Ku suwerenności technologicznej Europy. ProtectEU jako kształtowanie modelu zarządzania bezpieczeństwem technologicznym EU

KONTEKST RYWALIZACJI TECHNOLOGICZNEJ

Współczesne problemy bezpieczeństwa w Europie wymagają kompleksowego podejścia, które wykracza poza tradycyjne koncepcje obrony i obejmuje szeroki spektrum zagrożeń hybrydowych, cyberzagrożeń oraz geopolitycznych wyzwań. W obliczu zmieniającego się krajobrazu bezpieczeństwa, charakteryzującego się nasilającymi się atakami na infrastrukturę krytyczną, cyberprzestępczością oraz działaniami wrogich państw obcych, Unia Europejska stanęła przed koniecznością redefinicji modelu zarządzania bezpieczeństwem wewnętrznym w tym bezpieczeństwem technologicznym. Komisja Europejska odpowiedziała na te wyzwania, prezentując 1 kwietnia 2025 roku strategię ProtectEU - Europejską Strategię Bezpieczeństwa Wewnętrznego, która wyznacza nowe standardy ochrony europejskiego społeczeństwa i gospodarki. Dokument ten stanowi fundamentalny element szerszej wizji bezpiecznej i odpornej Europy, uzupełniając Strategię Unii Gotowości oraz Europejską Białą Księgę Obrony, a jego znaczenie wykracza daleko poza kwestie bezpieczeństwa wewnętrznego, obejmując także aspekty suwerenności technologicznej i strategicznej autonomii.

KLASYFIKACJA POLITYK I POJĘĆ W OBSZARZE BEZPIECZEŃSTWA TECHNOLOGICZNEGO UE

Dokument ten można potraktować jako próbę systematyzacji i syntezy poszczególnych podejść odnoszących się do bezpieczeństwa technologicznego i wskazać zakres jego realizacji w obszarze suwerenności technologicznej, suwerenności cyfrowej i autonomii strategicznej. Przedstawione poniżej definicje mają charakter autorski i zostały opracowane na podstawie dokumentu REPowerEU oraz własnych analiz i wniosków badawczych. Stanowią odpowiedź na potrzebę uporządkowania podejść odnoszących się do bezpieczeństwa technologicznego w dokumentach strategicznych UE.

Bezpieczeństwo technologiczne można uznać za stan, w którym technologie, systemy oraz infrastruktury technologiczne są chronione przed zagrożeniami i ryzykami a ich

DOI: https://doi.org/10.36735/FHTY6993

funkcjonowanie jest zapewnione w sposób odporny i niezawodny. Obejmuje to zarówno ochronę fizycznych jak i cyfrowych systemów, zapewnienie ciągłości usług (szczególnie infrastruktury krytycznej), implementację nowoczesnych technologii zabezpieczeń, skoordynowane działania w zakresie certyfikacji, monitoringu oraz reagowania na zagrożenia.

Definicja ta odnosi się do wskazanych wcześniej trzech głównych polityk: suwerenności technologicznej, suwerenności cyfrowej i strategicznej autonomii. W dokumencie podkreśla się, że bezpieczeństwo technologiczne ma strategiczne znaczenie dla utrzymania stabilności, odporności i funkcjonowania Unii Europejskiej w obliczu obecnych zagrożeń hybrydowych, cyberzagrożeń oraz geopolitycznych wyzwań, a także dla zapewnienia bezpieczeństwa wewnętrznego i ochrony praw podstawowych obywateli UE.

Wykres 1.: Filary bezpieczeństwa technologicznego UE

Źródło: opracowanie własne.

Suwerenność technologiczna rozumiana jest jako zdolność Unii do kierowania rozwojem i wdrażaniem nowych technologii, minimalizowania zależności technologicznych od podmiotów zewnętrznych oraz zwiększania własnych zdolności w zakresie technologii strategicznych i technologii kluczowych jak i coraz silniej odnosi się do bezpieczeństwa w obszarze łańcuchów wartości.

Suwerenność cyfrowa polega na zapewnieniu Unii zdolności do bezpiecznego przechowywania, przetwarzania i przesyłania danych oraz na budowie europejskiej infrastruktury cyfrowej. To także kontrola nad strategicznymi zasobami i technologiami cyfrowymi. Wiąże się bezpośrednio z zabezpieczeniami infrastruktury cyfrowej i komunikacyjnej oraz do ochrony strategicznych zasobów danych UE przed zagrożeniami zewnętrznymi i cyberatakami.

Autonomia strategiczna odnosi się do zdolności Unii do samodzielnego podejmowania działań w zakresie bezpieczeństwa, obrony i przemysłu obronnego, bez nadmiernej

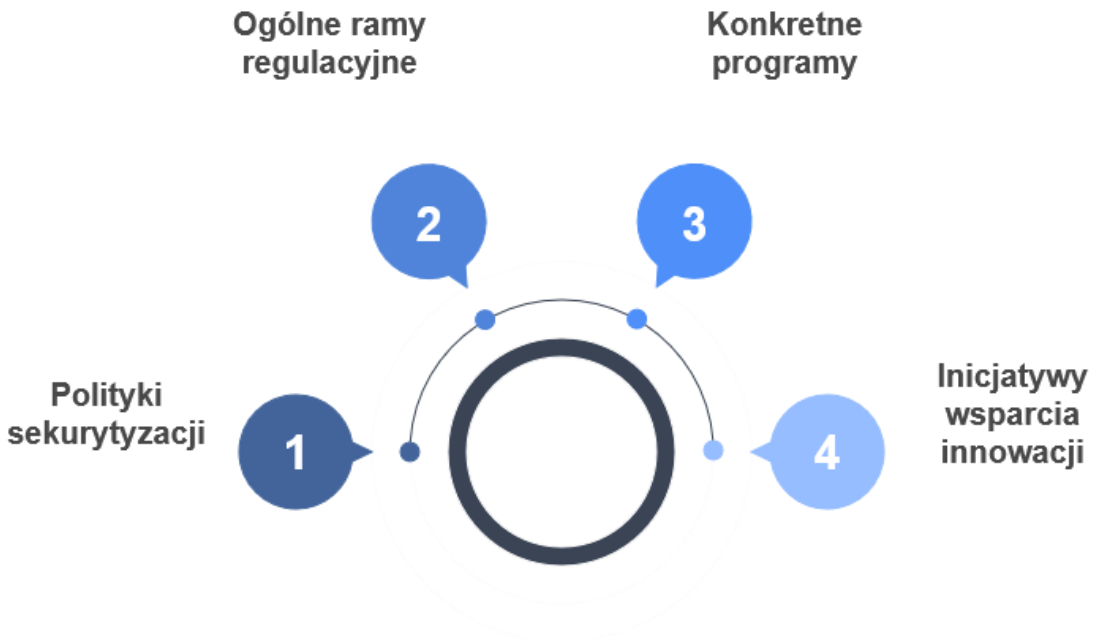
DOI: https://doi.org/10.36735/FHTY6993

zależności od podmiotów spoza UE. Obejmuje rozwój i nabywanie zdolności obronnych w UE, ochronę infrastruktury krytycznej, wzmocnienie zdolności operacyjnych oraz zdolność do skutecznej reakcji na zagrożenia hybrydowe i inne formy działań wrogich. Autonomia strategiczna stanowi fundament dla bezpieczeństwa wewnętrznego i jest wspierana przez polityki przemysłowe UE oraz koordynację na szczeblu unijnym i państw członkowskich.

PROTECTEU JAKO PRÓBA KSZTAŁTOWANIA MODELU ZARZĄDZANIA BEZPIECZEŃSTWEM TECHNOLOGICZNYM UE

Wśród wielu dokumentów strategicznych odnoszących się do bezpieczeństwa technologicznego ProtectEU wyróżnia się wskazaniem technologii, które można określić za strategiczne z punktu widzenia bezpieczeństwa wewnętrznego UE. Dla sekurytyzacji tychże obszarów technologicznych i technologii powołuje się lub usprawnia mechanizmy i narzędzia wdrożenia polityk ochrony infrastruktury krytycznej oraz łańcuchów dostaw zgodnie z politykami suwerenności technologicznej, suwerenności cyfrowej i autonomii strategicznej. Wśród nich są np.: metodyka testowania systemów przeciwdziałania dronom, SIS (System Informacyjny Schengen), akt o usługach cyfrowych, ramy

Wykres 2. Ramy modelu zarządzania bezpieczeństwem technologicznym UE



Źródło: opracowanie własne.

certyfikacji cyberbezpieczeństwa, europejską infrastrukturę komunikacji kwantowej (EuroQCI), monitoring i zabezpieczenia radiowe (przeciwdziałanie spoofingowi GNSS i zagłuszaniu). ProtectEU zapowiada kolejne rozwiązania prawne, jak akt o sytuacji

DOI: https://doi.org/10.36735/FHTY6993

nadzwyczajnej na rynku wewnętrznym i odporności rynku wewnętrznego (IMERA) lub odnosi się do już istniejących np.: dyrektywy dotyczące odporności podmiotów krytycznych (dyrektywa CER), dyrektywy o wysokim poziomie cyberbezpieczeństwa (dyrektywa NIS 2), czy akcie w sprawie surowców krytycznych (CRMA).

W ProtectUE wskazano następujące technologie, które są istotne dla bezpieczeństwa UE:

- kryptografia postkwantowa i technologie kwantowe,
- technologie biometryczne, urządzenia do wykrywania, drony,
- usługi chmurowe i telekomunikacyjne o wysokim poziomie cyberbezpieczeństwa,
- infrastruktura komunikacyjna i transportowa,
- systemy niejawne i korporacyjne systemy bezpieczeństwa UE,
- europejskie systemy certyfikacji cyberbezpieczeństwa.

Powyższe zestawienie wymaga uporządkowania technologii i obszarów technologicznych występujących w kontekście bezpieczeństwa Unii Europejskiej ze szczególnym uwzględnieniem trzech współistniejących polityk: **suwerenności technologicznej**, **suwerenności cyfrowej** oraz **strategicznej autonomii**. Warto przy tym dokonać identyfikacji dominujących obszarów technologicznych w UE, w kontekście bezpieczeństwa i odporności systemowej; przeanalizować istniejące synergie między obszarami technologicznymi a politykami bezpieczeństwa, by w przyszłości móc ocenić, które technologie wspierają konkretne cele strategiczne UE.

Tabela 1. Obszary technologiczne w architekturze bezpieczeństwa technologicznego UE: przegląd w obszarze polityk i priorytetyzacji

Technologia / Obszar technologiczny	Liczba wystąpień w dokumencie	Aspekty bezpieczeństwa i konteksty wykorzystania	Polityka dominująca	Polityki powiązane
Kryptografia postkwantowa	4	Zabezpieczenie komunikacji i danych przed atakami kwantowymi	Suwerenność cyfrowa	Suwerenność technologiczna, Autonomia strategiczna
Technologie kwantowe (QKD,	4	Infrastruktura EuroQCI; bezpieczeństwo	Suwerenność cyfrowa	Autonomia strategiczna

DOI: https://doi.org/10.36735/FHTY6993

wykrywanie kwantowe)		komunikacji; detekcja zagrożeń		
Sztuczna inteligencja (AI)	2	Wsparcie służb; analiza danych; automatyzacja zadań operacyjnych	Suwerenność technologiczna	Suwerenność cyfrowa
Protokoły internetowe najnowszej generacji	2	Bezpieczny i skalowalny internet; wzrost cyberbezpieczeństwa	Suwerenność cyfrowa	Suwerenność technologiczna
Chmura obliczeniowa	2	Cyberbezpieczeństwo danych i usług; wsparcie dla podmiotów krytycznych	Suwerenność cyfrowa	Autonomia strategiczna
Monitoring i zabezpieczenia częstotliwości radiowych (spoofing GNSS)	2	Ochrona przed zakłóceniami i atakami elektromagnetycznymi	Autonomia strategiczna	Suwerenność technologiczna
Bezzałogowe statki powietrzne (drony)	2	Testowanie i przeciwdziałanie szpiegostwu i atakom z użyciem dronów	Autonomia strategiczna	Suwerenność technologiczna
Systemy niejawne informatyczne	1	Odporność na zagrożenia kwantowe; ochrona informacji poufnych UE	Suwerenność technologiczna	Autonomia strategiczna
Internet rzeczy (IoT)	1	Integracja w sektorach bezpieczeństwa; kontrola infrastruktury krytycznej	Suwerenność cyfrowa	Suwerenność technologiczna
Technologie biometryczne	1	Kontrola graniczna; przeciwdziałanie zagrożeniom terrorystycznym	Autonomia strategiczna	Suwerenność technologiczna
Zaawansowane technologie wykrywania	1	Wykrywanie zagrożeń w infrastrukturze krytycznej	Autonomia strategiczna	Suwerenność technologiczna

DOI: https://doi.org/10.36735/FHTY6993

Usługi telekomunikacyjne	1	Cyberbezpieczeństwo usług komunikacyjnych i ich odporność	Suwerenność cyfrowa	Autonomia strategiczna
Systemy analizy i usuwania nielegalnych treści online	1	Eliminacja zagrożeń hybrydowych i manipulacji; przeciwdziałanie dezinformacji	Suwerenność cyfrowa	Autonomia strategiczna

Źródło: opracowanie własne na podstawie ProtectEU.

Wyraźnie widać, że technologie kwantowe i kryptografia postkwantowa pełnią rolę technologii o charakterze krytycznych w UE, choć ich rola obecnie wykracza poza bieżące potrzeby bezpieczeństwa. UE w ten sposób nie tylko reaguje, lecz próbuje kreować warunki dla geopolitycznej niezależności technologicznej, zanim nastąpi przymusowa adaptacja i prewencja.

Technologie chmurowe, sztuczna inteligencja i systemy przetwarzania danych nie są traktowane wyłącznie jako narzędzia wspierające funkcjonowanie państw. Ich rola rozszerza się na funkcje bezpieczeństwa wewnętrznego, kontroli granicznej, a nawet predykcji zagrożeń, co sugeruje przesunięcie akcentu z klasycznej obronności na kognitywne i predykcyjne formy ochrony społeczeństwa.

WNIOSKI

Powyższe zestawienie wskazuje, że obszary technologiczne przecinają się z wieloma wymiarami polityk unijnych, takimi jak cyfryzacja, infrastruktura krytyczna, bezpieczeństwo wewnętrzne i odporność systemowa. Model zarządzania bezpieczeństwem technologicznym UE przesuwa się z modelu sektorowego (hierarchicznego) na macierzowy (sieciowy), w którym istotne stają się: **technologie** i występujące pomiędzy ich rozwojem **synergie,** a także ich **zdolność** do współwystępowania w zintegrowanych systemach bezpieczeństwa, pobudzania innowacyjności i rozwoju gospodarki państw UE.

Należy przy tym wskazać, że podstawowym problemem powstających obecnie w ramach UE dokumentów strategicznych jest wielość definicji i niesystematyczność w zakresie jej stosowania. Widać to, po zaproponowanych tu interpretacjach autorskich do analizowania niniejszego dokumentu pojęć. Kolejnym wyzwaniem jest przenikanie się definicji technologii krytycznych (ang. critical technology), kluczowych technologii wspomagających (ang. key enabling technologies, KETs), technologii strategicznych (ang. strategic technologies), czy nowych przełomowych technologii (ang. emerging disruptive technologies, EDTs). Wielość tego rodzaju systematyzacji wraz z różnymi podejściami oraz

DOI: https://doi.org/10.36735/FHTY6993

odmiennymi mechanizmami ich rozwoju sprawia, że sytuacja dotycząca pobudzania innowacyjności i bezpieczeństwa technologicznego w UE staje się coraz większym wyzwaniem.

Coraz wyraźniej zauważalne stają się deficyty systemowe UE w obszarze polityczno-strategicznej równowagi między rozwojem gospodarczym, a implementacją technologii bezpieczeństwa. Narracje strategiczne o charakterze deklaratywnym koncentrują się na rozwijaniu nowoczesnych technologii (np. kwantowych, AI, chmurowych), natomiast mniej uwagi poświęca się aspektom ich praktycznej adaptacji w systemach zarządzania kryzysowego, edukacji czy społecznym zaufaniu. Może to skutkować asymetrią między potencjałem technologicznym a rzeczywistą odpornością UE, szczególnie w sytuacjach nagłych zakłóceń, dezinformacji lub eskalacji konfliktów hybrydowych.

Autor:

dr Piotr Lewandowski

Autor:

Piotr Lewandowski, dr – główny specjalista Łukasiewicz – ITECH. Analityk z zakresu polityk publicznych w obszarze innowacji i bezpieczeństwa technologicznego.