Mirosław Podgórski

Szkoła Główna Mikołaja Kopernika w Warszawie

https://orcid.org/0009-0008-8653-0681

Cyberbezpieczeństwo wschodniej flanki NATO w obliczu wojny rosyjsko-ukraińskiej

Streszczenie

Wojna rosyjsko-ukraińska stanowi punkt zwrotny w postrzeganiu cyberprzestrzeni jako jednego z kluczowych wymiarów współczesnych konfliktów zbrojnych. Działania prowadzone przez Federację Rosyjską wobec Ukrainy od 2014 roku, a w szczególności po rozpoczęciu pełnoskalowej inwazji w 2022 roku, potwierdziły, że cyberataki są integralnym elementem strategii hybrydowej, uzupełniając działania militarne, informacyjne i gospodarcze. Państwa wschodniej flanki NATO, skupione m.in. w formacie Bukaresztańskiej Dziewiątki, znalazły się w sytuacji szczególnej podatności na zagrożenia cybernetyczne, wynikającej z ich położenia geopolitycznego, roli infrastruktury krytycznej oraz zaangażowania w system bezpieczeństwa euroatlantyckiego.

Celem artykułu jest kompleksowa analiza znaczenia cyberbezpieczeństwa dla wschodniej flanki NATO w kontekście wojny rosyjsko-ukraińskiej oraz ocena zdolności państw regionu do przeciwdziałania zagrożeniom w cyberprzestrzeni. W pracy zastosowano podejście analityczno-syntetyczne, odwołujące się do paradygmatu realizmu oraz koncepcji bezpieczeństwa wielowymiarowego. Artykuł ukazuje rolę NATO i Unii Europejskiej w budowaniu odporności cybernetycznej, analizuje potencjał państw Bukaresztańskiej Dziewiątki oraz identyfikuje kluczowe wyzwania i kierunki dalszego rozwoju cyberochrony w Europie Środkowo-Wschodniej.

Słowa kluczowe: cyberbezpieczeństwo, NATO, wschodnia flanka, wojna rosyjsko-ukraińska, Bukaresztańska Dziewiątka.

Cybersecurity of NATO's eastern flank during the Russia-Ukraine war

Abstract

The Russian–Ukrainian war constitutes a turning point in the perception of cyberspace as one of the key dimensions of contemporary armed conflicts. Actions undertaken by the Russian Federation against Ukraine since 2014, and in particular following the launch of the full-scale invasion in 2022, have confirmed that cyberattacks are an integral element of hybrid strategy, complementing military, informational, and economic activities. States on NATO's eastern flank, including those cooperating within the Bucharest Nine format, have found themselves in a situation of particular vulnerability to cyber threats, resulting from their geopolitical location, the role of critical infrastructure, and their involvement in the Euro-Atlantic security system.

The aim of this article is to provide a comprehensive analysis of the significance of cybersecurity for NATO's eastern flank in the context of the Russian–Ukrainian war and to assess the capacity of the states in the region to counter threats in cyberspace. The study employs an analytical–synthetic approach, drawing on the paradigm of realism and the concept of multidimensional security. The article examines the role of NATO and the European Union in building cyber resilience, analyzes the potential of the Bucharest Nine states, and identifies key challenges as well as directions for the further development of cyber protection in Central and Eastern Europe.

Keywords: cybersecurity, NATO, eastern flank, Russian–Ukrainian war, Bucharest Nine.

Wprowadzenie

Postępująca cyfryzacja państw, społeczeństw i gospodarek sprawiła, że cyberprzestrzeń stała się jednym z kluczowych obszarów funkcjonowania współczesnego świata [1, 13, 15]. Równocześnie stała się ona nową domeną rywalizacji strategicznej, w której państwa wykorzystują narzędzia cybernetyczne do realizacji swoich interesów politycznych, militarnych i gospodarczych [3, 14, 16]. W tym kontekście cyberbezpieczeństwo przestało być wyłącznie problemem technicznym, a stało się jednym z fundamentalnych elementów bezpieczeństwa narodowego i międzynarodowego [4, 5].

Wojna rosyjsko-ukraińska unaoczniła skalę i charakter zagrożeń cybernetycznych, z jakimi mogą mierzyć się państwa zaangażowane w konflikt lub znajdujące się w jego bezpośrednim otoczeniu strategicznym [2, 28, 29]. Cyberataki stały się narzędziem destabilizacji państwa, osłabiania jego zdolności obronnych oraz oddziaływania na społeczeństwo i sojuszników [6, 7]. Państwa wschodniej flanki NATO, w tym Polska, Rumunia oraz państwa bałtyckie, znalazły się w sytuacji szczególnego ryzyka, co wymusiło intensyfikację działań na rzecz wzmocnienia odporności cybernetycznej [10, 11].

Celem niniejszego artykułu jest odpowiedź na pytanie, w jaki sposób wojna rosyjsko-ukraińska wpłynęła na postrzeganie i rozwój cyberbezpieczeństwa wschodniej flanki NATO oraz jakie znaczenie mają działania podejmowane przez NATO, Unię Europejską i państwa Bukaresztańskiej Dziewiątki dla stabilności bezpieczeństwa regionalnego 1, 12].

1. Cyberprzestrzeń jako domena współczesnych konfliktów zbrojnych

W literaturze przedmiotu cyberprzestrzeń coraz częściej traktowana jest jako pełnoprawna domena działań militarnych, porównywalna z lądem, morzem, powietrzem i przestrzenią kosmiczną [3, 7]. Rozwój technologii informacyjnych umożliwił prowadzenie operacji cybernetycznych o charakterze ofensywnym i defensywnym, których skutki mogą mieć bezpośredni wpływ na funkcjonowanie państwa oraz bezpieczeństwo międzynarodowe [14, 15].

Cyberoperacje charakteryzują się relatywnie niskim kosztem, możliwością zachowania anonimowości oraz działaniem poniżej progu wojny kinetycznej [16, 28]. Z tego względu stały się one szczególnie atrakcyjnym narzędziem dla państw dążących do realizacji celów strategicznych bez ryzyka bezpośredniej eskalacji militarnej [25, 26]. Koncepcje cyberodstraszania wskazują, że zdolność do obrony oraz do zadawania strat w cyberprzestrzeni stanowi istotny element równowagi strategicznej [15, 28].

Działania Federacji Rosyjskiej wobec Ukrainy od 2014 roku stanowią jeden z najbardziej kompleksowych przykładów zastosowania cybernarzędzi w konflikcie zbrojnym [2, 3]. Ataki na infrastrukturę energetyczną, administrację publiczną oraz sektor finansowy Ukrainy miały na celu osłabienie zdolności państwa do funkcjonowania oraz wywołanie chaosu społecznego [6, 11].

Po 2022 roku cyberataki stały się integralnym elementem działań wojennych, uzupełniając operacje kinetyczne [1, 28]. Kampanie dezinformacyjne, ataki typu DDoS oraz złośliwe oprogramowanie destrukcyjne były wykorzystywane równolegle z ofensywą militarną 14, 29]. Doświadczenia Ukrainy stanowią istotne źródło wiedzy dla państw wschodniej flanki NATO, pokazując możliwe scenariusze zagrożeń [5, 12].

2. Cyberbezpieczeństwo jako element bezpieczeństwa wschodniej flanki NATO

Państwa wschodniej flanki NATO charakteryzują się szczególną wrażliwością na zagrożenia cybernetyczne ze względu na swoje położenie geopolityczne, strukturę infrastruktury krytycznej oraz rolę w systemie bezpieczeństwa euroatlantyckiego [1, 5]. Cyberataki mogą prowadzić do paraliżu systemów energetycznych, transportowych i komunikacyjnych, co bezpośrednio wpływa na zdolności obronne Sojuszu [6, 27].

Uznanie cyberprzestrzeni za domenę operacyjną NATO stanowiło przełom w podejściu do planowania obronnego [7, 10]. Oznacza to, że cyberataki mogą być traktowane jako przesłanka do uruchomienia mechanizmów kolektywnej obrony, w tym art. 5 Traktatu Waszyngtońskiego [1, 7].

Państwa Bukaresztańskiej Dziewiątki odgrywają kluczową rolę w kształtowaniu bezpieczeństwa wschodniej flanki NATO [12, 20]. W ostatnich latach państwa te zintensyfikowały działania na rzecz rozwoju krajowych systemów cyberbezpieczeństwa, tworząc wyspecjalizowane instytucje, strategie oraz mechanizmy reagowania na incydenty [4,

11]. Szczególną rolę odgrywają państwa bałtyckie, które dzięki wcześniejszym doświadczeniom z cyberatakami stały się liderami w zakresie cyberodporności [2, 6]. Polska i Rumunia pełnią funkcję państw wiodących w regionie, zarówno pod względem potencjału instytucjonalnego, jak i znaczenia politycznego w ramach NATO [1, 5].

3. Rola NATO i Unii Europejskiej w budowaniu odporności cybernetycznej

NATO i Unia Europejska odgrywają komplementarne role w zakresie cyberbezpieczeństwa [7, 27]. NATO koncentruje się na wymiarze militarnym i strategicznym, rozwijając zdolności cyberobrony oraz mechanizmy odstraszania [1, 3]. Unia Europejska natomiast skupia się na harmonizacji regulacji prawnych, ochronie infrastruktury krytycznej oraz wsparciu państw członkowskich w budowaniu odporności systemowej [8, 9].

Współpraca NATO–UE w obszarze cyberbezpieczeństwa nabrała szczególnego znaczenia po 2022 roku, kiedy zagrożenia cybernetyczne zaczęły być postrzegane jako jedno z kluczowych wyzwań dla bezpieczeństwa całej Europy [27, 28].

Do głównych wyzwań stojących przed państwami wschodniej flanki NATO należą niedobory wysoko wykwalifikowanych specjalistów, szybkie tempo rozwoju technologii oraz rosnąca skala zagrożeń hybrydowych [13, 29]. Istotnym problemem pozostaje również konieczność integracji systemów cywilnych i wojskowych w zakresie cyberochrony [4, 17].

Perspektywy rozwoju cyberbezpieczeństwa w regionie są ściśle związane z dalszym pogłębianiem współpracy regionalnej, w tym w ramach Bukaresztańskiej Dziewiątki, oraz zacieśnianiem relacji z NATO i Unią Europejską [12, 27].

4. Cyberodstraszanie i odporność cyfrowa jako nowe filary bezpieczeństwa regionalnego

Rozwój cyberprzestrzeni jako domeny działań strategicznych doprowadził do wykształcenia nowych koncepcji bezpieczeństwa, wśród których szczególne znaczenie zyskały cyberodstraszanie oraz odporność cyfrowa [15, 28]. Cyberodstraszanie opiera się na założeniu, że potencjalny agresor powstrzyma się od działań w cyberprzestrzeni, jeżeli spodziewane koszty polityczne, militarne lub gospodarcze przewyższą możliwe korzyści [3, 7]. W odróżnieniu od klasycznego odstraszania nuklearnego lub konwencjonalnego,

cyberodstraszanie cechuje się wysokim poziomem niejednoznaczności, trudnością w atrybucji ataków oraz relatywnie niskim progiem eskalacji [14, 16].

Państwa wschodniej flanki NATO, analizując doświadczenia Ukrainy, coraz wyraźniej dostrzegają, że skuteczne cyberodstraszanie nie może opierać się wyłącznie na zdolnościach ofensywnych [2, 28]. Kluczowe znaczenie ma zdolność do szybkiego wykrywania incydentów, minimalizowania ich skutków oraz zapewnienia ciągłości funkcjonowania państwa i infrastruktury krytycznej [6, 9]. Odporność cyfrowa staje się zatem komplementarnym elementem odstraszania, wzmacniając wiarygodność całego systemu bezpieczeństwa regionalnego [1, 27].

5. Infrastruktura krytyczna jako główny cel cyberataków

Jednym z najważniejszych wniosków płynących z analizy wojny rosyjsko-ukraińskiej jest rola infrastruktury krytycznej jako głównego celu cyberataków [6, 11]. Systemy energetyczne, telekomunikacyjne, transportowe oraz finansowe stanowią fundament funkcjonowania nowoczesnych państw, a ich zakłócenie może prowadzić do paraliżu administracji publicznej i destabilizacji społecznej [8, 29].

Państwa wschodniej flanki NATO, ze względu na swoje położenie geopolityczne oraz funkcję zaplecza logistycznego Sojuszu, są szczególnie narażone na tego rodzaju zagrożenia [5, 12]. Cyberataki na infrastrukturę krytyczną mogą mieć charakter skoordynowany z działaniami kinetycznymi lub stanowić element długotrwałej presji strategicznej prowadzonej poniżej progu wojny [3, 27]. W tym kontekście kluczowe znaczenie ma harmonizacja standardów ochrony infrastruktury krytycznej w ramach Unii Europejskiej oraz NATO [8, 10].

6. Edukacja, kapitał ludzki i innowacje technologiczne

Jednym z najpoważniejszych wyzwań dla cyberbezpieczeństwa państw wschodniej flanki NATO pozostaje deficyt wysoko wykwalifikowanych specjalistów [13, 29]. Dynamiczny rozwój technologii, w tym sztucznej inteligencji, uczenia maszynowego oraz Internetu Rzeczy, powoduje, że zapotrzebowanie na ekspertów ds. cyberbezpieczeństwa rośnie szybciej niż możliwości systemów edukacyjnych [15, 28].

Państwa Bukaresztańskiej Dziewiątki podejmują coraz bardziej zróżnicowane działania w tym obszarze, rozwijając programy kształcenia akademickiego, szkolenia dla administracji publicznej oraz współpracę z sektorem prywatnym [4, 11]. Inwestycje w kapitał ludzki należy postrzegać jako element długofalowej strategii bezpieczeństwa, którego znaczenie jest porównywalne z modernizacją sił zbrojnych [17, 25].

7. Współpraca regionalna w ramach Bukaresztańskiej Dziewiątki

Format Bukaresztańskiej Dziewiątki, mimo że nie posiada sformalizowanych struktur instytucjonalnych, odgrywa istotną rolę w koordynacji stanowisk państw wschodniej flanki NATO w zakresie bezpieczeństwa, w tym cyberbezpieczeństwa [12, 20]. Regularne konsultacje polityczne oraz wymiana doświadczeń umożliwiają lepsze dostosowanie polityk narodowych do wyzwań regionalnych [5, 17].

W kontekście cyberbezpieczeństwa B9 może pełnić funkcję platformy integrującej działania państw regionu, zwłaszcza w obszarze ochrony infrastruktury krytycznej, reagowania na incydenty oraz przeciwdziałania dezinformacji [2, 6]. Wzmocnienie współpracy w tym formacie mogłoby przyczynić się do zwiększenia spójności działań NATO na wschodniej flance [1, 27].

8. Cyberbezpieczeństwo a art. 5 Traktatu Waszyngtońskiego

Jednym z kluczowych problemów teoretycznych i praktycznych pozostaje kwestia zastosowania art. 5 Traktatu Waszyngtońskiego w odpowiedzi na cyberatak [1, 7]. Brak jednoznacznych kryteriów określających, kiedy cyberatak może zostać uznany za zbrojną napaść, powoduje, że cyberprzestrzeń pozostaje obszarem strategicznej niejednoznaczności [3, 26].

Z perspektywy państw wschodniej flanki NATO szczególnie istotne jest wypracowanie wspólnych procedur reagowania na poważne incydenty cybernetyczne, które mogłyby zagrozić bezpieczeństwu całego Sojuszu [27, 28]. W tym kontekście kluczową rolę odgrywa współpraca polityczna oraz ćwiczenia symulacyjne prowadzone w ramach NATO [7, 10].

9. Znaczenie wojny rosyjsko-ukraińskiej dla przyszłości bezpieczeństwa Europy

Wojna rosyjsko-ukraińska ma charakter przełomowy nie tylko z perspektywy bezpieczeństwa regionalnego, lecz także globalnego porządku międzynarodowego [25, 26]. Cyberprzestrzeń stała się trwałym elementem rywalizacji mocarstw, a jej znaczenie będzie rosło wraz z postępującą cyfryzacją społeczeństw i gospodarek 14, 15].

Dla państw wschodniej flanki NATO konflikt ten stanowi impuls do przyspieszenia reform w obszarze cyberbezpieczeństwa oraz do pogłębienia współpracy regionalnej i transatlantyckiej [1, 12]. Doświadczenia Ukrainy pokazują, że brak odpowiedniej odporności cyfrowej może prowadzić do eskalacji kryzysów i osłabienia zdolności obronnych państwa [2, 28].

Wnioski

Cyberbezpieczeństwo wschodniej flanki NATO w obliczu wojny rosyjsko-ukraińskiej należy postrzegać jako jeden z kluczowych wymiarów współczesnego bezpieczeństwa regionalnego i międzynarodowego [1, 7]. Analiza przeprowadzona w artykule wskazuje, że cyberprzestrzeń stała się trwałym polem rywalizacji strategicznej, a jej znaczenie będzie rosło w nadchodzących dekadach [15, 25].

Państwa Bukaresztańskiej Dziewiątki, działając w ramach NATO i Unii Europejskiej, posiadają potencjał do budowy spójnego systemu cyberbezpieczeństwa, który może skutecznie wzmacniać odstraszanie i odporność wschodniej flanki Sojuszu [12, 27]. Warunkiem powodzenia tych działań jest dalsza integracja polityk narodowych, inwestycje w kapitał ludzki oraz konsekwentne traktowanie cyberbezpieczeństwa jako elementu strategicznego bezpieczeństwa państwa i regionu 4, 17, 29].

Bibliografia

1. NATO, *NATO 2022 Strategic Concept*, Madryt 2022.
2. ENISA, *ENISA Threat Landscape 2023*, Ateny 2023.
3. NATO CCDCOE, *Cyber Operations and the Use of Force*, Tallinn 2021.
4. Ministerstwo Obrony Narodowej RP, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2022.
5. Polski Instytut Spraw Międzynarodowych, *Cyberbezpieczeństwo Polski i wschodniej flanki NATO*, Warszawa 2023.
6. ENISA, *Cybersecurity and Resilience of Critical Infrastructure*, Ateny 2022.
7. NATO CCDCOE, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.
8. Komisja Europejska, *Dyrektywa NIS2*, Bruksela 2022.
9. Komisja Europejska, *EU Cybersecurity Strategy for the Digital Decade*, Bruksela 2020.
10. NATO, *Cyber Defence Pledge*, Bruksela 2016.
11. Ministerstwo Cyfryzacji RP, *Krajowy System Cyberbezpieczeństwa – założenia i funkcjonowanie*, Warszawa 2021.
12. Polski Instytut Spraw Międzynarodowych, *Współpraca regionalna w Europie Środkowej po agresji Rosji na Ukrainę*, Warszawa 2024.
13. Bógdał-Brzezińska A., *Cyberbezpieczeństwo państwa*, Warszawa 2019.
14. Klimburg A., *The Darkening Web: The War for Cyberspace*, New York 2017.
15. Nye J., *Cyber Power*, Cambridge 2010.
16. Kuehl D., *From Cyberspace to Cyberpower*, Washington 2009.
17. Zenderowski R., *Europa Środkowo-Wschodnia w XX i XXI wieku*, Warszawa 2018.
18. Świder K., *Europa Środkowo-Wschodnia w myśli geopolitycznej XX wieku*, Warszawa 2018.
19. Eberhardt P., *Europa Środkowa jako region geopolityczny*, Warszawa 2005.

20. Gizicki W., Łoś P., *Geopolityka Trójmorza*, Przestrzeń Społeczna 2019.

21. Kurečić P., *The Three Seas Initiative: Geographical Determinants and Geopolitical Foundations*, Hrvatski Geografski Glasnik 2018.

22. Bieńczyk-Missala A., *Od Międzymorza do Trójmorza – meandry polityki zagranicznej Polski*, Stosunki Międzynarodowe 2018.

23. Melissen J., *The New Public Diplomacy*, London 2005.

24. Druckman D., Wallensteen P., *Negotiating with Leaders*, London 2016.

25. Cohen S., *Geopolitics: The Geography of International Relations*, Lanham 2015.

26. Mackinder H.J., *Democratic Ideals and Reality*, London 1919.

27. Rada Unii Europejskiej, *EU–NATO Cooperation on Cybersecurity*, Bruksela 2022.

28. RAND Corporation, *Cyber Deterrence and Stability*, Santa Monica 2020.

29. World Economic Forum, *Global Cybersecurity Outlook*, Geneva 2023.