Cyberodporność – co nam zagraża, jak się bronić?

Prof. Grażyna Szpor
Uniwersytet Kardynała Stefana Wyszyńskiego

Transformacja cyfrowa zmienia sposób działania instytucji, ale też redefiniuje samo pojęcie bezpieczeństwa. W dobie narastających zagrożeń w cyberprzestrzeni rośnie znaczenie cyberodporności – zdolności państw, instytucji i społeczeństw do utrzymania ciągłości funkcjonowania mimo ataków i zakłóceń. Tymczasem regulacje prawne, definicje i narzędzia wciąż nie nadążają za potrzebami. Czy potrafimy myśleć o bezpieczeństwie cyfrowym nie tylko jako o ochronie systemów, lecz jako o wspólnym zobowiązaniu państwa, samorządów i obywateli? Jak budować odporność w warunkach dynamicznej zmienności, niskich kompetencji cyfrowych i rosnących zależności technologicznych?

Cyberbezpieczeństwo – między sterowaniem a odpornością

Bezpieczeństwo i odporność należą do dużej grupy terminów, którym dodaje się dziś przedrostek „cyber-" – wywodzący się z greckiego słowa „cybernetyka", oznaczającego pierwotnie „sterowanie", a współcześnie odnoszącego się do interdyscyplinarnej nauki o systemach sterowania i komunikacji. W dzisiejszym dyskursie prefix ten łączy się najczęściej z transformacją cyfrową – jej strategiami, zasadami i działaniami.

Bezpieczeństwo to jedna z tych wartości, które w kontekście transformacji cyfrowej wymagają reinterpretacji ogólnych praw i zasad.

Kamieniem milowym regulacji w tym obszarze była najpierw dyrektywa NIS z 2016 roku – koncentrująca się na reagowaniu na cyberincydenty – zaimplementowana w Polsce ustawą z 2018 roku o krajowym systemie cyberbezpieczeństwa. Kolejnym krokiem było unijne rozporządzenie z 2019 roku powołujące Agencję UE ds. Cyberbezpieczeństwa (ENISA), a następnie dyrektywa NIS 2 z 2022 roku, kładąca nacisk na prewencję i redukcję cyberzagrożeń.

Transpozycja przepisów NIS 2 wymaga nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która w Polsce wciąż nie została zakończona. Obecnie funkcjonują więc dwie równoległe definicje cyberbezpieczeństwa. Dla skutecznego „sterowania nawą państwową" kluczowe staje się przyjęcie takiej wersji regulacji, która umożliwi jednoznaczne powiązanie cyberbezpieczeństwa z odpornością

sieci, systemów i ludzi na rosnące spektrum zagrożeń w cyberprzestrzeni.

Cyberbezpieczeństwo to dziś nie tylko ochrona danych, lecz warunek sterowności państwa w cyfrowym świecie – wymaga jasnych definicji, sprawnych instytucji i odporności systemów oraz ludzi.

Cyberodporność – potrzeba redukcji zagrożeń

Choć termin „cyberodporność" zyskał ostatnio popularność i coraz częściej pojawia się w dokumentach urzędowych i analizach strategicznych, dopiero niedawno zaczął funkcjonować w języku prawnym i nie ma legalnej definicji. W najbardziej ogólnym ujęciu oznacza zdolność do nieprzerwanego realizowania zamierzonych celów mimo wystąpienia cyberincydentów.

Cyberodporność obejmuje zarówno zdolność do wykrywania zagrożeń i przeciwdziałania im, jak i umiejętność szybkiego reagowania na zdarzenia niepożądane oraz zapewnienia ciągłości działania. Osiągnięcie akceptowalnego poziomu odporności wymaga działań prewencyjnych – takich, które pozwolą identyfikować zagrożenia zanim zdążą one wywołać negatywne skutki.

Określenie to stosowane jest w różnych kontekstach: od bezpieczeństwa systemów informatycznych i ochrony infrastruktury krytycznej, poprzez procesy biznesowe i funkcjonowanie organizacji społecznych, po odporność państw. Funkcjonuje zarówno w ujęciu krajowym, jak i w wymiarze unijnym oraz globalnym. W tak szerokim spektrum trudno o jedną, uniwersalną definicję.

Dlatego to w aktach prawnych i dokumentach publicznych, w których pojawia się termin „cyberodporność", powinno się każdorazowo określać jego znaczenie w danym kontekście. To istotne, by ograniczyć interpretacyjną niepewność i umożliwić skuteczne stosowanie przepisów. W przeciwnym razie ryzykujemy sytuację, w której znaczenie kluczowego pojęcia będzie ustalane nie przez ustawodawcę czy instytucje publiczne, lecz przez narzędzia sztucznej inteligencji – a wątpliwości będą rozstrzygane przez ChatGPT.

Między suwerennością a cybersolidarnością

Napięcie między potrzebą zachowania suwerenności państwowej a koniecznością budowania „cybersolidarności" w ramach Unii Europejskiej pogłębiają dynamiczne zmiany geopolityczne oraz doświadczenia związane z tzw. „cyberpandemią" – przełomowym momentem, który unaocznił kruchość dotychczasowych zabezpieczeń cyfrowych.

Cyberodporność jako zdolność do redukcji zagrożeń wymaga gotowości do działania zanim nadejdzie kryzys.

Rosnąca świadomość zagrożeń znalazła odzwierciedlenie w strategicznych dokumentach Unii Europejskiej, które wyznaczyły kierunki działań na trzecią dekadę XXI wieku. Należą do nich m.in. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/241 ustanawiające Instrument na rzecz Odbudowy

i Zwiększania Odporności, rozporządzenie 2021/694 oraz decyzja Parlamentu Europejskiego i Rady 2022/2481. Mimo słusznych założeń, zastrzeżenia budziły wówczas: sposób formułowania celów – zbyt silne skupienie na ilościowych wskaźnikach ich realizacji oraz niedopracowane metody weryfikacji kompetencji cyfrowych.

Cybersuwerenność bez cybersolidarności osłabia nasze krajowe i europejskie bezpieczeństwo, – trwały efekt da wyłącznie ich dojrzała równowaga.

Z czasem te braki zaczęto korygować, m.in. w ramach Deklaracji praw i zasad w cyfrowej dekadzie oraz aktu w sprawie cybersolidarności. Niemniej, w warunkach złożonych konfliktów interesów między państwami członkowskimi, akty prospektywne wymagają ciągłego monitorowania i korekt – tak, aby ich implementacja rzeczywiście wzmacniała cyberodporność Unii jako całości[1].

Kompetencje cyfrowe – najsłabsze ogniwo systemu

W krajowych planach transformacji cyfrowej dostrzeżono, że o sile systemów decydują ich najsłabsze ogniwa i przeznaczono znaczne środki na podnoszenie kompetencji cyfrowych. W przypadku Polski, która od lat zajmuje niskie miejsca w unijnym rankingu DESI (*Digital Economy and Society Index*), jest to szczególnie istotne. Duże znaczenie dla rozpoznania cyberzagrożeń oraz podjęcia inicjatyw zmierzających do ich redukcji mają informacje z raportów Najwyższej Izby Kontroli. Wynika z nich jasno, że pilnym wyzwaniem jest w Polsce właśnie zwiększenie efektywności działań podnoszących kompetencje w zakresie cyberbezpieczeństwa.

Odpowiedzią na te potrzeby ma być m.in. uruchomiony w 2024 roku projekt „Cyberbezpieczny Samorząd" w ramach Programu Operacyjnego FERC 2021–2027 (Działanie 2.2: Wzmocnienie krajowego systemu cyberbezpieczeństwa). Budżet projektu wynosi ok. 1,5 mld złotych, a jednostki samorządu terytorialnego mogą ubiegać się o granty w wysokości od 200 tys. do 850 tys. zł.

Wdrażanie programu ujawnia jednak istotną lukę regulacyjną, zidentyfikowaną również na poziomie unijnym – brak wyraźnego uwzględnienia gier edukacyjnych i symulatorów wśród uznanych form podnoszenia i weryfikacji kompetencji cyfrowych. Choć badania potwierdzają ich wysoką skuteczność, a zainteresowanie środowisk akademickich i samorządowych jest znaczące, wybory dokonywane w trybie zamówień publicznych wciąż zbyt często determinowane są przez kryterium najniższej ceny, a nie efektywności.

W cyfrowym świecie systemy są tak silne, jak kompetencje ich użytkowników – a interaktywna edukacja to inwestycja w prawdziwą cyberodporność.

Tymczasem to właśnie edukacyjne gry komputerowe – dzięki swojej interaktywności i immersji – mogą najskuteczniej wspierać

1 Zob. *Internet. Globalne gry*, red. G. Szpor, A. Gryszczyńska, W. R. Wiewiórowski, Warszawa 2021, s. 352; *Internet. Solidarność cyfrowa*, Warszawa 2024.

rozwój cyberodporności. Dlatego ich tworzenie, rozwijanie i wdrażanie powinno uzyskać systemowe wsparcie ze strony instytucji krajowych i unijnych.

Cyberodporność a inteligentny rozwój terytorialny

„Akt o cyberodporności", czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847, ustanawia horyzontalne wymagania w zakresie cyberbezpieczeństwa dla produktów z elementami cyfrowymi. Akt ten zwraca uwagę na rosnące zagrożenia wynikające z przenikania się przestrzeni geograficznej i cyberprzestrzeni, szczególnie w kontekście dynamicznego rozwoju Internetu rzeczy (IoT).

W odpowiedzi na te wyzwania, władze publiczne podejmują dziś działania zmierzające do wzmocnienia zasad wielodomenowej ochrony infrastruktury krytycznej – obejmującej zarówno przestrzeń fizyczną, jak i wirtualną. Jednak konieczne jest szersze podejście: cyberodporność powinna zostać włączona jako jedno z podstawowych kryteriów przy ocenie i aktualizacji strategii inteligentnego rozwoju (*smart development*).

Ma to szczególne znaczenie w kontekście decyzji podejmowanych przez jednostki samorządu terytorialnego. Wybór modeli dalszego rozwoju inteligentnych gmin – zarówno w wersji *smart cities*, jak i *smart villages* – powinien uwzględniać kwestie odporności cyfrowej jako element kluczowy. W praktyce oznacza to konieczność projektowania lokalnych systemów zarządzania, usług publicznych i infrastruktury cyfrowej z uwzględnieniem odporności na cyberzagrożenia oraz zdolności reagowania na incydenty.

Cyberodporność to nie tyle kosztowna bariera inteligentnego rozwoju ile warunek tworzenia jego odpornych fundamentów.

Jak wskazano w najnowszej literaturze przedmiotu, cyberodporność powinna być postrzegana nie jako koszt, lecz jako inwestycja warunkująca stabilność i zrównoważony rozwój wspólnot lokalnych w cyfrowym świecie[2]. ■

2 G. Szpor, A. Gryszczyńska, A. Syryt, *Transformacja cyfrowa samorządu terytorialnego*, w: *System prawa samorządu terytorialnego*, red. I. Lipowicz, t. 3, Warszawa 2023.

O AUTORCE

prof. Grażyna Szpor – Kierownik Katedry Prawa Informatycznego i Dyrektor Centrum Liderów Transformacji Cyfrowej Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Prezes Zarządu Stowarzyszenia Naukowe Centrum Prawno-Informatyczne skupiającego ekspertów z kilkunastu uczelni, sektora publicznego i biznesu. Autorka i redaktor naukowy ponad 200 publikacji, w tym monografii „Jawność i jej ograniczenia", szesnastu tomów serii dotyczącej bezpieczeństwa w Internecie oraz komentarzy do ustaw: o informatyzacji działalności podmiotów realizujących zadania publiczne, o dostępności cyfrowej stron internetowych i aplikacji mobilnych, o krajowym systemie cyberbezpieczeństwa. Laureatka wielu nagród za działalność badawczo-rozwojową i edukacyjną związaną z informatyzacją i podnoszeniem kompetencji cyfrowych.

Partnerzy

SAMORZĄD WOJEWÓDZTWA POMORSKIEGO

Pomorski Fundusz Rozwoju
sp. z o.o. z siedzibą w Gdańsku
Spółka Samorządu Województwa Pomorskiego

2000-2025 LAT
POLSKO-AMERYKAŃSKA FUNDACJA WOLNOŚCI

Maritex
ELECTRONIC COMPONENTS

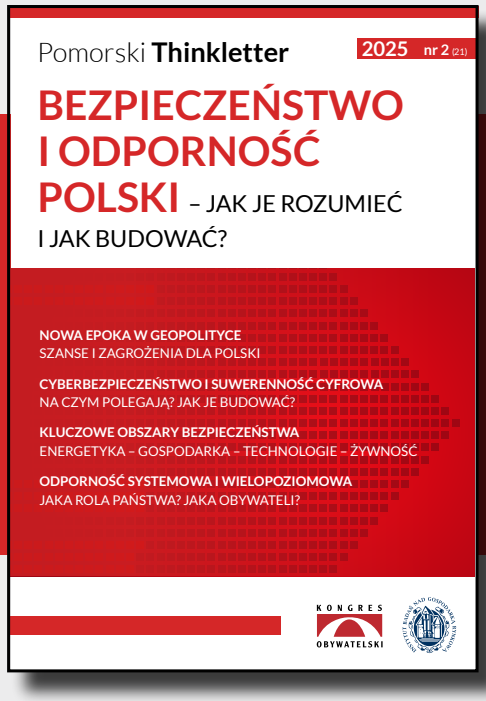
ORLEN

BGK
BANK GOSPODARSTWA KRAJOWEGO

PFR
Polski Fundusz Rozwoju

BNP PARIBAS
FOOD & AGRO

Nestlé



POBIERZ CAŁĄ PUBLIKACJĘ

www.kongresobywatelski.pl