STYCZEŃ 2026

JAK ZBUDOWAĆ STRATEGICZNĄ SUWERENNOŚĆ TECHNOLOGICZNĄ W OBSZARZE AI UNIKAJĄC AUTARKII

PIIT
Komitet Przełomowych Technologii
Polskiej Izby Informatyki i Telekomunikacji

JAK ZBUDOWAĆ STRATEGICZNĄ SUWERENNOŚĆ TECHNOLOGICZNĄ W OBSZARZE AI UNIKAJĄC AUTARKII

STANOWISKO KOMITETU PRZEŁOMOWYCH TECHNOLOGII
POLSKIEJ IZBY INFORMATYKI I TELEKOMUNIKACJI

Koncepcja: dr Izabella Krzemińska, Borys Stokalski,
Wsparcie merytoryczne: Piotr Brzyski, Maciej Lewandowski,

Komitet Przełomowych Technologii, PIIT.

WPROWADZENIE

Suwerenność technologiczna stała się ważnym elementem dyskusji o strategii rozwoju zarówno w Polsce jak i w Europie.

Polska Izba Informatyki i Telekomunikacji zaangażowana jest od lat w konstruktywną debatę i konsultacje towarzyszące formułowaniu strategii cyfryzacji, polityk technologicznych, oraz regulacji technologii cyfrowych w Polsce i Unii Europejskiej.

Autorzy prezentują niniejsze stanowisko na temat istoty suwerenności technologicznej, oraz scenariuszy jej implementacji w obszarze Sztucznej Inteligencji, z nadzieją, że stanowić ono będzie wartościową inspirację dla osób odpowiedzialnych za te zagadnienia.

Mając świadomość, że przedstawione w dokumencie koncepcje rozwiązań wymagają w wielu aspektach uszczegółowienia autorzy gotowi są do ich pogłębienia i rozwoju we współpracy z decydentami, instytucjami i organizacjami zainteresowanymi wykorzystaniem zawartych w stanowisku propozycji rozwiązań.

SUWERENNOŚĆ TECHNOLOGICZNA

PODSTAWY SUWERENNOŚCI

Pojęcie suwerenności technologicznej można definiować szeroko jako zdolność do niezakłóconego zabezpieczenia, funkcjonowania i rozwoju państwa na wszystkich polach, gdzie zasadnicze znaczenie odgrywa technologia i związane z nią zasoby (kompetencje, infrastruktura, dane, prawa własności intelektualnej).

Zapewnienie takiej zdolności również w sytuacjach nadzwyczajnych (katastrofy, zaburzenia w globalnych łańcuchach dostaw, kryzysy polityczne, konflikty zbrojne) charakteryzuje kraje i gospodarki o wysokiej suwerenności technologicznej.

Przykłady tak rozumianych “pól suwerenności”:

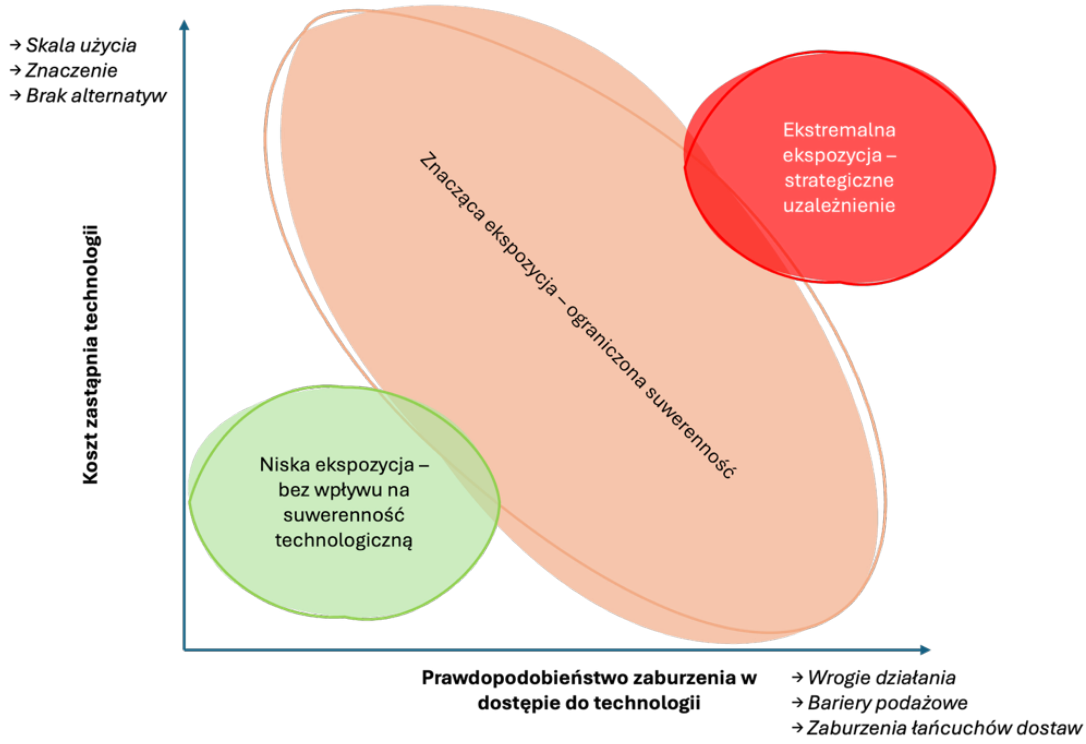
- Infrastruktura: logistyczno transportowa, system finansowy, system energetyczny, łączność
- Ochrona zdrowia
- Bezpieczeństwo publiczne
- Badania naukowe
- Rozwój usług i produktów cyfrowe, w tym usługi i produkty AI+ (wykorzystujące AI i inne przełomowe technologie)

Poziom suwerenności technologicznej można interpretować i mierzyć w kategoriach zarządzania ryzykiem. Ekspozycja na ryzyko zaburzenia w dostępie do krytycznych

rozwiązań dla poszczególnych pól to iloczyn prawdopodobieństwa wystąpienia zaburzenia i kosztu zastąpienia technologii w danym polu. Suwerenność to odwrotność ekspozycji – im większa ekspozycja, tym bardziej ograniczona suwerenność.

Suwerenność często utożsamiamy z postawą (podejściem, strategią postępowania) wobec tych zagrożeń. Z tego punktu widzenia można określić trzy fundamentalne postawy w zapewnieniu suwerenności technologicznej:

1. **Samowystarczalność** (suwerenność autarkiczna) – całkowita niezależność w



Rys 1. Suwerenność technologiczna z perspektywy zarządzania ryzykiem

zakresie projektowania, produkcji i wdrażania technologii, w tym pełny krajowy łańcuch dostaw (hardware, software, infrastruktura, talenty). Taka postawa nie jest szeroko dostępna dla Polski, ze względu na brak zasobów przemysłowych (w szczególności w zakresie produkcji mikroelektroniki i hardware'u), kapitału oraz skali rynkowej. Może mieć zastosowanie jedynie w ograniczonym zakresie w wybranych elementach łańcucha wartości do eliminacji obszarów ekstremalnej ekspozycji na ryzyko zaburzeń.

2. **Multisourcing** (suwerenność systemowa) – postawa zapewnienia niezależności poprzez systemową kontrolę kluczowych elementów łańcucha wartości oraz stosów/platform technologicznych, przy jednoczesnym korzystaniu z wybranych komponentów zewnętrznych. Jej istotą jest obniżanie ekspozycji na ryzyko zaburzeń dzięki standaryzacji wymagań w domenach,

segmentacji rozwiązań i dostawców, umowom ramowym określającym gwarancje dostępności itp. To podejście, powszechnie stosowane przez duże organizacje musi być systematycznie budowane w dłuższym terminie jako narzędzie implementacji polityk i strategii cyfrowego rozwoju przy optymalnym wykorzystaniu lokalnych kompetencji i kluczowych partnerstw.

3. **Utylitaryzm funkcjonalny** (zarządzany outsourcing) – zdolność do korzystania z gotowych rozwiązań zewnętrznych w sposób względnie niezależny, dzięki odpowiednim umowom, certyfikacji, interoperacyjności i redundancji dostawców. Ten poziom wydaje się być najszybciej dostępny natychmiast, choć z ograniczoną możliwością kontroli nad rozwojem technologii.

PODEJŚCIE SYSTEMOWE DLA POLSKI

W warunkach polski, podstawowym celem w procesie budowania suwerenności technologicznej powinno być osiągnięcie i utrzymanie suwerenności systemowej w wybranych krytycznych obszarach, z zabezpieczeniem funkcjonalnym tam, gdzie pełna kontrola jest niemożliwa lub nieopłacalna.

Doświadczenia organizacji wdrażających w praktyce multisourcing wskazuje na to, że suwerenność systemowa opierać się musi o skuteczne mechanizmy ładu (governance). Program suwerenności technologicznej łączy decyzje polityczne (domeny, cele, priorytety, „political return") i techniczne (mapy drogowe rozwoju technologii, segmentacja rozwiązań i partnerów strategicznych, określanie domen i procedur zakupowych, powoływanie i finansowanie projektów kluczowych dla rozwoju technologii). Konsekwencje techniczne wyborów politycznych mają charakter długookresowy, wymagają konsekwencji w działaniu zapewniającej skuteczność i efektywność. Podejście systemowe wymaga w związku mechanizmów pozwalających w sposób transparentny równoważyć te dwie perspektywy.

Co do zasady niezbędne są tutaj dwa mechanizmy o charakterze horyzontalnym (międzyresortowym) – kierunkowy, bazujący na krajowej agendzie rozwoju technologii definiujący założenia strategii suwerenności, oraz implementacyjny, o charakterze nadzorczym lub nadzorczo-wykonawczym.

W obszarze zapewnienia suwerenności technologicznej w Polsce brakuje takich mechanizmów, co prowadziło do reaktywnej polityki i przypadkowej adaptacji. Strategia suwerenności powinna to zmienić: budując trwałą, krajową zdolność do wyznaczania i egzekucji kierunków rozwoju technologicznego, również w warunkach kryzysowych i sytuacji nacisku geopolitycznego. Taka zdolność powinna być zinstytucjonalizowana tworząc „bastion suwerenności".

Administracja posiada przy tym mechanizmy które można udoskonalić i zaadoptować do tych nowych celów. W obszarze technologii cyfrowych warto wspomnieć choćby Krajowe Ramy Interoperacyjności, stworzone w MC, zatwierdzone na poziomie KRMC i kształtujące rozwój technologii w sektorze publicznym od 2012.

W obszarze technologii cyfrowych, w tym AI, Krajowe Ramy Interoperacyjności mogłyby stać się fundamentem dla poszerzonych Krajowych Ram Suwerenności Technologicznej (KRST) –zestawu zasad, które nie tylko zapewniają spójność techniczną systemów państwa, lecz także budują realną zdolność Polski do działania na własnych warunkach w obszarze kluczowych technologii, w tym sztucznej inteligencji. Aby KRST faktycznie wpływały na wzrost suwerenności, konieczne są trzy kroki.

Po pierwsze, ewolucja prawna: przygotowanie nowelizacji obecnego rozporządzenia KRI w kierunku KRST, wprowadzającej wymogi suwerennościowe, takie jak kontrola nad danymi, zapewnienie mechanizmów zastępowalności rozwiązań i technologii, a następnie uchwalenie ustawy określającej proces nadzorczy i certyfikacyjny.

Po drugie, ciągła integracja z procesem zamówień publicznych i finansowaniem: systematyczna segmentacja, stopniowe wprowadzanie wiążących profili technicznych KRST jako wymagań przetargów, oraz centralnych umów ramowych zapewniających interoperacyjność, audytowalność i możliwość strategicznego multisourcingu.

Po trzecie, wdrożenie mechanizmów egzekucji i transparentności: monitorowanie ex ante i ex post prowadzone przez stały zespół wspierający, publiczny rejestr systemów AI i komponentów spełniających standardy KRST, a także powiązanie oceny zgodności z możliwością finansowania projektów i ich utrzymania w sektorze publicznym. Dzięki temu KRST stałyby się operacyjną konstytucją technologiczną państwa, stopniowo wzmacniając niezależność od zagranicznych dostawców i zwiększając odporność Polski na wstrząsy geopolityczne oraz ryzyka związane z gwałtownym rozwojem technologii.

KRST to przykład zmian możliwych do zrealizowania w relatywnie prosty sposób. Nie wyczerpują one jednak potrzeb związanych z efektywnym i skutecznym zapewnienieniem suwerenności technologicznej.

SUWERENNOŚĆ W OBSZARZE TECHNOLOGII AI

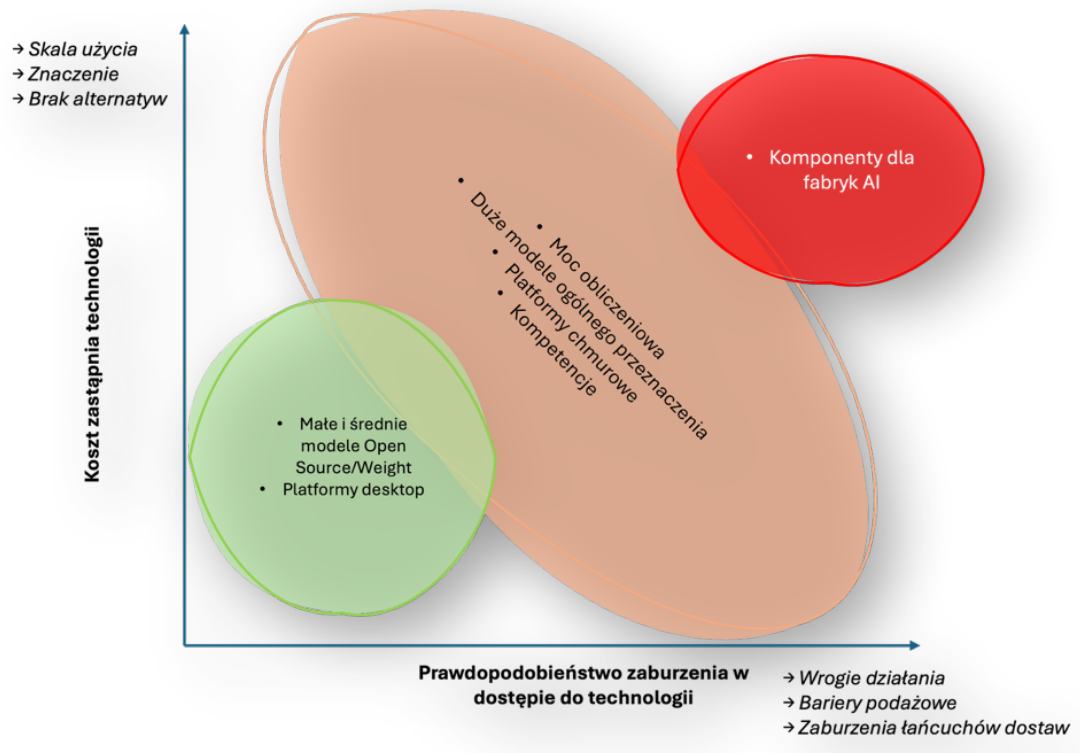
Suwerenność technologiczna w obszarze AI oznacza: zdolność do samodzielnego tworzenia, testowania i wdrażania konkurencyjnych systemów AI zgodnych z wartościami i interesami kraju, dzięki dostępowi użytkowników i twórców produktów AI do alternatywnych rozwiązań i zasobów w łańcuchu wartości AI (w tym – elementów stosu technologicznego).

Tak rozumiana suwerenność to zdolność która rodzi dylematy (tradeoffs) związane ze strategicznymi wyborami, szansami i ryzykami jakie z nich wynikają, oraz ich konsekwencjami ekonomicznymi. W tym sensie suwerenność nie jest kategorią absolutną, lecz wynikiem optymalizacji tych wyborów z punktu widzenia przyjętych celów, kryteriów i założeń.

W aktualnie toczonych dyskusjach mówi się głównie o specyficznych ryzykach (np uzależnienie od rozwiązań firm "Big Tech", utrata specjalistów) pomijając pozostałe aspekty – w tym tak fundamentalny aspekt jak koszt suwerenności niezbędny i możliwy do poniesienia.

FUNDAMENTALNE ZAŁOŻENIA DLA SUWERENNOŚCI W OBSZARZE TECHNOLOGII AI

1. Celem suwerenności w obszarze technologii AI jest umożliwienie wykorzystania przez Polskę szans rozwoju gospodarki i dobrostanu społecznego płynących z wytwarzania i wdrażania innowacji AI poprzez ograniczenie negatywnego wpływu aktorów realizujących niezależne, często konkurencyjne agendy: globalne korporacje technologiczne, wrogie Państwa i aktorzy poza-państwowi.
2. Polska jako kraj średniej wielkości musi postrzegać swoją suwerenność technologiczną jako element globalnych łańcuchów wartości, ze zdefiniowanymi polami specjalizacji oraz kluczowymi, elastycznymi partnerstwami, opartymi na parytecie wzajemnych korzyści.
3. Zapewnienie suwerenności wymaga zaangażowania zasobów, proporcjonalnych do zagrożeń i oczekiwanych rezultatów.
4. Suwerenność technologiczna nie oznacza izolacji ani autarkii, lecz zdolność do podejmowania własnych decyzji i zachowania kontroli nad krytycznymi komponentami ekosystemu AI. kluczowym są kompetencje. Polska dysponuje kapitałem ludzkim w obszarze AI i software, który musi zostać strategicznie wykorzystany, zamiast zasilać obce podmioty.



Rys 2. Przykładowa analiza zagrożeń dla suwerenności AI.

5. Działania muszą być realistyczne i strategia nie może zakładać niemożliwego (np. całkowitej niezależności sprzętowej), ale powinna koncentrować się na obszarach, w których możliwe jest realne wzmocnienie suwerenności.
6. Kluczowe ekspozycje dla suwerenności, zarysowane na rysunku 2, AI dotyczą (1) komponentów niezbędnych dla budowy mocy obliczeniowej i dostęp do mocy obliczeniowej pozwalającej na efektywne kosztowo budowanie dużych modeli (2) dużych modeli ogólnego przeznaczenia stosowanych jako platforma rozwiązań AI (3) kompetencje specjalistów i ekspertów (4) dostęp do platform chmurowych niezbędnych dla budowy i dystrybucji produktów AI. Należy podkreślić że tego typu analiza uwzględniać musi specyfikę poszczególnych „pól suwerenności" w których postrzeganie zagrożeń oraz wybór znaczenie technologii mogą się istotnie różnić.
7. Krytyczne komponenty wspierające suwerenność to: lokalne modele foundation models (trening i tuning), kontrola nad warstwą danych i pipeline'ów, niezależna infrastruktura compute oraz systemy oceny i certyfikacji.
8. Partnerstwa międzynarodowe powinny być zawierane z pozycji siły negocjacyjnej, wspieranej przez realne aktywa strategiczne i kompetencje.

PUNKT WYJŚCIA: ZASTOSOWANIA (USE CASES)

Strategiczna suwerenność technologiczna Polski w obszarze sztucznej inteligencji nie polega na samowystarczalności ani replikowaniu rozwiązań największych graczy (USA, Chiny). Kluczem jest rozsądny bilans trzech elementów:

- realnych szans na sukces produktowy,
- kosztów rozwoju oraz
- ryzyka zależności.

Ten bilans budują konkretne zastosowania – zwłaszcza w sektorach o dużym znaczeniu gospodarczym i presji modernizacyjnej (priorytetowe pola suwerenności technologicznej w obszarze AI). To tam powstaje popyt na modele, dane, kompetencje i infrastrukturę. Konkretne zastosowania generują wartość, stwarzają warunki do weryfikacji wartości technologii zarówno w wymiarze technicznym (czy działa) jak i biznesowym (czy jej stosowanie jest opłacalne). To one, a nie modele per se, budują zdolność kraju do skalowalnej, niezależnej innowacji.

Konkretne zastosowania warto wyprowadzać z wcześniej określonych scenariuszy strategicznych i zagrożeń systemowych. Takie podejście scenariuszowe pozwala lepiej zarządzać ryzykiem systemowym i długofalowym horyzontem niż orientacja na punktowe zastosowania, identyfikowane ad hoc.

Alternatywą, pozwalającą uniknięcie nadmiernie złożonych (i często nieoczywistych – co utrudnia podejmowanie decyzji) deliberacji jest model hybrydowy, polegający na wyłonieniu kilku flagowych zastosowań, które pozostają istotne w przewidywanych

scenariuszach rozwoju sytuacji geopolitycznej i technologicznej (tzw. invariant cases), przy jednoczesnej dbałości o zdolność do elastycznej adaptacji strategii przy zachodzących zmianach. Zastosowania nie powinny więc determinować struktury całej strategii, lecz stanowić jej pierwszy „krąg operacjonalizacji" – zintegrowany z mechanizmami oceny ryzyka, komponentami infrastruktury suwerennościowej oraz działaniami bastionu operacyjnego.

WYMIARY POLSKIEJ SUWERENNOŚCI AI

Z perspektywy strategii zorientowanej na zastosowania i elastyczne scenariusze rozwoju, kluczowe wymiary suwerenności powinny odpowiadać na konkretne potrzeby wdrożeniowe, nie zaś tworzyć zamknięty katalog celów. Można jednak wyróżnić następujące obszary jako **strukturalne warunki suwerenności operacyjnej**:

1. **Dane i pipeline'y ML** - powinny być przechowywane, wersjonowane i audytowalne w kraju. Ich kontrola jest niezbędna zarówno dla ochrony interesu publicznego, jak i efektywności adaptacyjnej modeli.
2. **Modele i kod** - trenowane i dokumentowane w sposób audytowalny, z interoperacyjnością między. Dotyczy to zwłaszcza modeli średniej wielkości. Analiza modeli repozytorium Hugginface wydaje się wskazywać, że w wielu klasach modeli ta grupa stanowi modele najchętniej adaptowane do zastosowań.
3. **Infrastruktura** - krajowe zasoby powinny pełnić funkcję strategicznego bufora oraz stabilizatora kosztów. Kluczowe są tu otwarte standardy, lokalna kontrola i mechanizmy harmonogramowania. Standardy te kluczowe są dla kolejnego punktu (4)
4. **Wymienność dostawców usług compute** - możliwa dzięki otwartym standardom (wspomnianym w punkcie 3) i konteneryzacji, chroniąca przed vendor lock-in.
5. **Narzędzia wspomagające projektowanie i testowanie AI –** czyli narzędzia i platformy inżynierii AI, w tym również te oparte na AI, niezbędne do zapewnienia bezpieczeństwa, jakości i zgodności z wymogami regulacyjnymi (audyt, testy, ewaluacja).
6. **Ekosystem innowacji** -oparty o sektorowe *piaskownice innowacji*, centra inkubacji i skalowania, gdzie popyt spotyka się z eksperymentem, a doświadczenia z procesów innowacji wspiera rozwój i upowszechnianie wiedzy.
7. **Mechanizmy bilansujące i rozliczeniowe** - np. systemy harmonogramowania, tokenizacji kosztów, lokalne schedulery zdolne do zarządzania zasobami z wielu źródeł.

Uporządkowanie powyższych wymiarów nie oznacza konieczności ich równoczesnej realizacji – są one podporządkowane **priorytetyzacji wynikającej ze scenariuszy strategicznych i flagowych zastosowań**

SUWERENNOŚĆ AI A KLUCZOWE ZASOBY

Budowanie suwerenności AI musi odnosić się do kluczowych zasobów, w sposób najbardziej fundamentalny wpływających na zdolność do osiągania celów suwerenności, a więc stanowiących też obszar interwencji państwa. Należą do nich: wiedza, dane, infrastruktura obliczeniowa oraz komponenty stosu technologicznego (narzędzia, platformy itp.).

WIEDZA

Podstawowym elementem jest wiedza, t.j. posiadane wykształcenie oraz umiejętności. Kształcenie kadr naukowych oraz wspieranie praktycznych umiejętności tworzenia rozwiązań AI determinują zdolność gospodarki do zachowania zdolności rozwoju AI. O ile jednak ważny dla suwerenności jest wzrost liczby dobrze przygotowanych specjalistów, a także rosnący udział polskiej nauki w przełomowych badaniach, ten obszar nie może być obszarem „samowystarczalności". Zaangażowanie w rozwój polskich rozwiązań i technologii AI ekspertów i specjalistów spoza Polski, oraz udział polskich badaczy w realizacji ambitnych, przełomowych projektów jest ważnym czynnikiem dynamizującym rozwój wiedzy i sukces jej zastosowań. Polska powinna pozostawać radykalnie otwarta na wszelkie kooperacje (tworzenie centrów R&D, udział w konsorcjach naukowych, otwarcie rynku pracy na zagranicznych specjalistów), pod warunkiem troski o atrakcyjność Polski jako miejsca pracy dla najlepszych specjalistów AI.

DANE

Zdrowy komercyjny rynek danych, chroniący przed eksploatacją ze strony globalnych techno-korporacji to jeden z warunków szybkiego i bardziej masowego rozwoju produktów i usług AI. Komercyjny rynek danych to czynnik równie ważny – o ile nie ważniejszy – jak otwarte dane. O ile w obszarze otwartych danych Polska ma w skali UE osiągnięcia to kwestia komercyjnego rynku danych wymaga zdecydowanych działań otwierający możliwość ograniczonego, oparte o mechanizmy biznesowe współdzielenia danych treningowych, oczywiście w sposób respektujący prywatność, interes ekonomiczny, czy prawo własności intelektualnej.

INFRASTRUKTURA I STOS TECHNOLOGICZNY

Infrastruktura obliczeniowa – od superkomputerów po „edge GPU" – **jest niezbędna, ale nie wystarczy**. Celem nie jest posiadanie mocy obliczeniowej dla niej samej, lecz stworzenie dostępu do:

- przestrzeni eksperymentu i testowania (dla uczelni, start-upów, przemysłu),
- miejsca narodowej refleksji technologicznej (modele, dane, pipeline'y),
- bufora strategicznego w momentach kryzysu (kosztowego, prawnego, geopolitycznego).

Dlatego celem nie jest replikowanie skali największych globalnych podmiotów, lecz zapewnienie dostępności do technologii (w szczególności do **komplementarnego, kontrolowalnego i przewidywalnego środowiska obliczeniowego) na potrzeby budowy, rozwoju i utrzymania ciągłości działania** strategicznych zastosowań – przede wszystkim tych o znaczeniu publicznym, krytycznym lub systemowym.

SYSTEMOWA SUWERENNOŚĆ INFRASTRUKTURY

Polska potrzebuje strategii, która łączy **efektywną dystrybucję zasobów obliczeniowych (compute mix)** z **dynamicznym systemem piaskownic innowacyjnych (innovation sandboxes)**, realizowanych przez branżowe konglomeraty. W tym modelu krajowe zasoby:

- zapewniają niezależność strategiczną,
- równoważą ceny,
- gwarantują ciągłość krytycznych projektów,
- wspierają edukację i eksperyment.

Równocześnie, europejskie i międzynarodowe zasoby (np. Gaia-X, EuroHPC) są włączane na zasadach interoperacyjnych i pod kontrolą do portfela usług obliczeniowych, zaś sektorowe **piaskownice innowacji** (prowadzone przez liderów innowacji w sektorach, wspieranych przez państwo) stają się mechanizmem **ciągłego testowania, urynkowienia i skalowania innowacji**, bez potrzeby budowania biurokratycznych programów grantowych.

Celem nie jest tylko subsydiowanie infrastruktury, ale **strategiczne przypisanie jej do flagowych zastosowań**, w których państwo pełni funkcję integratora i współ-inwestora (poprzez system PFR Ventures i programy dotacyjne).

Finansowanie infrastruktury powinno być powiązane z oceną spełniania celów suwerenności operacyjnej, w tym:

- poziomem otwartości (open model / open data),
- użyciem w projektach publicznych i edukacyjnych,
- wdrożeniami spełniającymi wymogi oceny ryzyk i wartości (zgodnie z AI Act).

Taki komplementarny **compute mix** nie tylko umożliwia działanie niezależnie od globalnych napięć, ale pozwala też rozwijać własne modele w sposób kosztowo

zrównoważony – szczególnie istotny w przypadku średniej wielkości modeli dedykowanych lokalnym problemom.

Sektorowe piaskownice innowacyjne (prowadzone przez liderów innowacji w sektorach, wspieranych przez państwo) powinny być uzupełnione o stały mechanizm ciągłego urynkowienia i skalowania innowacji, bez potrzeby budowania biurokratycznych programów grantowych.

Optymalnym podejściem do realizacji celów suwerenności w obszarze infrastruktury obliczeniowej jest multisourcing (podejście systemowe). Mix możemy realnie zbudować wyłącznie w kooperacji z partnerami globalnymi i europejskimi z racji (1) poziomu niezbędnych nakładów inwestycyjnych oraz (2) konieczności działania w skali bez której nie jest możliwe zapewnienie efektywności kosztowej takich inwestycji (w szczegłoności w zakresie zapotrzebowania na energię).

Warunkiem niezbędnym dla realizacji takiej strategii jest umiejętność oszacowania polskiego zapotrzebowania na zasoby obliczeniowe i systematyczna aktualizacja tego oszacowania w sposób pozwalający zapewnić podaż tych zasobów w stopniu odpowiadającym popytowi oraz pozwalającym na kontrolę kosztów dla gospodarki. Można takie działanie porównać do zarządzania rezerwami walutowymi przez NBP.

Niezbędne jest zbudowanie modelu prognostycznego uwzględniającego kluczowe źródła popytu:

- budowa i doskonalenie srednich i dużych modeli AI (pipeline'y ML), w tym potrzeby piaskownic regulacyjnych i innowacyjnych
- eksploatacja skomercjalizowanych dużych i średnich modeli AI (inferencja)
- badania naukowe

REALIZACJA

ROLA BASTION OPERACYJNEGO

W ramach strategii suwerenności technologicznej postulujemy stworzenie trwałego, stabilnego i odpornego na zmiany polityczne „bastionu operacyjnego". To instytucja odpowiedzialna za realizację strategii suwerenności, integrator kompetencji oraz przede wszystkim gwarant ciągłości działania i odporności w sytuacjach kryzysowych o charakterze lokalnym jak i międzynarodowym.

Bastion powinien być zespołem kompetentnych specjalistów działających na styku technologii, regulacji i interesu publicznego, niezależnie od polityki. Umocowanie bastionu w strukturach państwa powinno łączyć niezależność ze skutecznością w realizacji zadań związanych z podnoszeniem i utrzymaniem poziomu suwerenności technologicznej

Zadania bastion obejmują:

- Transparentne monitorowanie poziomu suwerenności AI i skuteczności implementacji jej założeń i celów
- Budowę i utrzymanie podstawowej infrastruktury suwerennościowej: otwarte modele, repozytoria, compute, narzędzia MLOps, systemy certyfikacji w koordynacji z interesariuszami publicznymi i prywatnymi.
- Projektowanie i prowadzenie piaskownic sektorowych oraz mechanizmów oceny ryzyk, standardów bezpieczeństwa i zgodności z wartościami.
- Nadzór nad krajowym systemem piaskownic regulacyjnych i eksperymentalnych w zakresie AI, w ścisłej współpracy z regulatorami sektorowymi oraz przedstawicielami środowiska naukowego i liderami innowacji w sektorach.
- Utrzymanie zdolności do niezależnej walidacji modeli i usług AI wdrażanych w krytycznych obszarach państwa, w tym w administracji publicznej i infrastrukturze strategicznej.

Bastion powinien być powiązany ze strukturami kontroli strategicznej państwa i działać niezależnie od kadencyjnych fluktuacji politycznych, przy stabilnym finansowaniu.

Bastion jest koncepcją ambitną jednak realną – zarówno w świetle ustroju państwa, jak i doświadczeń polskiej administracji. W strukturach państwa funkcjonują już instytucje o podobnych cechach: trwałe, odporne na zmiany polityczne, posiadające własne zaplecze eksperckie i zdolność do zarządzania krytyczną infrastrukturą (patrz – tabela poniżej).

Przykład	Aspekty Bastionu	Sposób realizacji
NBP	Niezależność i trwałość • Stabilność systemowa • Prognozowanie i zarządzanie zasobami krytycznymi	Konstytucyjnie gwarantowana niezależność • Systemy rozliczeń i clearingowe • Monitorowanie podaży i popytu w systemie finansowym
GPW	Transparentność i neutralność • Reguły gry między państwem a rynkiem • Infrastruktura zaufania	Operacyjny operator rynku kapitałowego • Oddzielenie regulacji (KNF) od implementacji • Jasne, przejrzyste mechanizmy działania
KNF	Nadzór regulacyjny • Piaskownice regulacyjne • Wsparcie dla innowacji w sektorach krytycznych	Standaryzacja procesów i wymogów • Ochrona uczestników rynku finansowego • Piaskownica fintech jako model dla AI
ULC	Bezpieczeństwo sektorowe • Integracja z regulacjami międzynarodowymi • Certyfikacja systemów autonomicznych	Procedury certyfikacji dronów i autonomicznych systemów lotniczych • Współpraca z EASA i ICAO • Nadzór nad krytycznym sektorem technologicznym

Przykłady takie jak NBP, GPW, KNF czy ULC pokazują, że Polska potrafi tworzyć podmioty łączące niezależność instytucjonalną z operacyjną skutecznością i dużym znaczeniem dla całego ekosystemu. Bastion może być kolejnym krokiem – skoncentrowanym na strategicznych technologiach i sztucznej inteligencji, analogicznie do tego, jak NBP dba o stabilność finansową, a GPW zapewnia transparentne funkcjonowanie rynku kapitałowego

Szczególnym przykładem instytucjonalnego zapewnienia suwerenności jest Komponent Wojsk Obrony Cyberprzestrzeni. KWOC to jeden z filarów suwerenności państwa oraz ważny "motor innowacji" polskich sił zbrojnych. Zespół KWOC to wszystronna i silna merytorycznie organizacja. Angażuje się na cyfrowym teatrze działań, a jednocześnie zapewnia "sieciocentryczność" polskich sił zbrojnych. Dostarcza bezpieczną, mobilną komunikację cyfrowej. Wspiera interoperacyjności systemów zapewnienia świadomości sytuacyjnej i dowodzenia. Wdraża rozwiązania AI w zadaniach w których szybkość i trafność decyzji buduje przewagę operacyjną.

Suwerenność technologiczna jako element strategii sojuszu NATO oraz naszej własnej strategii i polityki w zakresie ciągłej modernizacji sił zbrojnych musi uwzględniać ogromną złożoność współczesnych systemów. Kluczem do tego aby technologia w domenie bezpieczeństwa narodowego była jednocześnie suwerenna i nowoczesna jest interoperacyjność systemów, oparta na standardach i precyzyjnie zdefiniowanych założeniach.

WARUNKI BRZEGOWE DLA SKUTECZNEJ REALIZACJI STRATEGII

Strategia suwerenności technologicznej w obszarze AI może być skutecznie wdrażana tylko przy spełnieniu określonych **warunków brzegowych** – niezbędnych dla trwałości, skalowalności i odporności przyjętego modelu:

1. **Stabilne i selektywne finansowanie** – niezbędne są mechanizmy finansowania infrastruktury i projektów strategicznych (zwłaszcza flagowych zastosowań), które nie podlegają doraźnym wahaniom budżetowym ani presji programów grantowych. Oznacza to m.in.:
    - wprowadzenie zasad finansowania infrastruktury zależnych od jej zgodności z celami suwerenności,
    - współfinansowanie na zasadach partnerstwa publiczno prywatnego, lub poprzez system PFR Ventures projektów prywatnych o wysokim potencjale strategicznym,
    - selektywne wspieranie ekosystemów piaskownic branżowych ukierunkowane na zwiększenie skuteczności procesów inkubacji i skalowania produktów.
2. **Koordynacja i stałość instytucjonalna** - konieczne jest powołanie **bastionu operacyjnego** o stabilnym statusie i klarownym mandacie, odpornego na

zmiany polityczne. Bastion ten powinien pełnić funkcje nadzorcze, integracyjne i walidacyjne – niezależnie od bieżącej koniunktury politycznej.

3. **Punkt ciężkości strategicznej** - strategia wymaga istnienia instytucjonalnego punktu ciężkości, który wyznacza kierunki, pilnuje spójności działań oraz zapewnia szybką reakcję w sytuacjach kryzysowych. Stanowi go narodowa agenda rozwoju technologii AI, której źródłem może być np. polityka AI, strategia cyfryzacji lub inne dokumenty określające kierunki i priorytety rozwoju. Muszą one być – z uwagi na tempo rozwoju technologii – systematycznie aktualizowane z perspektywy naukowej, zmian w ekosystemie technologicznym, oraz zmian otoczenia gospodarczego i politycznego.
4. **Interoperacyjność i otwartość standardów** - infrastruktura, modele, pipeline'y i narzędzia MLOps muszą być zgodne z otwartymi standardami, aby uniknąć uzależnień i zapewnić wymienność komponentów. Jest to warunek działania strategii „compute mix".
5. **Wzmacnianie lokalnych kompetencji** - kluczowe jest systemowe wzmacnianie kompetencji technicznych (AI/ML, MLOps, AI safety) oraz regulacyjnych (risk assessment, auditing, compliance), także poprzez tworzenie lokalnych ośrodków ekspertyzy i edukacji dla sektorów kluczowych.
6. **Włączenie środowisk użytkowników AI** -strategia musi uwzględniać głos użytkowników (zwłaszcza w administracji, edukacji, służbie zdrowia, przemyśle) – ponieważ to ich problemy wyznaczają kształt zastosowań i potrzeb infrastrukturalnych.

RYZYKA I DETERMINANTY ZEWNĘTRZNE

Każda strategia suwerenności operacyjnej musi być odporna nie tylko na ryzyka techniczne, ale także na presję geopolityczną, ekonomiczną i kulturową. Nadrzędną funkcją bastionu operacyjnego jest wykrywanie tych zagrożeń i reagowanie z wyprzedzeniem.

Ryzyka systemowe:

- **Uzależnienie infrastrukturalne** - ryzyko dominacji zewnętrznych dostawców compute i usług AI (np. API foundation models), skutkujące brakiem realnej kontroli nad wdrożeniami.
- **Fragmentacja działań krajowych** -brak jednego punktu ciężkości prowadzi do powielania inwestycji, niespójnych standardów i marnotrawienia zasobów.
- **Presja regulacyjna bez narzędzi** - obowiązki wynikające z AI Act i innych przepisów mogą przekroczyć realne zdolności państwa i firm, jeśli nie powstanie odpowiednia infrastruktura oceny zgodności, testowania i walidacji.

- **Brak flagowych zastosowań** - jeśli strategia nie znajdzie konkretnego zakorzenienia w sektorach priorytetowych, stanie się zbiorem abstrakcyjnych celów bez realnej trakcji.

Determinanty zewnętrzne:

- **Skala rynku** – Polska samodzielnie nie posiada rynku o skali umożliwiającej budowę pełnego ekosystemu AI; konieczna jest współpraca europejska i partnerstwa międzynarodowe.
- **Ceny energii i dostępność surowców** - efektywność inwestycji w compute zależy bezpośrednio od kosztów energii i bezpieczeństwa dostaw (np. GPU, pamięci).
- **Niestabilność geopolityczna** - strategie AI państw trzecich (USA, Chiny) mogą wpływać na dostępność technologii, komponentów i partnerstw.
- **Globalny wyścig innowacyjny** - szybki rozwój foundation models, agentów i systemów multimodalnych wymaga zdolności do błyskawicznego eksperymentowania, co oznacza konieczność elastycznego modelu sandbox + bastion.

KONKLUZJA

Strategiczna suwerenność technologiczna w AI to nie wielkość GPU, lecz zdolność do tworzenia i wdrażania modeli odpowiadających na własne potrzeby – na własnych warunkach, z zachowaniem kontroli i z możliwością wyboru.

Strategiczna suwerenność technologiczna w obszarze AI **nie oznacza samowystarczalności** ani budowy pełnego autarkicznego ekosystemu. Jest to **zdolność do działania na własnych warunkach** – w warunkach ograniczeń zasobowych, presji geopolitycznej i szybkich zmian technologicznych.

Wersja operacyjna tej suwerenności opiera się na kluczowych filarach:

1. **Elastyczna strategia scenariuszowa** - umożliwiająca reagowanie na zmienne warunki zewnętrzne, poprzez wybór ścieżek działania zależnych od poziomu kontroli, znaczenia sektora i dostępności zasobów.
2. **Zakotwiczenie w flagowych zastosowaniach** - które uruchamiają realny popyt, pozwalają testować modele wdrożeniowe i budować kompetencje w sposób praktyczny. Zastosowania są nie tylko celem, lecz mechanizmem mobilizacji i weryfikacji całej strategii.
3. **Bastion operacyjny i compute mix** - jako gwarant trwałości, ciągłości i kontroli. Bastion pozwala zarządzać infrastrukturą, kompetencjami i zgodnością wdrożeń z wartościami państwa. Compute mix zapewnia stabilność, redundancję i możliwość eksperymentu bez uzależnień.
4. Sektorowe piaskownice innowacyjne – prowadzone przez konsorcja branżowe, łączące popyt gospodarki z eksperymentem technologicznym, wspierane regulacyjnie i infrastrukturalnie przez państwo.
5. System monitorowania i prognozowania zapotrzebowania na zasoby AI – analogiczny do zarządzania rezerwami strategicznymi, umożliwiający planowanie inwestycji i kontrolę kosztów dla gospodarki.
6. Interoperacyjność i otwarte standardy – w modelach, danych, narzędziach i infrastrukturze, aby uniknąć uzależnienia od pojedynczych dostawców.

Strategia ta wymaga jednocześnie realnych, choć selektywnych inwestycji, instytucjonalnej ciągłości (zapewnianej przez “bastion operacyjny”), oraz interoperacyjności technologicznej. Dla skutecznej realizacji niezbędnym warunkiem jest włączenie środowisk użytkowników i ekspertów a w sferze operacyjnego zarządzania - transparentne zarządzanie ryzykiem i kosztami.

Polska może zbudować systemową suwerenność, nie uczestnicząc w cyberwyścigu ale budując odpowiedzialne,efektywne innowacje AI, z rozsądną, operacyjną architekturą możliwości, wspartą właściwym wyborem zastosowań, strategią oraz odpornością instytucjonalną.