KONGRES OBYWATELSKI

Suwerenność cyfrowa jako fundament bezpieczeństwa państwa

DR KRZYSZTOF GAWKOWSKI
Wiceprezes Rady Ministrów, Minister Cyfryzacji, Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Wojna w Ukrainie pokazała, że współczesna geopolityka nie toczy się wyłącznie na polach bitew. Rozstrzyga się również w sieciach energetycznych, systemach administracyjnych i algorytmach platform cyfrowych. W warunkach permanentnej presji hybrydowej państwo, które nie kontroluje swojej infrastruktury cyfrowej, nie jest zdolne egzekwować prawa wobec globalnych podmiotów technologicznych ani skutecznie chronić przestrzeni informacyjnej, traci realną zdolność działania. Suwerenność cyfrowa staje się jednym z kluczowych filarów bezpieczeństwa narodowego.

Nowy wymiar bezpieczeństwa

Współczesna geopolityka zmieniła swoje narzędzia. Obok czołgów i rakiet pojawiły się algorytmy, infrastruktura chmurowa, łańcuchy dostaw półprzewodników oraz platformy cyfrowe zdolne kształtować debatę publiczną i zachowania społeczne. Rywalizacja państw dotyczy nie tylko terytorium, lecz także kontroli nad danymi, standardami technologicznymi i architekturą cyfrowego ładu.

Polska znajduje się w centrum tej zmiany. Na styku geopolitycznym Wschodu i Zachodu, a jednocześnie w środowisku cyfrowym zdominowanym przez globalne korporacje. W tym podwójnym napięciu suwerenność zyskuje nowy wymiar. To już nie tylko kwestia granic i siły militarnej, lecz także zdolności do kontrolowania własnej przestrzeni cyfrowej.

W realiach wojny hybrydowej państwo, które nie panuje nad infrastrukturą cyfrową, traci część swojej sprawczości. Suwerenność cyfrowa staje się warunkiem bezpieczeństwa narodowego.

Od modernizacji do odporności

Przez lata cyfryzacja była postrzegana przede wszystkim jako narzędzie modernizacji i wzrostu gospodarczego. Wojna hybrydowa ujawniła jednak jej drugi wymiar: instrumentu presji i destabilizacji.

Cyberataki na infrastrukturę energetyczną, wodno-kanalizacyjną czy systemy administracyjne nie są dziś incydentami. Stały się elementem stałej, zorganizowanej presji. Działania w cyberprzestrzeni mają charakter długotrwały i ukierunkowany nie tylko na zakłócenie usług czy kradzież danych, lecz także na podważenie zaufania do państwa i wywołanie chaosu społecznego.

W tym kontekście suwerenność cyfrowa przestaje być projektem rozwojowym. Oznacza zdolność państwa do utrzymania ciągłości działania kluczowych systemów, od energetyki po administrację lokalną, nawet w warunkach stałego zagrożenia.

Wobec wrogich działań hybrydowych suwerenność cyfrowa przestaje być projektem rozwojowym. Oznacza zdolność państwa do utrzymania ciągłości działania kluczowych systemów, od energetyki po administrację lokalną, nawet w warunkach stałego zagrożenia.

Państwo jako architekt odporności

Budowa suwerenności cyfrowej wymaga spójnej architektury instytucjonalnej. Kluczową rolę odgrywa Krajowy System Cyberbezpieczeństwa, który zapewnia jednolite standardy ochrony, klarowny podział kompetencji oraz sprawną wymianę informacji między sektorem publicznym i prywatnym. Po blisko 6 latach legislacyjnej batalii Polska zaczyna właśnie wdrażanie tego systemu, nowe regulacje weszły w życie 3 kwietnia br.

W warunkach rosnącej liczby cyberataków opóźnienia legislacyjne czy brak koordynacji bezpośrednio obniżają poziom bezpieczeństwa. Suwerenność cyfrowa nie polega na izolacji, lecz na zdolności do skutecznego stanowienia i egzekwowania prawa.

Istotny jest także poziom lokalny. To samorządy odpowiadają za funkcjonowanie infrastruktury krytycznej: wodociągów, transportu czy systemów energetycznych, które coraz częściej stają się celami ataków. Wzmocnienie ich odporności oznacza inwestycje nie tylko w technologie, lecz także w kompetencje i systemy reagowania kryzysowego.

Technologia jako narzędzie wpływu

Rywalizacja geopolityczna coraz silniej przenosi się do sfery informacyjnej. Sztuczna inteligencja umożliwia tworzenie zaawansowanych treści dezinformacyjnych, trudnych do rozpoznania deepfake'ów, a algorytmy platform cyfrowych wzmacniają ich zasięg. Wojna o infrastrukturę toczy się równolegle z wojną o percepcję.

Suwerenność cyfrowa obejmuje więc również ochronę przestrzeni informacyjnej. Nie oznacza to administracyjnej kontroli treści, lecz budowę mechanizmów prawnych i instytucjonalnych ograniczających systemowe nadużycia oraz zapewniających przejrzystość działania platform.

Wolność słowa pozostaje fundamentem demokracji, ale nie może oznaczać bezradności wobec zorganizowanych operacji dezinformacyjnych. Państwo potrzebuje realnych narzędzi do szybkiego i sprawnego reagowania.

Wojna toczy się także o percepcję. Dlatego w trosce o naszą cyfrową suwerenność musimy również chronić naszą przestrzeń informacyjną. Wolność słowa nie może oznaczać bezradności wobec zorganizowanych operacji dezinformacyjnych.

Technodominacja: nowe oblicze zależności

Współczesna geopolityka obejmuje nie tylko relacje między państwami, lecz także rosnącą rolę globalnych korporacji technologicznych. Kontrolują one infrastrukturę cyfrową, standardy technologiczne i kluczowe kanały komunikacji,

wpływając tym samym na debatę publiczną i funkcjonowanie demokracji.

Zależność od ich ekosystemów ma charakter strukturalny. Im głębsza integracja administracji, biznesu i obywateli z globalnymi platformami, tym trudniejsze staje się zachowanie kontroli nad danymi i standardami bezpieczeństwa.

Suwerenność cyfrowa to również zdolność państwa do wyznaczania zasad funkcjonowania nowoczesnych technologii i platform cyfrowych w granicach interesu publicznego. Wymaga to efektywnych regulacji, które będą chroniły użytkowników także w cyfrowej rzeczywistości.

Suwerenność cyfrowa nie oznacza odcięcia się od globalnych technologii. Oznacza zdolność państwa do wyznaczania zasad ich funkcjonowania w granicach interesu publicznego.

Granice między rynkiem a interesem publicznym

Platformy cyfrowe stały się infrastrukturą współczesnych społeczeństw. Ich decyzje wpływają na debatę publiczną, bezpieczeństwo informacyjne i ochronę użytkowników.

Regulacja nie jest zaprzeczeniem wolności, lecz narzędziem przywracania równowagi. Europejskie rozwiązania, takie jak *Akt o usługach cyfrowych* (DSA), zwiększają przejrzystość i odpowiedzialność platform. Ostateczne rozstrzygnięcia w sporach dotyczących treści powinny należeć do niezależnych sądów, a nie być zależne od algorytmów czy arbitralnych decyzji.

Państwo, które nie potrafi egzekwować prawa wobec globalnych podmiotów technologicznych, traci sprawczość. Suwerenność cyfrowa oznacza zdolność do stosowania prawa w przestrzeni cyfrowej na równych zasadach jak poza nią.

Sojusz bez wasalizacji

Relacje transatlantyckie pozostają fundamentem bezpieczeństwa Polski. Współpraca militarna i polityczna wzmacnia stabilność regionu, jednak interesy korporacyjne nie zawsze są tożsame z interesami państw.

W realiach technodominacji współpraca sojusznicza często musi współistnieć z rywalizacją regulacyjną. Wyzwaniem jest pogodzenie lojalności sojuszniczej z zachowaniem autonomii decyzyjnej.

Suwerenność cyfrowa nie jest skierowana przeciwko żadnemu państwu. Jest odpowiedzią na asymetrię między globalnymi podmiotami technologicznymi a państwami narodowymi.

Cztery (powiązane ze sobą) filary suwerenności cyfrowej Polski to: odporność infrastrukturalna, sprawność instytucjonalna, podmiotowość regulacyjna i rozwój kompetencji technologicznych.

Europa jako przestrzeń współdzielonej suwerenności

W globalnej konkurencji pojedyncze państwo europejskie ma ograniczoną siłę oddziaływania. Dlatego suwerenność cyfrowa ma również wymiar europejski.

Wspólne regulacje, inwestycje w infrastrukturę i koordynacja polityk publicznych wzmacniają

pozycję całej Unii Europejskiej. W tym obszarze suwerenność narodowa i europejska wzajemnie się uzupełniają.

Cztery filary suwerenności cyfrowej

W polskich warunkach suwerenność cyfrowa opiera się na czterech wzajemnie powiązanych elementach:

1. **Odporność infrastrukturalna**: ochrona systemów kluczowych dla funkcjonowania państwa.

2. **Sprawność instytucjonalna**: jasna architektura zarządzania i skuteczne wdrażanie regulacji.

3. **Podmiotowość regulacyjna**: zdolność do wyznaczania zasad funkcjonowania platform cyfrowych.

4. **Rozwój kompetencji technologicznych**: inwestycje w sztuczną inteligencję, centra danych i kadry.

Suwerenność cyfrowa nie jest pojedynczym działaniem, lecz systemem powiązanych polityk publicznych, które muszą być realizowane równolegle.

Suwerenność jako zdolność wyboru

Najpoważniejszym zagrożeniem dla państw średniej wielkości jest utrata zdolności samodzielnego wyboru. Suwerenność cyfrowa nie oznacza izolacji ani samowystarczalności technologicznej. Oznacza możliwość decydowania o własnych standardach bezpieczeństwa, modelu regulacyjnym i kierunkach rozwoju.

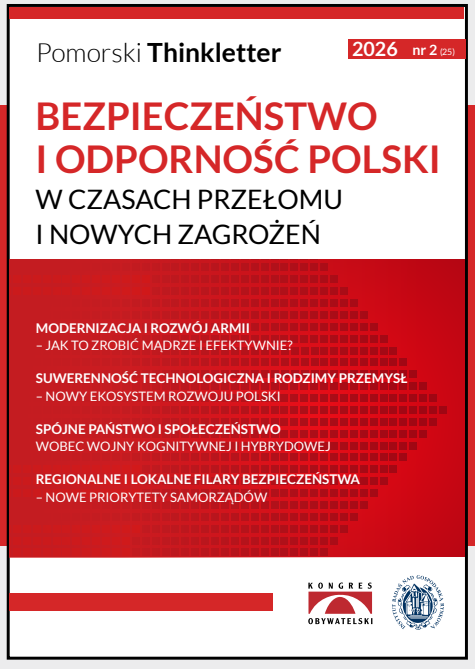
Najpoważniejszym zagrożeniem dla państw średniej wielkości jest utrata zdolności samodzielnego wyboru. Jeśli Polska chce zachować podmiotowość geopolityczną, musi być również podmiotem w świecie cyfrowym.

W świecie, w którym granice państw przecinają światłowody i linie kodu, ochrona infrastruktury, danych i przestrzeni informacyjnej staje się miarą realnej suwerenności. Państwo, które chce zachować podmiotowość geopolityczną, musi być również podmiotem w świecie cyfrowym. ■

O AUTORZE

dr **Krzysztof Gawkowski** – Wiceprezes Rady Ministrów, Minister Cyfryzacji, Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Doktor nauk humanistycznych, absolwent studiów podyplomowych z zakresu prawa pracy na Uniwersytecie Warszawskim. W latach 2002–2010 Radny Rady Miejskiej w Wołominie, 2010-2014 Radny Sejmiku Województwa Mazowieckiego. Od 2019 roku Poseł na Sejm RP z okręgu bydgoskiego, Członek Sejmowej Komisji Cyfryzacji, *Innowacyjności i Nowoczesnych Technologii*. W latach 2019-2023 Przewodniczący Klubu Parlamentarnego Lewicy, od 2021 roku Wiceprzewodniczący partii Nowa Lewica. Wykładowca akademicki, ekspert w zakresie cyberbezpieczeństwa państwa. W latach 2015-2020 Członek Komitetu Technicznego Polskiego Komitetu Normalizacyjnego. Autor licznych artykułów naukowych oraz publikacji monograficznych poświęconych nowym technologiom, cyfryzacji, sztucznej inteligencji i cyberbezpieczeństwu, w tym książki *Cyberkolonializm. Poznaj świat cyfrowych przyjaciół i wrogów*, wyróżnionej przez Polskie Towarzystwo Informatyczne.

Partnerzy



POBIERZ CAŁĄ PUBLIKACJĘ

www.**kongresobywatelski**.pl