa i obywateli są zasobem strategicznym. Nie oznacza to izolacji ani autarkii. Oznacza zdolność wyboru dostawcy, kontrolę nad kluczowymi systemami oraz możliwość utrzymania usług publicznych także w sytuacji kryzysowej.

4.1. Polski model językowy jako infrastruktura państwa

Polska ma już podstawy do budowy własnych modeli językowych. Projekty takie jak PLLuM pokazują, że można tworzyć rozwiązania uwzględniające polską gramatykę, kulturę, język urzędowy i specyfikę instytucji publicznych.

Sam model nie wystarczy. Potrzebny jest cały ekosystem: wysokiej jakości zbiory danych, dostęp do mocy obliczeniowej, jasne prawa do trenowania modeli, wsparcie zamówień publicznych, piaskownice regulacyjne oraz kapitał na skalowanie produktów.

Państwo powinno być pierwszym klientem bezpiecznych polskich rozwiązań AI, zwłaszcza w administracji, prawie, cyberbezpieczeństwie, edukacji, medycynie i obsłudze języka polskiego.

5. DSA, AI Act i ryzyko europejskiej nadregulacji

Mówiąc o ambicji budowy cyberpotęgi, musimy uczciwie ocenić kierunek regulacyjny Unii Europejskiej. Digital Services Act reguluje przede wszystkim odpowiedzialność platform i przestrzeń informacyjną. Rozwój systemów sztucznej inteligencji obejmuje natomiast AI Act. Do tego dochodzą GDPR, DMA, Data Act, prawo autorskie i przepisy krajowe.

Każdy z tych aktów ma uzasadnione cele: ochronę prywatności, konsumentów, konkurencji, bezpieczeństwa i praw obywatelskich. Problemem jest jednak skumulowany ciężar regulacyjny, wielość organów, niejednolite interpretacje i niepewność prawna.

Europa może stać się pierwszym kontynentem, który bardzo dokładnie reguluje technologie tworzone głównie poza Europą.

Nie należy twierdzić, że regulacje są jedyną przyczyną technologicznego dystansu. Znaczenie mają również mniejszy rynek kapitałowy, wysokie ceny energii, ograniczona dostępność GPU, fragmentacja rynku, słabsza komercjalizacja badań oraz odpływ talentów. Nadregulacja pogłębia jednak te problemy i szczególnie mocno uderza w startupy oraz mniejsze firmy.

5.1. Dane pokazujące skalę europejskiego dystansu

Według Stanford AI Index 2025 prywatne inwestycje w AI w Stanach Zjednoczonych wyniosły w 2024 roku około 109,1 mld dolarów. Było to niemal 12 razy więcej niż w Chinach i około 24 razy więcej niż w Wielkiej Brytanii, najwyżej sklasyfikowanym państwie europejskim.

W 2024 roku instytucje amerykańskie stworzyły 40 znaczących modeli AI, chińskie 15, a europejskie zaledwie kilka. Europejski Trybunał Obrachunkowy wskazał ponadto, że luka inwestycyjna między Unią a Stanami Zjednoczonymi w dziedzinie AI wyraźnie się zwiększyła.

To oznacza, że Europa pozostaje silna naukowo i regulacyjnie, ale zbyt słaba w skalowaniu firm, budowie największych modeli i przyciąganiu kapitału późnego etapu.

5.2. Bez pieniędzy nie będzie potęgi AI

Jeżeli sztuczna inteligencja ma być nową rewolucją przemysłową, nie możemy finansować jej jak kolejnego projektu informatycznego administracji. Rozwój AI wymaga ogromnych nakładów na centra danych, procesory, energię, badania, wynagrodzenia specjalistów, dostęp do danych oraz kapitał potrzebny do globalnego skalowania firm.

Światowy wyścig technologiczny jest więc także wyścigiem inwestycyjnym. Według Stanford AI Index 2026 prywatne inwestycje w AI w Stanach Zjednoczonych osiągnęły w 2025 roku około 285,9 mld dolarów. W Chinach wyniosły około 12,4 mld dolarów. Sama różnica w inwestycjach prywatnych była zatem ponad dwudziestotrzykrotna. Trzeba jednak pamiętać, że dane prywatne nie pokazują pełnej skali chińskiego finansowania, w którym znaczącą rolę odgrywają państwowe fundusze, banki i programy przemysłowe.

Dla porównania rok wcześniej, w 2024 roku, prywatne inwestycje w AI w Stanach Zjednoczonych wynosiły 109,1 mld dolarów, w Chinach 9,3 mld dolarów, a w Wielkiej Brytanii 4,5 mld dolarów. Dynamika wzrostu pokazuje, jak szybko podnoszona jest stawka tego wyścigu.

Unia Europejska zapowiedziała inicjatywę InvestAI, która ma zmobilizować 200 mld euro na rozwój sztucznej inteligencji, w tym 20 mld euro na budowę kilku gigafabryk AI. Jest to potrzebny kierunek, ale słowo „zmobilizować" nie oznacza, że cała ta kwota została już wydzielona w budżecie i jest dostępna dla firm. Program ma łączyć środki publiczne, instrumenty finansowe, inwestycje państw członkowskich i kapitał prywatny.

Europa musi więc mierzyć nie tylko wartość ogłoszonych planów, ale także tempo ich uruchamiania, liczbę dostępnych procesorów, rzeczywisty dostęp startupów do infrastruktury oraz zdolność firm do pozyskiwania kapitału na późnych etapach rozwoju. W AI liczy się nie tylko wysokość deklaracji, lecz także szybkość, z jaką pieniądze zamieniają się w centra danych, modele, produkty i przedsiębiorstwa.

5.2.1. V4: potencjał bez wspólnego budżetu

W odniesieniu do Grupy Wyszehradzkiej trudno wskazać jedną porównywalną kwotę rocznych nakładów na AI. Polska, Czechy, Słowacja i Węgry finansują sztuczną inteligencję z wielu rozproszonych źródeł: budżetów uczelni i instytutów, funduszy

europejskich, krajowych programów badawczych, cyfryzacji administracji, inwestycji przedsiębiorstw, superkomputerów oraz projektów realizowanych w ramach planów odbudowy.

Brakuje natomiast wspólnego, przejrzystego budżetu V4 na AI, wspólnej infrastruktury obliczeniowej i mechanizmu finansowania przedsiębiorstw zdolnych do globalnego wzrostu. To zasadnicza słabość. Państwa V4 mają łącznie około 62 mln mieszkańców, znaczącą bazę przemysłową, bardzo dobrych informatyków i dużą liczbę zastosowań dla AI, ale każde z nich osobno jest zbyt małe, aby finansowo konkurować z amerykańskimi koncernami lub chińskim modelem państwowo-przemysłowym.

Współpraca V4 powinna więc wyjść poza deklaracje. Potrzebne są: wspólny fundusz inwestycyjny dla firm AI, regionalna infrastruktura GPU, wspólne zamówienia publiczne, wielojęzyczne modele dla Europy Środkowej oraz program zatrzymywania talentów. Fundusz o wartości kilku miliardów euro nie pozwoli od razu rywalizować z największymi modelami amerykańskimi, ale może zbudować silną specjalizację w przemyśle, administracji, energetyce, medycynie, cyberbezpieczeństwie i językach regionu.

5.2.2. Potrzebny mierzalny cel finansowy

Samo podawanie kwot nominalnych może być mylące, ponieważ gospodarki Stanów Zjednoczonych, Chin i państw V4 mają różną wielkość. Dlatego Polska i jej partnerzy powinni przyjąć mierzalny cel nakładów na AI, obejmujący badania, infrastrukturę obliczeniową, wdrożenia w przedsiębiorstwach, cyfryzację przemysłu, rozwój modeli językowych oraz cyberbezpieczeństwo związane ze sztuczną inteligencją.

Jednocześnie należy zwiększać tempo wdrażania AI w gospodarce. Według Eurostatu w 2025 roku z technologii AI korzystało około 20% przedsiębiorstw w Unii Europejskiej zatrudniających co najmniej 10 osób. Sam rozwój modeli nie wystarczy, jeżeli przedsiębiorstwa nie będą miały kapitału, kompetencji i zachęt do ich praktycznego zastosowania.

Nie da się zbudować cyberpotęgi samymi strategiami, ustawami i konferencjami. Potęga technologiczna kosztuje. Jeżeli traktujemy AI jako nową rewolucję przemysłową, musimy finansować ją jak strategiczny projekt gospodarczy i bezpieczeństwa narodowego.

Polska ma ludzi, uczelnie, przedsiębiorców i doświadczenie przemysłowe. Grupa V4 ma odpowiednią skalę ludnościową i gospodarczą. Bez wspólnego funduszu,

infrastruktury obliczeniowej i zdecydowanego zwiększenia nakładów pozostaniemy jednak użytkownikami technologii stworzonych przez innych. Użytkownik technologii nie jest cyberpotęgą – jest klientem cyberpotęgi.

5.3. Jakiej regulacji potrzebuje Europa?

Odpowiedzią nie powinno być zniesienie wszystkich zasad. Systemy wysokiego ryzyka stosowane w medycynie, sądownictwie, finansach czy infrastrukturze krytycznej muszą podlegać szczególnym wymogom.

Potrzebujemy jednak zasady proporcjonalności: startup, uczelnia i mała firma nie mogą ponosić takich samych kosztów zgodności jak globalny koncern. Regulacja powinna zależeć od rzeczywistego ryzyka i skali działania, a nie wyłącznie od kategorii technologii.

Najważniejsze postulaty dla Unii Europejskiej to:

- jedna, spójna interpretacja przepisów cyfrowych w całej Unii;
- szerokie piaskownice regulacyjne dla AI i modeli otwartych;
- europejski paszport zgodności, aby produkt zatwierdzony w jednym państwie mógł działać na całym rynku;
- jasne zasady korzystania z danych do trenowania modeli z poszanowaniem praw twórców;
- uproszczenie raportowania i zakaz dublowania tych samych obowiązków;
- obowiązkowa ocena wpływu nowych regulacji na startupy, inwestycje i konkurencyjność;
- przegląd łącznego oddziaływania DSA, DMA, AI Act, GDPR i Data Act przed przyjmowaniem kolejnych obciążeń;
- szybsze procedury budowy centrów danych i infrastruktury energetycznej;
- rozwój europejskiego rynku kapitałowego i finansowania późnych etapów wzrostu.

6. Polska ma talent: światowe sukcesy informatyków

Polska posiada jeden z najważniejszych niewykorzystanych atutów technologicznych w Europie: wybitny kapitał ludzki.

W historycznej klasyfikacji Międzynarodowej Olimpiady Informatycznej polscy uczniowie zdobyli dziesiątki złotych, srebrnych i brązowych medali, plasując Polskę w ścisłej światowej czołówce. Jest to wynik wyjątkowy, zwłaszcza w zestawieniu z wielkością naszego kraju i skalą budżetów państw konkurencyjnych.

Podobnie wygląda sytuacja akademicka. Uniwersytet Warszawski dwukrotnie wygrał światowy finał International Collegiate Programming Contest (Akademickie Mistrzostwa Świata w Programowaniu Zespołowym), a jego zespoły od wielu lat regularnie kwalifikują się do finałów. Polscy programiści osiągają sukcesy także w konkursach algorytmicznych, matematycznych i cyberbezpieczeństwa.

Polska nie ma problemu z brakiem talentów. Ma problem z przekształcaniem talentów w trwałą własność intelektualną, globalne firmy i kapitał pozostający w kraju.

Nasza szkoła potrafi wykształcić światowej klasy programistę. Polski i europejski system wciąż zbyt rzadko potrafi zbudować wokół niego światowej klasy przedsiębiorstwo.

7. Kompetencje cyfrowe i odporność społeczna

Kompetencje cyfrowe to nie tylko umiejętność obsługi komputera. Obejmują rozpoznawanie dezinformacji, ochronę tożsamości, bezpieczne korzystanie z bankowości, rozumienie działania AI, ochronę danych oraz podstawy cyberhigieny.

Polska potrzebuje powszechnego programu odporności cyfrowej społeczeństwa. Senior powinien umieć rozpoznać fałszywy SMS. Uczeń powinien wiedzieć, czym jest deepfake. Urzędnik musi rozumieć, jakich danych nie wolno przekazywać publicznym narzędziom AI. Przedsiębiorca powinien potrafić zabezpieczyć firmę przed atakiem.

Bez kompetencji obywateli nawet najlepsza strategia technologiczna pozostanie dokumentem, a nie realną zmianą.

8. Dezinformacja, algorytmy i wolność słowa

Wojna informacyjna trwa codziennie. Wykorzystuje media społecznościowe, boty, fałszywe konta, mikrotargetowanie, deepfake i mechanizmy wzmacniające emocje.

Demokratyczne państwo musi jednocześnie chronić wolność słowa i przeciwdziałać obcej ingerencji, oszustwom oraz skoordynowanym operacjom

wpływu. Odpowiedzią, nie powinna być arbitralna cenzura, lecz przejrzystość i odpowiedzialność.

Obywatel powinien wiedzieć, dlaczego widzi określone treści. Państwo powinno mieć narzędzia do badania nielegalnego finansowania kampanii wpływu. Platformy powinny ujawniać podstawowe zasady działania systemów rekomendacyjnych, zwłaszcza w czasie wyborów.

Wolność słowa nie może oznaczać bezkarności algorytmów, ale walka z dezinformacją nie może stać się pretekstem do politycznej kontroli debaty.

9. Czy Polska może działać samodzielnie?

Polska może i powinna samodzielnie rozwijać modele wyspecjalizowane: dla administracji, prawa, medycyny, edukacji, cyberbezpieczeństwa, przemysłu i języka polskiego.

Jednocześnie zbudowanie od podstaw modelu granicznego konkurującego z największymi systemami amerykańskimi i chińskimi wymaga ogromnych nakładów na chipy, energię, dane, centra obliczeniowe i kadry. W tej kategorii samotne działanie Polski byłoby bardzo trudne.

Dlatego potrzebne są dwa poziomy działania: polska suwerenność językowa i sektorowa oraz regionalna skala obliczeniowa, kapitałowa i badawcza.

10. V4 jako środkowoeuropejski biegun sztucznej inteligencji

Państwa Grupy Wyszehradzkiej mają łącznie około 62 mln mieszkańców i gospodarkę o wartości przekraczającej 1,6 bln dolarów. To skala, która uzasadnia wspólne przedsięwzięcia technologiczne.

Polska wnosi największy rynek i silne zaplecze programistyczne. Czechy dysponują rozwiniętą infrastrukturą superkomputerową i przemysłową. Słowacja i Czechy mają silny sektor motoryzacyjny, a Węgry rozbudowują przemysł elektroniczny, bateryjny i centra technologiczne.

Obecnie strategie państw V4 są jednak rozproszone i brakuje wspólnego systemu finansowania, infrastruktury oraz komercjalizacji. V4 nie zastąpi całej Unii w globalnym wyścigu z USA i Chinami, ale może zbudować regionalny biegun technologiczny, którego żadne z naszych państw nie stworzy samodzielnie.

10.1. Wyszehradzka Inicjatywa Sztucznej Inteligencji

Współpraca V4 mogłaby obejmować:

- wspólny fundusz dla startupów AI;
- regionalną infrastrukturę GPU i dostęp do superkomputerów;
- wspólną przestrzeń danych językowych i przemysłowych;
- rodzinę modeli wielojęzycznych dla języków Europy Środkowej;
- program wymiany naukowców, inżynierów i studentów;
- wspólne zamówienia publiczne i pierwsze wdrożenia referencyjne;
- centrum testowania AI dla przemysłu, administracji, energetyki i cyberbezpieczeństwa;
- wspólne stanowisko wobec nadregulacji i fragmentacji prawa unijnego.

Wspólny model środkowoeuropejski nie powinien zastępować modeli narodowych. Mógłby tworzyć wspólną warstwę technologiczną, a polski PLLuM pozostałby jednym z fundamentów i modułów językowych.

11. Strategia ambitnej Polski: dziesięć priorytetów

1. **Cyberodporność państwa.** Minimalne standardy dla urzędów, szpitali, szkół, samorządów i spółek strategicznych; stałe finansowanie oraz regularne testy odporności.
2. **Suwerenność danych.** Traktowanie danych administracji, obywateli i infrastruktury krytycznej jako zasobu strategicznego.
3. **Polska AI.** Rozwój własnych modeli językowych i sektorowych, zespołów badawczych oraz wdrożeń publicznych.
4. **Moc obliczeniowa.** Dostęp dla uczelni i startupów do GPU, superkomputerów, bezpiecznej chmury i centrów danych.
5. **Kompetencje cyfrowe.** Powszechna edukacja od szkoły podstawowej po seniorów, administrację i przedsiębiorców.
6. **Cyfrowa solidarność.** Równy dostęp do infrastruktury i usług także w mniejszych miejscowościach i na obszarach wiejskich.

7. **Kapitał na skalowanie.** Fundusze zdolne finansować późne etapy wzrostu bez konieczności przenoszenia firmy poza Europę.
8. **Zamówienia publiczne.** Państwo jako pierwszy klient bezpiecznych polskich i europejskich technologii.
9. **Inteligentna regulacja.** Proporcjonalność, piaskownice regulacyjne, jeden standard interpretacyjny i ograniczenie dublowania obowiązków.
10. **Regionalna współpraca.** Budowa wspólnego potencjału AI i cyberbezpieczeństwa w V4 i szerzej w Europie Środkowej.

12. Zakończenie

Polska nie jest skazana na cyfrowe peryferia. Mamy dobrych informatyków, rozwinięty sektor IT, silne uczelnie, doświadczenie przemysłowe, duży rynek i pierwsze własne modele językowe.

Nie wystarczy jednak posiadać potencjał. Trzeba stworzyć warunki, w których talent może przejść drogę od konkursu i laboratorium do firmy, produktu, własności intelektualnej i globalnego rynku.

Europa potrzebuje regulacji chroniących człowieka, ale nie może budować systemu, w którym innowacja przegrywa z biurokracją. Polska powinna aktywnie zabiegać o inteligentne prawo: oparte na ryzyku, proporcjonalne i przyjazne dla młodych firm.

Polska samodzielnie może zbudować cyfrową suwerenność w kluczowych obszarach. Wspólnie z państwami V4 może stworzyć silny regionalny biegun AI. Działając zdecydowanie w Unii Europejskiej, powinna domagać się, aby Europa była miejscem, w którym wielkie technologie nie tylko się reguluje, lecz przede wszystkim tworzy.

Mniej cyfrowych haseł, więcej realnych zdolności. Mniej zależności, więcej własnych kompetencji. Mniej biurokratycznej ostrożności, więcej strategicznej odwagi.

Odpowiedź na pytanie z tytułu panelu powinna być jednoznaczna: Polska nie może być cyfrową peryferią. Polska musi mieć ambicję cyberpotęgi.

13. Wybrane źródła i materiały

1. Ministerstwo Cyfryzacji, „Realizacja Strategii Cyfryzacji Państwa", gov.pl.
2. Ministerstwo Cyfryzacji, „Strategia Cyfryzacji Polski do 2035 roku", gov.pl.

3. Komisja Europejska, Digital Services Act oraz AI Act – materiały wdrożeniowe i informacyjne.
4. Stanford Institute for Human-Centered AI, AI Index Report 2025.
5. Europejski Trybunał Obrachunkowy, raport specjalny dotyczący unijnych ambicji w dziedzinie sztucznej inteligencji.
6. Mario Draghi, raport o przyszłości europejskiej konkurencyjności.
7. International Olympiad in Informatics, statystyki medalowe Polski.
8. International Collegiate Programming Contest, wyniki i historia udziału Uniwersytetu Warszawskiego.
9. Bank Światowy, dane gospodarcze państw Grupy Wyszehradzkiej.
10. Materiały dotyczące polskiego modelu językowego PLLuM i krajowej infrastruktury obliczeniowej.
11. Ministerstwo Cyfryzacji i Instytut Łączności – PIB, „Polska w zasięgu sieci", dane SIDUSIS według stanu na 31 marca 2026 roku.
12. Stanford Institute for Human-Centered AI, AI Index Report 2026, dane o globalnych inwestycjach prywatnych w AI.
13. Komisja Europejska, InvestAI oraz AI Continent Action Plan, informacje o mobilizacji 200 mld euro i finansowaniu gigafabryk AI.
14. Eurostat, „20% of EU enterprises use AI technologies", dane za 2025 rok.

14. Słowniczek pojęć i skrótów

Poniższe objaśnienia upraszczają specjalistyczne pojęcia użyte w referacie. Definicje odnoszą się do kontekstu cyfryzacji, cyberbezpieczeństwa i sztucznej inteligencji.

5G – Piąta generacja sieci komórkowej. Zapewnia większą szybkość transmisji danych, mniejsze opóźnienia i możliwość jednoczesnego podłączenia bardzo dużej liczby urządzeń.

6G – Planowana szósta generacja sieci komórkowej, rozwijana jako następca 5G. Ma oferować jeszcze większą przepustowość i wspierać zaawansowane zastosowania sztucznej inteligencji, przemysłu oraz komunikacji między urządzeniami.

AI (Artificial Intelligence) – Sztuczna inteligencja – systemy komputerowe wykonujące zadania wymagające zwykle ludzkiego rozumowania, takie jak analiza tekstu, rozpoznawanie obrazów, prognozowanie lub podejmowanie decyzji.

AI Act – Unijne rozporządzenie ustanawiające zasady tworzenia i stosowania systemów sztucznej inteligencji. Obowiązki są uzależnione przede wszystkim od poziomu ryzyka związanego z danym zastosowaniem.

Algorytm – Ściśle określony zestaw instrukcji, według których komputer rozwiązuje problem, analizuje dane albo podejmuje decyzję.

Biała plama – Punkt adresowy lub obszar, na którym nie ma dostępu do odpowiednio szybkiej sieci szerokopasmowej. W praktyce dotyczy to najczęściej terenów słabo zaludnionych i oddalonych od istniejącej infrastruktury.

Bot – Program automatycznie wykonujący zadania w internecie. Boty mogą służyć legalnym celom, ale bywają również wykorzystywane do spamu, oszustw, sztucznego zwiększania zasięgów i rozpowszechniania dezinformacji.

Chmura obliczeniowa – Model korzystania z serwerów, pamięci masowej, baz danych i oprogramowania przez sieć, bez konieczności utrzymywania całej infrastruktury na własnych komputerach.

Cyberhigiena – Podstawowe nawyki ograniczające ryzyko ataku, takie jak stosowanie silnych haseł, uwierzytelnianie wieloskładnikowe, aktualizacje oprogramowania, ostrożność wobec linków i regularne kopie zapasowe.

Cyberodporność – Zdolność instytucji lub firmy do zapobiegania cyberatakom, utrzymania najważniejszych usług w czasie incydentu oraz szybkiego odtworzenia działania po ataku.

Cyberpotęga – Państwo dysponujące silnymi kadrami, własnymi technologiami, bezpieczną infrastrukturą, zdolnością reagowania na cyberataki i wpływem na międzynarodowe reguły cyfrowe.

Data Act – Unijne rozporządzenie dotyczące dostępu do danych i ich wykorzystywania, zwłaszcza danych wytwarzanych przez urządzenia i usługi cyfrowe.

Deepfake – Fałszywy materiał audio, wideo lub graficzny wygenerowany albo zmodyfikowany przez sztuczną inteligencję tak, aby realistycznie przedstawiał osobę mówiącą lub robiącą coś, czego w rzeczywistości nie zrobiła.

Dezinformacja – Celowe rozpowszechnianie fałszywych lub zmanipulowanych informacji w celu wywarcia wpływu na odbiorców, debatę publiczną albo decyzje polityczne i gospodarcze.

DMA (Digital Markets Act) – Unijne rozporządzenie ograniczające nadużywanie dominującej pozycji przez największe platformy cyfrowe, określane jako strażnicy dostępu do rynku.

DSA (Digital Services Act) – Unijne rozporządzenie o usługach cyfrowych. Określa obowiązki platform internetowych dotyczące m.in. nielegalnych treści, reklam, przejrzystości algorytmów i ochrony użytkowników.

FERC – Fundusze Europejskie na Rozwój Cyfrowy – polski program finansowany ze środków Unii Europejskiej, wspierający m.in. rozwój szybkiego internetu, e-usług i cyberbezpieczeństwa.

GDPR / RODO – Ogólne rozporządzenie o ochronie danych osobowych. GDPR to skrót angielski, a RODO – powszechnie używana polska nazwa tego samego unijnego aktu prawnego.

GPU – Procesor graficzny, który dzięki wykonywaniu wielu obliczeń równocześnie jest podstawowym elementem infrastruktury służącej do trenowania i uruchamiania zaawansowanych modeli AI.

Infrastruktura krytyczna – Systemy i obiekty niezbędne do funkcjonowania państwa i społeczeństwa, np. energetyka, wodociągi, telekomunikacja, transport, bankowość i ochrona zdrowia.

KPO – Krajowy Plan Odbudowy i Zwiększania Odporności – program inwestycji i reform finansowany z europejskiego Instrumentu na rzecz Odbudowy i Zwiększania Odporności.

Mikrotargetowanie – Kierowanie reklam lub komunikatów do bardzo precyzyjnie wybranych grup osób na podstawie ich danych, zainteresowań, zachowań lub przewidywanych poglądów.

Model graniczny – Najbardziej zaawansowany model sztucznej inteligencji w danym okresie, trenowany na bardzo dużych zbiorach danych i wymagający ogromnej mocy obliczeniowej.

Model językowy – System AI uczony na dużych zbiorach tekstów, który potrafi analizować i generować język naturalny, odpowiadać na pytania, streszczać dokumenty lub wspierać wyszukiwanie informacji.

Moc obliczeniowa – Zdolność komputerów lub centrów danych do wykonywania obliczeń. W AI zależy m.in. od liczby i wydajności procesorów GPU oraz dostępnej energii.

NGA (Next Generation Access) – Sieci dostępu nowej generacji, zapewniające bardzo szybki i stabilny internet. Biała plama NGA oznacza adres bez dostępu do sieci spełniającej wymagane parametry wysokiej przepustowości.

Piaskownica regulacyjna – Kontrolowane środowisko, w którym firma lub instytucja może testować innowacyjne rozwiązanie pod nadzorem właściwego organu, zanim zostanie ono w pełni wprowadzone na rynek.

PLLuM – Rodzina polskich dużych modeli językowych rozwijanych z myślą o języku polskim, administracji publicznej i krajowym ekosystemie sztucznej inteligencji.

Ransomware – Złośliwe oprogramowanie, które szyfruje pliki albo blokuje system, a następnie służy przestępcom do żądania okupu za przywrócenie dostępu.

SIDUSIS – System Informacyjny o Dostępie do Usług Stacjonarnego Internetu Szerokopasmowego. Gromadzi informacje o zasięgu sieci i planowanych inwestycjach telekomunikacyjnych w Polsce.

Startup – Młoda firma tworzona w celu szybkiego rozwijania i skalowania innowacyjnego produktu lub usługi, często technologicznej.

Superkomputer – Bardzo wydajny system obliczeniowy używany do skomplikowanych symulacji, analiz naukowych, przetwarzania wielkich zbiorów danych i trenowania modeli AI.

System rekomendacyjny – Algorytm wybierający i porządkujący treści, produkty lub filmy pokazywane użytkownikowi na podstawie jego aktywności i przewidywanych zainteresowań.

V4 / Grupa Wyszehradzka – Forma współpracy Polski, Czech, Słowacji i Węgier. W referacie V4 jest przedstawiana jako możliwa platforma wspólnych inwestycji w AI, centra obliczeniowe, dane i cyberbezpieczeństwo.

Gigafabryka AI – Bardzo duże centrum obliczeniowe wyposażone w tysiące zaawansowanych procesorów, przeznaczone do trenowania i uruchamiania największych modeli sztucznej inteligencji.

InvestAI – Inicjatywa Unii Europejskiej mająca mobilizować środki publiczne i prywatne na rozwój AI, w tym na europejskie gigafabryki obliczeniowe.

Inwestycje prywatne w AI – Kapitał przekazywany przez przedsiębiorstwa, fundusze i inwestorów prywatnych na rozwój firm, modeli, infrastruktury i produktów opartych na sztucznej inteligencji.

Kapitał późnego etapu – Finansowanie dla firm, które mają już produkt i klientów, ale potrzebują bardzo dużych środków, aby wejść na wiele rynków i konkurować globalnie.

PKB (produkt krajowy brutto) – Łączna wartość dóbr i usług wytworzonych w gospodarce w określonym czasie. Udział wydatków w PKB pozwala porównywać wysiłek finansowy państw o różnej wielkości.

Autorzy



Kamil Basaj

Założyciel i prezes Fundacji INFO OPS Polska. Kieruje pracami zespołów ds. reagowania na zagrożenia hybrydowe, w tym operacji informacyjnych. Twórca procesów bezpieczeństwa środowiska informacyjnego. Zawodowo związany z resortem obrony narodowej. Doświadczenie zawodowe obejmuje pracę w ramach zespołu reagowania na incydenty CSiRT MON, Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, Ministerstwa Obrony Narodowej, Departamentu Bezpieczeństwa Narodowego KPRM, Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni oraz Rządowego Centrum Bezpieczeństwa.

Konsultant projektów badawczych i naukowych nad zjawiskami oddziaływania informacyjnego, psychologicznego, bezpieczeństwa środowiska informacyjnego i cyberbezpieczeństwa. Wykładowca Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa, Politechniki Warszawskiej i Szkoły Głównej Handlowej. Jest prelegentem na krajowych i zagranicznych konferencjach poświęconych bezpieczeństwu środowiska informacyjnego i poznawczego

---



Mariusz Błaszczak

Poseł na Sejm VI, VII, VIII, IX i X kadencji. W latach 2002–2004 pełnił funkcję zastępcy burmistrza warszawskiej dzielnicy Wola, zaś od 2004 do 2005 roku – burmistrza dzielnicy Śródmieście. W latach 2006–2007 zasiadał w sejmiku mazowieckim. Szef Kancelarii Prezesa Rady Ministrów (2005–2007), minister-członek Rady Ministrów w rządzie Jarosława Kaczyńskiego (2007), minister spraw wewnętrznych i administracji w rządzie Beaty Szydło i pierwszym rządzie Mateusza Morawieckiego (2015–2018), minister obrony narodowej w pierwszym, drugim i trzecim rządzie Mateusza Morawieckiego (2018–2023), wiceprezes Rady Ministrów (2022–2023). Wiceprezes Prawa i Sprawiedliwości. Obecnie pełni funkcję szefa Klubu Parlamentarnego PiS.



Zbigniew Bogucki

Prawnik, adwokat, samorządowiec, wojewoda zachodniopomorski, poseł na Sejm RP X kadencji, członek Komitetu Politycznego Prawa i Sprawiedliwości oraz prezes Zarządu Okręgowego PiS w okręgu szczecińskim, obecnie Szef Kancelarii Prezydenta Rzeczypospolitej Polskiej.

Urodził się 26 stycznia 1980 r. w Górze na Dolnym Śląsku. Ukończył prawo na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego, a następnie aplikację prokuratorską jednocześnie pracując w Zachodniopomorskim Oddziale Wojewódzkim NFZ. W latach 2009–2012 jako asesor wykonywał obowiązki prokuratorskie. Od 2012 roku prowadził własną kancelarię adwokacką.

W latach 2018–2020 był radnym Sejmiku Województwa Zachodniopomorskiego. Równolegle angażował się w działalność społeczną – był członkiem Społecznego Komitetu Budowy Pomnika śp. Prezydenta RP Lecha Kaczyńskiego w Szczecinie oraz jednym z założycieli Szczecińskiego Towarzystwa Dialogu o Prawie. Doświadczenie zarządcze i biznesowe poza własną działalnością gospodarczą zdobywał także jako członek rady nadzorczej Zarządu Morskich Portów Szczecin i Świnoujście, a następnie przewodniczący rady nadzorczej Polskiej Wytwórni Papierów Wartościowych.

W listopadzie 2020 r. objął funkcję Wojewody Zachodniopomorskiego, którą sprawował do listopada 2023 roku.

W wyborach parlamentarnych w 2023 roku uzyskał mandat posła na Sejm X kadencji, zdobywając zaufanie 26375 wyborców. Zasiadał w Komisji Administracji i Spraw Wewnętrznych, Komisji Sprawiedliwości i Praw Człowieka, Komisji Śledczej dot. kwestii wizowych oraz Komisji Nadzwyczajnej do spraw zmian w kodyfikacjach.

Z dniem 7 sierpnia 2025 r. powołany przez Prezydenta RP Karola Nawrockiego na stanowisko Szefa Kancelarii Prezydenta Rzeczypospolitej Polskiej.



gen. bryg. rez. Mirosław Bryś

Zastępca Szefa Biura Bezpieczeństwa Narodowego. Absolwent WSO im. Tadeusza Kościuszki we Wrocławiu, Akademii Obrony Narodowej oraz Uniwersytetu Humanistyczno–Przyrodniczego w Kielcach. Doświadczenie zdobywał służąc w Wojskach Aeromobilnych (25BKPow i 6BPD) na wszystkich szczeblach dowodzenia w kraju i zagranicą. Czynnie uczestniczył w formowaniu Wojsk Obrony Terytorialnej oraz był twórcą 4 Warmińsko Mazurskiej Brygady Obrony Terytorialnej. Uczestnik czterech misji pokojowych poza granicami kraju, w ramach SFOR w Bośni i Hercegowinie, dwukrotnie w ramach PKW Irak (V i IX zmiana)

oraz w ramach XI zmiany PKW Afganistan. W latach 2022–2024 będąc Szefem Centralnego Wojskowego Centrum Rekrutacji, stworzył system promocji i rekrutacji do Sił Zbrojnych Rzeczypospolitej Polskiej oraz przeprowadził reformę Terenowych Organów Wykonawczych MON. Specjalizuje się w problematyce zarządzania procesem zmian w organizacjach, bezpieczeństwem demograficznym państwa oraz krajowym systemem zarządzania kryzysowego.



PROF. KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Prof. dr hab. nauk społecznych, prawo (doktorat UW i habilitacja UJ) w Akademii Leona Koźmińskiego, radca prawny, dyrektor ds. Rejestru domen internetowych w NASK PIB. W latach 1996-2010 prawnik m.in. w Krajowej Radzie Radiofonii i Telewizji, Telewizji Polsat S.A. oraz w TVP S.A. W latach 2011-2018 wicedyrektor Narodowego Instytutu Audiowizualnego. Wieloletni pracownik naukowy AON i ASZWOJ, do 2024 r. dyrektor Akademickiego Centrum Polityki Cyberbezpieczeństwa. Członek Rady ds. cyfryzacji trzech kadencji, członek Rady ds. Bezpieczeństwa i Obronności w Narodowej Radzie Rozwoju w Kancelarii Prezydenta RP. Pomysłodawczyni, wydawczyni i redaktorka naczelna pisma Cybersecurity and Law. Jako naukowiec prowadzi prace badawcze dotyczące regulacji prawnych w obszarze mediów cyfrowych, cyberbezpieczeństwa, zagrożeń bezpieczeństwa informacyjnego, ochrony własności intelektualnej, procesów cyfryzacji i wpływu nowych technologii na rozwój Państwa i sytuację prawną Jednostki. Autorka i współautorka monografii i licznych artykułów, do których zaliczyć można takie pozycje jak: Prawo nowych technologii, Cyberodpowiedzialność, Bezpieczeństwo, Prywatność, Tożsamość, Media audiowizualne. Konflikt regulacyjny w dobie cyfryzacji, Audiowizualne usługi medialne. Reglamentacja w warunkach konwersji cyfrowej, Prawna ochrona treści cyfrowych, Prawne granice dezinformacji.



SEBASTIAN CHWAŁEK

Doświadczony manager, polityk, prawnik, urzędnik zaangażowany w służbie publicznej. Absolwent Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie. Ekspert w zakresie bezpieczeństwa, modernizacji technicznej sił zbrojnych, przemysłu zbrojeniowego. W latach 2015–2017 Podsekretarz Stanu, a w latach 2017–2018 Sekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji oraz Pełnomocnik Rządu ds. Repatriacji. W tym okresie uczestniczył w pracach administracji rządowej jako członek Komitetu Stałego Rady Ministrów, członek (współprzewodniczący) Komisji Wspólnej Rządu

i Samorządu Terytorialnego, współprzewodniczący Komisji Wspólnej Rządu i Mniejszości Narodowych i Etnicznych, Członek Komisji Wspólnej Rządu i Episkopatu. Uczestniczył w pracach wielu zespołów międzyresortowych z zakresu bezpieczeństwa. W roku 2018 i w latach 2020–2021 Sekretarz Stanu w Ministerstwie Obrony Narodowej, gdzie nadzorował m. in. proces modernizacji technicznej i rozbudowy sił zbrojnych, infrastrukturę oraz służbę zdrowia. Koordynował w tym okresie m. in. prace nad projektem utworzenia Agencji Uzbrojenia. Przewodniczył także Trójstronnemu Zespołowi ds. Rozwoju Przemysłowego Potencjału Obronnego i Modernizacji Technicznej Sił Zbrojnych w ramach Rady Dialogu Społecznego. W latach 2018–2020 Wiceprezes Polskiej Grupy Zbrojeniowej, a w latach 2021–2024 Prezes Polskiej Grupy Zbrojeniowej. Był też członkiem stałym zarządu Aerospace and Defence Industries Association of Europe (ASD). Był członkiem Rady Naukowej kwartalnika „Wojskowy Przegląd Prawniczy". Członek Narodowej Rady Rozwoju – Rady ds. Strategicznych Projektów Rozwojowych. Keynote speaker i panelista licznych krajowych i międzynarodowych konferencji w zakresie bezpieczeństwa wewnętrznego i militarnego, modernizacji sił zbrojnych, rozbudowy potencjału produkcyjnego, produkcji uzbrojenia i wyposażenia sił zbrojnych, nowoczesnych technologii w przemyśle zbrojeniowym.



DR HAB. IRENEUSZ DĄBROWSKI, PROF. SGH

Ekonomista i prawnik, doktor habilitowany nauk ekonomicznych, profesor Szkoły Głównej Handlowej w Warszawie, specjalista w zakresie problemów stabilności systemów, równowagi ogólnej oraz ekonomii ewolucyjnej, w latach 2005–2006 wicewojewoda opolski, w latach 2006–2007 wiceminister skarbu państwa.

Ukończył studia w Szkole Głównej Handlowej w Warszawie oraz na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego. Pracuje w Szkole Głównej Handlowej w Warszawie, gdzie w 2006 obronił rozprawę doktorską, a w 2017 uzyskał habilitację. W SGH był adiunktem, a następnie został profesorem nadzwyczajnym SGH i objął funkcję kierownika Zakładu Ekonomii Monetarnej. Wykładał także w Wyższej Szkole Ubezpieczeń i Bankowości w Warszawie.

W latach 2002–2005 był radnym warszawskiej dzielnicy Śródmieście, w której pełnił funkcję wiceprzewodniczącego Komisji Polityki Gospodarczej, Budżetu i Finansów. Od grudnia 2005 do 31 sierpnia 2006 pełnił funkcję wicewojewody opolskiego. Następnie do 16 lipca 2007 zajmował stanowisko podsekretarza stanu w Ministerstwie Skarbu Państwa. W 2018 objął funkcję redaktora naczelnego czasopisma naukowego „Bank i Kredyt". W latach 2019-2021 był dyrektorem Departamentu Badań Ekonomicznych NBP. W lutym 2022 prezydent Andrzej Duda powołał go na członka Rady Polityki Pieniężnej na okres sześcioletniej kadencji.



Wojciech Dąbrowski

Wojciech Dąbrowski menedżer z wieloletnim doświadczeniem w dużych grupach kapitałowych, administracji rządowej i samorządowej. Związany z branżą energetyczną, kierował największymi podmiotami w Polsce, PGNIG Termika (aktualnie Grupa PKN Orlen), PGE Energia Ciepła oraz w latach 2020-24 największą polską grupą energetyczną PGE S.A. Aktualnie członek Rady Energii i Zasobów Naturalnych przy Prezydencie Rzeczypospolitej Polskiej. Prezes zarządu think tanku Fundacja SET (Security Energy Technology).



Marietta Gieroń

Pełni funkcję Prezes Zarządu Instytutu Kościuszki oraz Przewodniczącej Rady Nadzorczej Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland. W latach 2024-2025 była Przewodniczącą Rady Programowej CYBERSEC. Doświadczona liderka, skoncentrowana na wzmacnianiu współpracy międzynarodowej i międzysektorowej. W Instytucie Kościuszki angażuje się w działania na rzecz promowania równości płci w sektorze IT, rozwoju edukacji cyfrowej młodzieży oraz wspierania projektów dedykowanych regionowi Europy Środkowo-Wschodniej. Absolwentka prawa na Uniwersytecie Jagiellońskim w Krakowie oraz studiów podyplomowych z zakresu prawa karnego materialnego i procesowego, a także wyzwań cywilizacyjnych i nowych technologii.



dr Karolina Grenda

Doktor nauk prawnych, członek Rady Nowych Technologii i Cyfryzacji przy Prezydencie RP, członek Rady Fundacji SET.Przedsiębiorca, wykładowca akademicki, analityk bezpieczeństwa. Specjalizuje się w AI, prawie nowych technologii oraz cyberbezpieczeństwie.

Przez ponad dwie dekady związana ze strukturami państwowymi i spółkami o strategicznym znaczeniu. Jako oficer Policji pełniła funkcje kierownicze i dowódcze kończąc służbę w strukturach bezpieczeństwa w stopniu pułkownika. www.KarolinaGrenda.pl



Bartossz Grodecki

Bartosz Grodecki (ur. 1980 w Warszawie) – dyplomata, urzędnik państwowy i ekspert ds. bezpieczeństwa oraz polityki migracyjnej. Absolwent Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego oraz studiów MBA w zakresie zarządzania cyberbezpieczeństwem w Wojskowej Akademii Technicznej.

W latach 2020-2023 był podsekretarzem stanu w Ministerstwie Spraw Wewnętrznych i Administracji, odpowiedzialnym m.in. za politykę migracyjną i graniczną, współpracę z UE w obszarze spraw wewnętrznych, kwestie cudzoziemców, obywatelstwa, cyberbezpieczeństwa i repatriacji. W czasie kryzysu na granicy polsko-białoruskiej koordynował działania oraz prezentował stanowisko Polski na forum międzynarodowym i w relacjach z naszymi partnerami, akcentując ochronę bezpieczeństwo państwa polskiego, ochronę granic zewnętrznych UE oraz przeciwdziałanie presji migracyjnej i przemytowi ludzi. Uczestniczył także w działaniach dotyczących wsparcia Ukrainy, pomocy uchodźcom wojennym w trakcie kryzysu po wybuchu wojny. Miał także ważny udział w procesie ewakuacji współpracowników NATO z Afganistanu po decyzji o wycofaniu amerykańskich wojsk z tego kraju. Współpracował z demokratycznymi środowiskami na Białorusi i w Mołdawii.

Wcześniej, w latach 2006-2020 pracował w Ministerstwie Spraw Zagranicznych, pełniąc funkcje konsularne i kierownicze, m.in. na placówkach w Los Angeles, Malmö i Sztokholmie. Jako dyrektor Departamentu Konsularnego MSZ odpowiadał za koordynację działań polskiej służby konsularnej oraz zarządzanie sytuacjami kryzysowymi dotyczącymi obywateli polskich za granicą.

Po odejściu z administracji publicznej zajął się działalnością doradczą i ekspercką. Od marca 2025 r. związany jest z Instytutem Sobieskiego jako ekspert. W ostatnich latach dzielił także się wiedzą ekspercką w obszarze przemysłu zbrojeniowego współpracując z instytucjami i podmiotami rynkowymi. W swoich publicznej aktywności koncentruje się głównie na kwestiach bezpieczeństwa państwa, odporności społeczeństwa, polityce migracyjnej oraz współpracy transatlantyckiej i regionalnej.



Piotr Guział

Absolwent Szkoły Głównej Handlowej w Warszawie (kierunek Gospodarka Publiczna), studiował także na Uniwersytecie w Kolonii (kierunek Ekonomia). Ukończył podyplomowe studia Commodity Trading – Inwestycje na rynkach towarowych oraz Ryzyko i ubezpieczenia majątkowe na Akademii Leona Koźmińskiego w Warszawie. Legitymuje się zdanym

egzaminem dla kandydatów na członków organów nadzorczych spółek z udziałem Skarbu Państwa. Jest członkiem rad programowych konferencji Smart City Forum i EuroPOWER & OZE POWER.

Współzałożyciel, wspólnik i prezes zarządu LOGiT sp. z o.o. – polskiego startupu legaltech – właściciela platformy LOGiT FLOW do analizy, audytu i tworzenia dokumentów prawnych, urzędowych i biznesowych z wykorzystaniem sztucznej inteligencji.

Zasiadał w zarządach i radach nadzorczych kilkunastu spółek. W latach 2019-2024 pełnił kluczowe funkcje zarządcze w Grupie Kapitałowej Orlen S.A., m.in. jako członek zarządu ds. rozwoju Orlen Deutschland GmbH – spółki zarządzającej siecią 607 stacji paliw marki star i Orlen w Niemczech oraz prezes zarządu Doppler Energie GmbH (obecnie Orlen Austria) – trzeciej co do wielkości sieci stacji paliw w Austrii, zarządzającej siecią 266 stacji paliw marki Turmöl. Pełnił funkcję Burmistrza Dzielnicy Ursynów m.st. Warszawy (2010-2014). Był również radnym m.st. Warszawy (2014-2018) oraz radnym Ursynowa (1998-2010). W latach 2019-2024 zasiadał w radzie nadzorczej Exatel S.A. – operatora telekomunikacyjnego i dostawcy usług cyberbezpieczeństwa.



Zbigniew Hoffmann

Poseł na Sejm RP IX i X kadencji, politolog, urzędnik państwowy, Wiceprzewodniczący Komisji ds. Służb Specjalnych. W latach 2020-2023 Minister-Członek Rady Ministrów, Sekretarz Komitetu Rady Ministrów ds. Bezpieczeństwa Narodowego i spraw Obronnych, Sekretarz Stanu w KPRM, 2015-2020 Wojewoda Wielkopolski, wcześniej ekspert ds. bezpieczeństwa w Kancelarii Prezydenta RP Prof. Lecha Kaczyńskiego, a także w Biurze Bezpieczeństwa Narodowego. Stypendysta rządu USA w zakresie bezpieczeństwa i porządku publicznego.



Jan Kostrzewa

Absolwent kierunku Artificial Intelligence na Politechnice Warszawskiej i twórca publikacji naukowych z zakresu AI oraz cyberbezpieczeństwa. Jest współtwórcą pierwszego polskiego satelity PW-Sat, projektu, który zapisał się w historii polskiej astronautyki. Kierował Centrum Cyberbezpieczeństwa, gdzie zespół pod jego przewodnictwem przeszkolił ponad 30.000 pracowników, zrealizował testy bezpieczeństwa kluczowych systemów oraz utworzył SOC 24/7 dla całego Resortu Sprawiedliwości. Inicjator największego polskiego konkursu CTF tj. Konkursu "CTF 153+1" w którym przez kilka edycji wzięło łącznie

udział kilkanaście tysięcy osób. Posiada certyfikaty branżowe, m.in. CISSP i CompTIA Security+, a także został zweryfikowany do dostępu do informacji o najwyższych klauzulach tajności. Łączy doświadczenie zdobyte w sektorze publicznym i prywatnym, co daje mu rzadką perspektywę łączenia potrzeb biznesu, administracji i bezpieczeństwa państwa. Obecnie, jako Członek Rady Nowych Technologii i Cyfryzacji przy Prezydencie RP oraz twórca unitu B3 CyberSecurity, dzieli się wiedzą z cyberbezpieczeństwa, sztucznej inteligencji i innowacji by kompleksowo zabezpieczać podmioty prywatne i państwowe.



PPŁK REZ. DR INŻ. ROBERT KOŚLA

Przewodniczący Rady Fundacji Bezpieczna Cyberprzestrzeń, absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie. Od 1994 r. służył w Biurze Szyfrów UOP, a następnie pełnił funkcje kierownicze w UOP i ABW, odpowiadając m.in. za procesy akcesyjne do NATO i UE oraz rozwój systemu badań i certyfikacji środków ochrony kryptograficznej i elektromagnetycznej.

W latach 2006–2008 kierował w MSWiA budową Systemu Informacyjnego Schengen, co umożliwiło wejście Polski do strefy Schengen w grudniu 2007 r. W latach 1998–2008 reprezentował Polskę w Podkomitecie INFOSEC NATO. W latach 2008–2018 był dyrektorem Sektora Bezpieczeństwa Narodowego i Obrony na region CEE w Microsoft.

W latach 2018–2021 kierował Departamentem Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, a następnie w KPRM. Odpowiadał m.in. za rozwój Krajowego Systemu Cyberbezpieczeństwa, Strategię Cyberbezpieczeństwa RP, Narodowe Standardy Cyberbezpieczeństwa, nadzór dostawcami usług zaufania eIDAS oraz budowę Narodowego Systemu Certyfikacji Cyberbezpieczeństwa, był autorem Programu Współpracy w Cyberbezpieczeństwie – PWCyber.

Od 2010 r. współtwórca i członek Rady Fundacji Bezpieczna Cyberprzestrzeń, a od 2024 r. jej przewodniczący. Od 2021 r. członek Rady Konsultacyjnej przy Morskim Centrum Cyberbezpieczeństwa oraz przewodniczący Komitetu ds. Bezstronności Jednostki Certyfikującej NASK-PIB. Wykładowca przedmiotu Cyberodporność na wojskowych i cywilnych studiach podyplomowych EMBA, MBA i DBA. W 2024 r. uzyskał stopień doktora w dyscyplinie nauki o bezpieczeństwie; rozprawa dotyczyła bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa wobec zagrożeń hybrydowych.



DR INŻ. PRZEMYSŁAW KOWALCZUK

Dr inż., MBA, menedżer sektora obronnego z ponad 23-letnim doświadczeniem w zarządzaniu przedsiębiorstwami przemysłu zbrojeniowego oraz projektami technologiczno-przemysłowymi o znaczeniu strategicznym.

Pełnił funkcje kierownicze w kluczowych spółkach polskiej branży zbrojeniowej. Odpowiadał za rozwój biznesu, zwiększanie mocy produkcyjnych oraz współpracę z globalnymi partnerami sektora obronnego, m.in. Lockheed Martin, Northrop Grumman, Raytheon, BAE Systems i Boeing. Jego doświadczenie obejmuje rozwój technologii obronnych, transfer technologii oraz realizację międzynarodowych programów zbrojeniowych, w tym w obszarze systemów obrony powietrznej, elektroniki wojskowej i produkcji amunicji.



PAWEŁ MAJEWSKI

Menedżer, prawnik, członek Rady Fundacji SET. Absolwent Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego oraz studiów podyplomowych Executive MBA.

Doświadczenie zawodowe zdobywał m.in. w przedsiębiorstwach branży energetyczno-paliwowej, lotniskowej i zbrojeniowej. Pracował w spółkach publicznych, notowanych na GPW, pełniąc kolejno funkcje: prezesa zarządu Grupy LOTOS, prezesa zarządu Polskiego Górnictwa Naftowego i Gazownictwa S.A. oraz prezesa zarządu Enea S.A. Wcześniej pracował na stanowiskach menedżerskich w Petrolot Sp. z o.o. (obecnie Orlen Aviation) i w PGNiG Termika S.A., pełnił także funkcje członka zarządu Lot Catering Sp. z o.o. (obecnie DO&CO Poland), prezesa zarządu ACS Sp. z o.o., wiceprezesa zarządu Huty Stalowa Wola S.A.



DR DANIEL MILEWSKI

Doktor nauk prawnych, ekonomista i parlamentarzysta. Poseł na Sejm RP i przedstawiciel Polski w Zgromadzeniu Parlamentarnym Rady Europy, gdzie pełni funkcję wiceprzewodniczącego komisji ds. zagadnień prawnych i praw człowieka. W Sejmie pracuje m.in. w Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, będąc wiceprzewodniczącym podkomisji stałej ds. cyberbezpieczeństwa. Jest wykładowcą akademickim i prorektorem Warszawskiej Uczelni Ekonomicznej. Obok problematyki funkcjonowania organizacji międzynarodowych, naukowo zajmuje się prawnymi aspektami rozwoju sztucznej inteligencji oraz możliwościami stosowania AI w administracji publicznej.



Michał Moskal

Poseł na Sejm RP X kadencji, prawnik, absolwent Uniwersytetu Warszawskiego. Były szef Gabinetu Wiceprezesa Rady Ministrów Jarosława Kaczyńskiego. Członek sejmowej Komisji Obrony Narodowej, zaangażowany w sprawy bezpieczeństwa państwa i gospodarki, zwłaszcza w kontekście strategicznych interesów Polski na forum międzynarodowym. Przewodniczący Rady Eksperckiej Obserwatorium Rozwoju Gospodarki i Demokracji (ORGiD) – konserwatywnego think-tanku analizującego kluczowe procesy polityczne i gospodarcze, skupionego na budowie silnych instytucji państwowych oraz wspieraniu rozwoju społeczno-gospodarczego kraju.



Maciej Olczak

Prezes Zarządu (CEO) Energy Market Observer sp. z o.o. (ENMARO). Ekspert ds. zarządzania i dyrektor wykonawczy z 30 letnim doświadczeniem który specjalizuje się w sektorze energetycznym, a w szczególności w operacjach Offshore Upstream i Downstream, inżynierii i komercyjnych aspektach projektów inwestycyjnych.

Absolwent Uniwersytetu Morskiego w Gdyni roku 1996. Karierę rozpoczął w sektorze Offshore jako inżynier elektryk, a następnie został inżynierem projektu i menedżerem. W 2013 roku ukończył program zarządzania w Harvard Business School w Bostonie.

W 2008 roku założył Asia Connecting Centre Pte. Ltd. (ACC). Firma założona w Singapurze oferuje usługi związane z prowadzeniem projektów kapitałowych w obszarze ropy, gazu i operacji Offshore.

Od 2017 roku pełni także funkcję prezesa zarządu spółki Energy Market Observer sp. z o.o. (ENMARO) działającej w Polsce. Firma wspiera klientów w realizacji strategicznych projektów rozwoju morskich farm wiatrowych, produkcji i transportu niskoemisyjnego wodoru i paliw alternatywnych, transportu morskiego skroplonego CO2 do sekwestracji (CCS) oraz dekarbonizacji transportu morskiego.

Jest członkiem i wykładowcą Society of Petroleum Engineers. Pełni rolę doradcy zarządów spółek zagranicznych i funduszy inwestycyjnych. Uczestnik oraz wykładowca wielu seminariów i szkoleń.



Jacek Sasin

Jacek Sasin, były wicepremier oraz minister aktywów państwowych (2019–2023), odpowiadał za nadzór nad spółkami Skarbu Państwa, które wytwarzają około 15% polskiego PKB. W tym okresie nadzorował połączenie PKN Orlen z Grupą Lotos, Energą i PGNiG, co doprowadziło do utworzenia jednego z największych koncernów multienergetycznych w Europie Środkowej. Był to projekt wzmacniający bezpieczeństwo energetyczne Polski i jej pozycję gospodarczą w regionie.

Pełnienie przez niego urzędu przypadło na czas pandemii COVID-19 oraz agresji Rosji na Ukrainę. W okresie pandemii koordynował zaangażowanie spółek Skarbu Państwa w działania wzmacniające bezpieczeństwo zdrowotne i odporność gospodarczą kraju. Wartość środków przeznaczonych na walkę ze skutkami pandemii przekroczyła 200 mln zł, a inwestycje spółek osiągnęły rekordowy poziom 39 mld zł w 2021 roku.

Po wybuchu wojny na Ukrainie nadzorowane przez niego spółki odegrały ważną rolę w działaniach wzmacniających bezpieczeństwo Polski i niezależność gospodarczą regionu. Utrzymały stabilność funkcjonowania kluczowych sektorów gospodarki oraz wspierały rozwój infrastruktury energetycznej i logistycznej istotnej dla bezpieczeństwa RP. Działania te wpisywały się w realizację polskiej racji stanu poprzez ograniczanie wpływów Rosji w regionie.

Od 2011 roku nieprzerwanie sprawuje mandat posła na Sejm RP kolejnych kadencji. Obecnie, w X kadencji Sejmu, zasiada w Komisji Finansów Publicznych.

W latach 2009–2010 pełnił funkcję zastępcy szefa Kancelarii Prezydenta RP Lecha Kaczyńskiego. Wcześniej był wojewodą mazowieckim (2007) oraz kierownikiem Urzędu Stanu Cywilnego m.st. Warszawy (2004–2006).



płk rez. Marcin Stachowski

Zastępca dyrektora Departamentu Strategii Bezpieczeństwa w Biurze Bezpieczeństwa Narodowego. Absolwent studiów wojskowych i podyplomowych z zakresu bezpieczeństwa narodowego oraz licznych kursów doskonalących realizowanych w kraju i za granicą. Obecnie doktorant Szkoły Doktorskiej Akademii Sztuki Wojennej.

W trakcie zawodowej służby wojskowej zajmował stanowiska dowódcze i sztabowe na wszystkich poziomach dowodzenia Sił Zbrojnych RP. Uczestniczył w pracach narodowych i sojuszniczych zespołów zajmujących się planowaniem operacyjnym oraz programowaniem rozwoju Sił Zbrojnych RP. Kierował pracami nad opracowaniem narodowego dokumentu

doktrynalnego „Wojska Obrony Terytorialnej w operacji" (DD-3.40) oraz współtworzył nowy model rekrutacji i naboru do Sił Zbrojnych RP, wdrażany w latach 2022–2024. Brał udział w pracach nad Strategią Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2020 i 2026 roku. Uczestnik misji pokojowej.

Autor i współautor publikacji poświęconych współczesnemu środowisku bezpieczeństwa, wojskom obrony terytorialnej, zarządzaniu kryzysowemu, ochronie ludności, obronie cywilnej oraz rezerwom osobowym.



Paweł Stańczyk

Paweł Stańczyk - wiceprezes Instytutu Strategii Narodowej, członek Rady Energii i Zasobów Naturalnych przy Prezydencie RP.

Menedżer z wieloletnim doświadczeniem w zarządzaniu projektami inwestycyjnymi, logistycznymi i infrastrukturalnymi. Pełnił kierownicze funkcje w spółkach sektora paliwowego i energetycznego, m.in. jako prezes OLPP i PERN, jednego z najważniejszych operatorów infrastruktury przesyłowej i magazynowej ropy naftowej oraz paliw w Europie Środkowej. Dwukrotnie zasiadał w radzie dyrektorów Polskiej Organizacji Przemysłu i Handlu Naftowego.



Dariusz Stefaniuk

Dariusz Stefaniuk – poseł na Sejm RP IX i X kadencji, samorządowiec i działacz społeczny. Urodzony 10 maja 1981 roku w Białej Podlaskiej. Absolwent politologii na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie oraz studiów podyplomowych w Szkole Głównej Handlowej. W latach 2006–2014 był radnym Rady Miasta Biała Podlaska, w latach 2014–2018 prezydentem miasta, a następnie wicemarszałkiem województwa lubelskiego. Od 2019 roku nieprzerwanie sprawuje mandat posła na Sejm RP, reprezentując okręg nr 7 (Chełm). W X kadencji pełni funkcję wiceprzewodniczącego Komisji Cyfryzacji, Innowacyjności i Nowych Technologii. W działalności parlamentarnej koncentruje się na rozwoju Polski Wschodniej, cyfryzacji, bezpieczeństwie oraz wspieraniu samorządów. Prywatnie jest mężem i ojcem trójki dzieci.



DR INŻ. PAWEŁ SZCZESZEK

Paweł Szczeszek, dr inż, absolwent Politechniki Śląskiej (Szkoła Doktorów) oraz Politechniki Częstochowskiej (studia magisterskie). W latach 2003-2004 przewodniczący Zarządu Krajowego Niezależnego Zrzeszenia Studentów (NZS). Menadżer z wieloletnim doświadczeniem w dużych grupach kapitałowych oraz administracji samorządowej. Związany z branżą energetyczną od ponad 20 lat. Kierował grupami energetycznymi takimi jak Tauron oraz Enea. Zarządzał również przedsiębiorstwami z branży ciepłowniczej (KOGENERACJA, PEC JASTRZĘBIE ZDRÓJ). Obecnie członek Rady Energii i Zasobów Naturalnych przy Prezydencie Rzeczypospolitej Polskiej . Członek Rady Programowej Fundacji SET.



MICHAŁ ŚMIGIELSKI

Michał Śmigielski – Morska Agencja Gdynia, w której pracuje od 2000 roku, w 2017 powołany na Prezesa Zarządu MAG.

Od grudnia 2025 roku został wybrany na Przewodniczącego Rady interesantów Portu Gdynia.

Podczas swojej pracy zawodowej czynnie uczestniczył w projektach związanych z logistyką największych polskich inwestycji związanych z różnymi gałęziami gospodarki w tym energetyką konwencjonalną, przemysłem chemicznym – ostatnie projekty to m.in Olefiny 3 czy Polimery Police, a wcześniej w latach 2006–2012 transporty urządzeń wiertniczych dla Polskiej Nafty i Gazu (obecnie Exalo). Od 2008 roku zajmuje się logistyką lądowych farm wiatrowych, głównie przeładunkami portowymi oraz transportem elementów turbin wiatrowych. W latach 2010 – 2025 udział MAG w rynku realizacji przeładunków portowych farm wiatrowych w Polsce wyniósł ponad 90%. Od samego początku rozwoju morskich farm wiatrowych w Polsce czynnie uczestniczy w pracach specjalistycznych grup roboczych w tematyce logistyki portowej. W latach 2021 – 2023 Koordynator grupy IV porozumienia sektorowego Morskiej Energetyki Wiatrowej przy Ministerstwie Klimatu zajmującej się Logistyką portową morskich farm wiatrowych i ich wpływu na regiony nadmorskie. W latach 2019–2023 Lider grupy portowej Polskiego Stowarzyszenia Energetyki Wiatrowej.

Wykładowca na Politechnice Gdańskiej na podyplomowych studiach morskiej energetyki wiatrowej z zakresu logistyki portowej.

Morska Agencja Gdynia jako jedna z niewielu polskich firm uczestniczy w logistyce pierwszych morskich farm wiatrowych budowanych w polskiej strefie Morza Bałtyckiego. W ostatnich latach temat udziału polskich firm w budowie morskich farm wiatrowych jest tematem wielu

wystąpień Prezesa Michała Śmigielskiego podczas konferencji branżowych i paneli dyskusyjnych organizowanych przez stowarzyszenia branżowe czy inne podmioty zajmujące się tematami związanymi z transformacją energetyczną Polski.



Paweł Turowski

Główny specjalista Departamentu Strategii Bezpieczeństwa w Biurze Bezpieczeństwa Narodowego. Absolwent kierunku historia w Instytucie Historycznym Uniwersytetu Warszawskiego. Od 2007 r. związany z Biurem Bezpieczeństwa Narodowego, gdzie pracował w departamentach zajmujących się problematyką prawa, bezpieczeństwa pozamilitarnego, bezpieczeństwa wewnętrznego oraz strategii bezpieczeństwa.

Specjalizuje się w zagadnieniach odporności państwa, zagrożeń hybrydowych, bezpieczeństwa energetycznego, cyberbezpieczeństwa, ochrony infrastruktury krytycznej, przeciwdziałania dezinformacji oraz zagrożeń poniżej progu konfliktu kinetycznego. Uczestniczył w pracach zespołów opracowujących Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014, 2020 i 2026 roku. Od 2019 r. pełni funkcję eksperta NATO w dziedzinie bezpieczeństwa energetycznego.

Uczestnik specjalistycznych kursów i projektów realizowanych m.in. w NATO School Oberammergau, George C. Marshall European Center for Security Studies w Garmisch-Partenkirchen, Euro-Atlantic Resilience Centre w Bukareszcie oraz Kwaterze Głównej NATO w Brukseli. Wykładowca akademicki współpracujący m.in. z Krajową Szkołą Administracji Publicznej, Akademią Górniczo-Hutniczą, Politechniką Rzeszowską oraz Collegium Civitas.



Paweł Wiszniewski

Zastępca Dyrektora Departamentu Technologii Przełomowych w Biurze Bezpieczeństwa Narodowego. Analityk i konsultant z wieloletnim doświadczeniem w sektorze publicznym oraz organizacjach międzynarodowych, w tym ONZ, UNESCO i UNDP. Specjalizuje się w zagadnieniach bezpieczeństwa narodowego, ze szczególnym uwzględnieniem technologii przełomowych (EDT), w tym systemów bezzałogowych, a także przeciwdziałania zagrożeniom hybrydowym i dezinformacji, komunikacji strategicznej oraz zarządzania cyberbezpieczeństwem w wymiarze krajowym i transatlantyckim. W swojej pracy koncentruje się na wykorzystaniu nowych technologii dla wzmacniania zdolności państwa oraz rozwijaniu współpracy międzyinstytucjonalnej w obszarze bezpieczeństwa.



Mateusz Wodejko

Wiceprezes Fundacji „Security-Energy-Technology". W swojej karierze zawodowej m.in. pełnił funkcje Wiceprezesa Zarządu ds. finansowych KGHM Polska Miedź, Poczty Polskiej oraz PERN i OLPP. Kierował pracami obszaru finansów a także inwestycji, IT i transformacji energetycznej. Jest absolwentem Szkoły Głównej Handlowej na kierunku Finanse i Bankowość oraz Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego.



gen. bryg. rez. pilot Dariusz Wroński

Dowodził elitarnymi jednostkami Wojska Polskiego. 49 pułk śmigłowców bojowych, 25 Brygada Kawalerii Powietrznej, 1 Brygada Lotnictwa Wojsk Lądowych. W Iraku, dowodził Samodzielną Grupą Powietrzno-Szturmową. Był Szefem Wojsk Aeromobilnych i Zmotoryzowanych, Szefem Szkolenia Wojsk Lądowych do czasu transformacji WP w 2014 r. Dyrektorem Programów Operacyjnych pozyskania śmigłowców dla SZRP. Prezesem Zarządu Centrum Wdrożeniowo-Produkcyjnego ITWL Sp. z o.o., tworząc firmę od podstaw. Przewodził zespołowi ds. ewaluacji Edukacja Dla Bezpieczeństwa przy MEiN. Jest doradcą, ekspertem lotniczym i wojskowym, a także Członkiem Rady Programowej Fundacji SET i Polskiej Platformy Bezpieczeństwa Wewnętrznego. Prowadzi działalność gospodarczą w obszarze zarządczym oraz doradztwa na rzecz Bezpieczeństwa i Obrony. Uczestniczył w pracach instytucji międzynarodowych, m.in.: Połączonego Dowództwa NATO ds. Transformacji (ACTA), Grupy NATO ds. Uzbrojenia Wojsk Lądowych (NAAG), Europejskiej Agencji Obrony (EDA), Stowarzyszenia FINABEL, OCCAR, JAPCC. Ukończył szkolenia w USA i Francji w zakresie Bojowego Poszukiwania i Ratownictwa na polu walki. Szkolenia w zakresie Członków Rad Nadzorczych z Udziałem Skarbu Państwa i Zamówień Publicznych. W 2017 roku uzyskał koncesję na obrót specjalny. Poświadczenia bezpieczeństwa NATO i UE.



Kasjan Wyligała

Kasjan Wyligała – menedżer i ekspert z wieloletnim doświadczeniem w sektorach surowcowym, górniczym i energetycznym. Obecnie pełni funkcję Prezesa Zarządu Permia 1 oraz Partnera w Keystone Partners, gdzie rozwija projekty związane z surowcami krytycznymi, istotnymi dla bezpieczeństwa gospodarczego i strategicznego Polski.

Specjalizuje się w pozyskiwaniu i rozwoju projektów górniczych, współpracy z inwestorami oraz zagadnieniach bezpieczeństwa surowcowego.

Pełnił funkcję Prezesa Zarządu Lubelskiego Węgla Bogdanka S.A., jednej z największych spółek górniczych w Europie. Odpowiadał za opracowanie i wdrożenie strategii rozwoju przedsiębiorstwa oraz identyfikację nowych projektów surowcowych. W okresie jego zarządzania spółka osiągnęła rekordowe wyniki finansowe.

Doświadczenie zdobywał również w KGHM Polska Miedź S.A., gdzie odpowiadał za nadzór właścicielski nad krajowymi i zagranicznymi spółkami Grupy KGHM. Zasiadał w organach spółek sektora surowcowego działających w Polsce, Kanadzie i Chinach, uczestnicząc w realizacji projektów o międzynarodowej skali.

Jest absolwentem Wydziału Prawa i Administracji Uniwersytetu Warszawskiego, studiów MBA w Instytucie Nauk Ekonomicznych PAN oraz programów z zakresu finansów korporacyjnych i innowacji realizowanych m.in. we współpracy ze Szkołą Główną Handlową i Stanford Research Institute. Ukończył również studia podyplomowe z geologii górniczej na Akademii Górniczo-Hutniczej w Krakowie.

Posiada stopień Dyrektora Górniczego I stopnia oraz został odznaczony odznaką „Zasłużony dla Górnictwa RP" za wkład w rozwój polskiego sektora górniczego.



Artur Zawisza

Artur Zawisza – Prezes (w latach 2016–2021 wiceprezes) Unii Producentów i Pracodawców Przemysłu Biogazowego i Biometanowego (używającej skrótu UPEBBI od angielskojęzycznego brzmienia nazwy), inwestor i menedżer w branży biogazu oraz konsultant doradzający inwestorom w sektorze energetycznym. Członek Rady Koordynacyjnej Porozumienia na rzecz Rozwoju Sektora Biogazu i Biometanu. Członek rad programowych: Forum Miasteczek Polskich, Konferencji Energetycznej EuroPOWER & OZE POWER, Międzynarodowego Kongresu EKOFORUM. W latach 1997-99 dyrektor gabinetu politycznego w Kancelarii Prezesa Rady Ministrów Jerzego Buzka, w latach 2001–2007 poseł na Sejm, przewodniczący sejmowej Komisji Gospodarki i komisji śledczej ds. sektora bankowego oraz członek Komisji Finansów Publicznych. Od 2008 r. bezpartyjny prywatny przedsiębiorca, działacz gospodarczy i komentator życia społecznego. Prezes Fundacji Patriotyzm i Wolność oraz Klubu Narodowej Myśli Politycznej „Votum"



Tomasz Zdzikot

Radca prawny, Zastępca Przewodniczącego Rady Bezpieczeństwa i Obronności przy Prezydencie RP, Przewodniczący Rady Fundacji SET Security-Energy-Technology.

W latach 2015-2018 Podsekretarz Stanu, a następnie Sekretarz Stanu w MSWiA, w latach 2018-2020 Sekretarz Stanu w MON, pełniący również funkcję Pełnomocnika MON ds. Bezpieczeństwa Cyberprzestrzeni, Prezes Zarządu Poczty Polskiej (2020-2022) i Prezes Zarządu KGHM Polska Miedź (2022-2024).










KONGRES
SET. POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO
W NIESTABILNYM ŚWIECIE?
DEBATA


KONGRES
SET. POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO
W NIESTABILNYM ŚWIECIE?
PANEL


KONGRES
SET. POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO
W NIESTABILNYM ŚWIECIE?
PANEL


KONGRES
SET. POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO
W NIESTABILNYM ŚWIECIE?
PANEL


KONGRES POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO W NIESTABILNYM ŚWIECIE?
PANEL


KONGRES POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO W NIESTABILNYM ŚWIECIE?
PANEL


KONGRES POLSKA AMBITNA
JAK WZMACNIAĆ PAŃSTWO W NIESTABILNYM ŚWIECIE?
PANEL
CYBERPOTĘGA CZY CYFROWE PERYFERIA?



ISBN 978-83-68653-18-2