



fundacja instytut
CYBERBEZPIECZEŃSTWA

Wpływ cyberwojen na geopolitykę globalną i w regionie Europy Środkowo-Wschodniej

dr Sławomir Żurawski



Fundusz
Sprawiedliwości



Ministerstwo
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



Wprowadzenie

W ciągu ostatnich dwóch dekad cyberprzestrzeń przekształciła się z neutralnego środowiska technologicznego w nowy obszar rywalizacji geopolitycznej. Wraz z cyfryzacją administracji, gospodarki i przestrzeni publicznej państwa coraz częściej wykorzystują środki cyfrowe do realizacji celów politycznych, militarnych i wywiadowczych. Zjawisko cyberwojen, rozumianych jako skoordynowane działania ofensywne prowadzone przez państwa (lub wspierane przez nie podmioty) w cyberprzestrzeni, zyskało na znaczeniu jako nowoczesne narzędzie wpływu i destabilizacji. Ich oddziaływanie jest dziś odczuwalne zarówno w globalnej równowadze sił, jak i bezpieczeństwie regionalnym poszczególnych państw.

Cyberprzestrzeń jako nowy wymiar rywalizacji mocarstw

W klasycznej teorii geopolityki dominowały trzy przestrzenie: ląd, morze i powietrze. W XXI w. do tej triady dołączyła cyberprzestrzeń, stanowiąca coraz istotniejsze pole konfrontacji między mocarstwami. Państwa takie jak Stany Zjednoczone, Rosja, Chiny, Iran czy Korea Północna inwestują w rozwój ofensywnych zdolności cybernetycznych, umożliwiających zarówno zakłócenie funkcjonowania infrastruktury przeciwnika, jak

i prowadzenie długoterminowych operacji szpiegowskich, sabotażowych czy dezinformacyjnych¹.

Współczesne konflikty zbrojne coraz częściej przenoszą się z pola walki do cyberprzestrzeni, gdzie operacje mają na celu destabilizację przeciwnika poprzez ataki na infrastrukturę krytyczną, systemy komunikacji czy instytucje rządowe². Do przykładów takich ataków należą: opera-

1 A. Krauz, Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej w globalnym świecie wiedzy, „Edukacja – Technika – Informatyka” 2013, nr 1, s. 389.

2 S. Żurawski, P. Waniek, K. Zygo, W. Barszczewski, Phishing jako narzędzie cyberwojny, „Studia Społeczne” 2024, nr 4 (47), s. 69.

cja Stuxnet przeciwko irańskiemu programowi nuklearnemu, rosyjskie ingerencje w wybory prezydenckie w USA, kampanie APT (ang. Advanced Persistent Threats) wymierzone w sektor energetyczny czy telekomunikacyjny, a także szeroko zakrojone działania dezinformacyjne w mediach

społecznościowych. Tego typu operacje pokazują skalę i złożoność współczesnych cyberkonfliktów. Cyberprzestrzeń pozwala prowadzić działania poniżej progu otwartej wojny, co sprawia, że staje się atrakcyjnym narzędziem w tzw. wojnie hybrydowej³.

Geopolityczne konsekwencje cyberataków

Cyberataki mogą mieć dalekosiężne skutki strategiczne. Zniszczenie lub zakłócenie działania infrastruktury krytycznej (np. systemów energetycznych, wodociągowych, transportowych czy łączności) prowadzi

do realnych strat ekonomicznych, paraliżu instytucji państwowych i spadku zaufania społecznego. W kontekście globalnym może to prowadzić do zmiany układu sił, osłabienia jednych graczy na rzecz innych



3 W. Goleński, D. Zimny, Przygotowanie państwa na zagrożenia hybrydowe – konieczność natychmiastowych działań, „Kontrola Państwowa” 2024, t. 69, nr 5 (418), s. 22.

i tworzenia nowych, asymetrycznych form przewagi strategicznej.

Jednym z najpoważniejszych zagrożeń jest wykorzystanie cyberataków do ingerencji w procesy demokratyczne – manipulowanie opinią publiczną, podsycanie konfliktów społecznych czy osłabianie autorytetu in-

stytucji państwowych. Przykładem są działania prowadzone przez rosyjskie farmy trolli i botów, których celem jest destabilizacja Zachodu poprzez sianie dezinformacji, pogłębianie podziałów społecznych i wspieranie ekstremistycznych narracji.

Cyberwojny a bezpieczeństwo regionalne – przypadek Europy Środkowo-Wschodniej

Region Europy Środkowo-Wschodniej stanowi jeden z kluczowych obszarów aktywności cybernetycznej ze względu na jego strategiczne położenie, obecność infrastruktury NATO i UE oraz napięcia geopolityczne, szczególnie związane z agresywną polityką Rosji. Polska, kraje bałtyckie, Ukraina i inne państwa regionu regularnie padają ofiarą cyberataków wymierzonych zarówno w systemy administracyjne, jak i sferę informacyjną.

W Polsce odnotowano liczne ataki na systemy teleinformatyczne administracji publicznej, instytucji finansowych czy mediów. Cyberprzestrzeń stała się także polem działań dezinformacyjnych – publikacja sfałszowanych dokumentów, podszywanie się pod polityków czy tworzenie fałszywych nar-

racji w mediach społecznościowych to elementy szerszej strategii destabilizacyjnej. Ataki te mają na celu nie tylko pozyskanie danych, lecz także podważenie zaufania obywateli do państwa i jego zdolności do zapewnienia bezpieczeństwa.

Ukraina jako państwo frontowe od lat doświadcza najintensywniejszych cyberataków, często będących preludem do działań konwencjonalnych⁴. Przykładem może być seria ataków na ukraiński sektor energetyczny, w tym przerwy w dostawie prądu, przypisywane rosyjskim grupom hakerskim. Konflikt w Ukrainie pokazuje, że cyberwojna nie jest zjawiskiem abstrakcyjnym – to realna forma prowadzenia działań wojennych, zsynchronizowana z działaniami militarnymi i politycznymi⁵.

4 L. Tretyak, Rosyjska cyberwojna wobec Ukrainy: analiza strategii i skutków, w: Ukraina: wojna, odpowiedzialność, przyszłość, A. Madera (red.), CBPE, Warszawa 2024, s. 70.

5 Z. Ciekanowski, S. Żurawski, Cyber Threat Analysis (CTA) in Current Conflicts, „IgMin Research” 2024, nr 2 (4), s. 225.

Trudności w identyfikacji i odpowiedzialności - odporność jako klucz do przetrwania

Cyberprzestrzeń na wiele sposobów wpływa na bezpieczeństwo międzynarodowe i pozycję poszczególnych graczy⁶. Jednym z największych wyzwań związanych z cyberwojnami jest problem atrybucji, czyli jednoznacznego przypisania danego ataku konkretnej stronie. Hakerzy często posługują się złożonymi technikami maskowania, wykorzystując infrastrukturę państw trzecich i działając przez grupy pośrednie. To powoduje, że reakcja polityczna i prawna na cyberataki jest opóźniona lub utrudniona, a atakujący często pozostają bezkarni.

Brak międzynarodowych regulacji prawnych dotyczących cyberkonfliktów sprawia, że cyberprzestrzeń pozostaje „dzikim zachodem” współczesnej geopolityki. Mimo podejmowanych prób stworzenia norm etycznych i prawnych (np. grupa ekspertów ONZ ds. cyberprzestrzeni, inicjatywy Tallinn Manual) nie udało się dotąd wypracować wiążących mechanizmów przeciwdziałania temu zagrożeniu i rozliczania agresorów.

Wobec rosnącego znaczenia cyberzagrożeń konieczne jest budowanie odporności państw zarówno na poziomie technologicznym, jak i społecznym. Inwestycje w bezpieczeństwo systemów informatycznych, szkolenia dla administracji, tworzenie centrów reagowania na incydenty (CSIRT), a także edukacja obywateli w zakresie zagrożeń cyfrowych stają się niezbędnymi elementami polityki bezpieczeństwa. Coraz większego znaczenia nabiera też współpraca międzynarodowa – zarówno w ramach sojuszy wojskowych (np. NATO), jak i struktur cywilnych (np. UE). Wspólne ćwiczenia, wymiana informacji o zagrożeniach, budowa wspólnych standardów bezpieczeństwa i mechanizmów reagowania to fundamenty skutecznej ochrony przed cyberatakami.



Wnioski

Cyberwojny redefiniują współczesną geopolitykę. Są mniej widocznym ale niezwykle skutecznym narzędziem realizacji interesów państwowych w środowisku, które dotąd nie było postrzegane jako strategiczne pole rywalizacji. Ich wpływ rozciąga się od destabilizacji państw, przez ingerencję w procesy demokratyczne, aż po kreowanie nowych osi konfliktu.

W świecie, w którym informacja staje się bronią, a linia frontu przebiega przez świat cyfrowy, zdolność do obrony w cyberprzestrzeni staje się nieodłącznym elementem

suwerenności państwowej. Państwa, które zlekceważą te wyzwania, narażają się nie tylko na straty, lecz także marginalizację w globalnym układzie sił. Z kolei ci, którzy potrafią skutecznie łączyć technologie, strategię i współpracę międzynarodową, mogą zyskać przewagę w nadchodzącej erze konfliktów cyfrowych.

⁶ J. Świątkowska, Walka z cyberzagrozeniami jako wyzwanie stojące przed globalnym bezpieczeństwem, „Przegląd Geopolityczny” 2017, nr 20, s. 165.

Bibliografia

Ciekanowski Z., Żurawski S., *Cyber Threat Analysis (CTA) in Current Conflicts*, „IgMin Research” 2024, nr 2 (4).

Goleński W., Zimny D., *Przygotowanie państwa na zagrożenia hybrydowe – konieczność natychmiastowych działań*, „Kontrola Państwowa” 2024, t. 69, nr 5 (418).

Krauz A., *Internet narzędziem groźnej broni cyfrowej dla infrastruktury krytycznej w globalnym świecie wiedzy*, „Edukacja – Technika – Informatyka” 2013, nr 1.

Świątkowska J., *Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem*, „Przeгляд Geopolityczny” 2017, nr 20.

Tretyak L., *Rosyjska cyberwojna wobec Ukrainy: analiza strategii i skutków*, w: *Ukraina: wojna, odpowiedzialność, przyszłość*, A. Madera (red.), CBPE, Warszawa 2024.

Żurawski S., Waniek P., Zygo K., Barszczewski W., *Phishing jako narzędzie cyberwojny*, „Studia Społeczne” 2024, nr 4 (47).



fundacja instytut
CYBERBEZPIECZEŃSTWA

www.instytutcyber.pl

