SPRAWY MIĘDZYNARODOWE

2025, t. 78, nr 3
ISSN 0038-853X
e-ISSN 2720-0361
DOI 10.35757/SM.2025.78.3.05

IGOR PROTASOWICKI
Akademia Finansów i Biznesu „Vistula"
ORCID: 0000-0002-8707-1092
igor@protasowicki.eu

Cyberbezpieczeństwo jako wektor napięć i negocjacji w relacjach Stanów Zjednoczonych i Federacji Rosyjskiej

Cyber Security as a Vector of Tension and Negotiation in Relations between the United States and the Russian Federation

Słowa kluczowe:
cyberprzestrzeń, Federacja Rosyjska, Rosja, Stany Zjednoczone, USA, zagrożenia, relacje, infrastruktura krytyczna, strategia

Keywords:
cyberspace, Russian Federation, Russia, United States, USA, threats, relations, critical infrastructure, strategy

Cyberbezpieczeństwo jako wektor napięć i negocjacji w relacjach Stanów Zjednoczonych i Federacji Rosyjskiej

Cyberprzestrzeń stała się kluczowym wymiarem stosunków międzynarodowych i pełnoprawnym polem rywalizacji strategicznej, wykraczając poza funkcje komunikacyjne i administracyjne. W artykule podjęto się analizy stosunków między Stanami Zjednoczonymi a Federacją Rosyjską realizowanych w cyberprzestrzeni, ukazując je jako złożoną mieszankę współzależności, konfrontacji i prób dialogu. Począwszy od zimnowojennych fundamentów infrastruktury sieciowej, przez transformacje geopolityczne lat dziewięćdziesiątych, aż po współczesne strategie cyberobrony obie strony rozwijały odmienne podejścia do cyberbezpieczeństwa. Federacja Rosyjska integruje operacje informacyjne z działaniami wywiadowczymi i wojskowymi, koncentrując się na asymetrycznym oddziaływaniu poprzez dezinformację, sabotaż infrastruktury krytycznej i cyberszpiegostwo. USA przyjęły z kolei proaktywną strategię *defend forward* i *persistent engagement*, dążąc do neutralizacji zagrożeń poza własnym terytorium. Istotnym narzędziem w tej rywalizacji są operacje wpływu, które – jak pokazały wybory w USA w 2016 i 2020 r. – mają potencjał destabilizacyjny. Strategiczne znaczenie zyskuje również ochrona infrastruktury krytycznej. W obliczu eskalujących napięć możliwe są trzy scenariusze rozwoju relacji tych państw: dalsza konfrontacja, zimna cyberwojna lub reset poprzez dyplomację cyfrową. Każdy z nich uzależniony jest od efektywności mechanizmów zaufania, norm prawnych i gotowości do współpracy w dynamicznie ewoluującym środowisku cybernetycznym.

Cyber Security as a Vector of Tension and Negotiation in Relations between the United States and the Russian Federation

Cyberspace has become a key dimension of international relations, going beyond communication and administrative functions to become a full-fledged field of strategic competition. This article undertakes an analysis of the relationship between the United States and the Russian Federation as implemented in cyberspace, showing it as a complex mix of interdependence, confrontation and attempts at dialogue. From the Cold War foundations of network infrastructure, through the geopolitical transformations of the 1990s, to contemporary cyber defence strategies, the two sides have developed different approaches to cyber security. The Russian Federation integrates information operations with intelligence and military operations, focusing on asymmetric influence through disinformation, sabotage of critical infrastructure and cyber espionage. The USA, on the other hand, has adopted a proactive defend forward and persistent engagement strategy, seeking to neutralise threats outside its own territory. Influence operations, which, as the 2016 and 2020 US elections have shown, have destabilising potential, are an important tool in this competition. The protection of critical infrastructure is also becoming critical. In the face of escalating tensions, three scenarios for the relationship are possible: further confrontation, cyber cold war or reset through digital diplomacy. Each depends on the effectiveness of trust mechanisms, legal norms and willingness to cooperate in a dynamically evolving cyber environment.

Cyberprzestrzeń jako wymiar stosunków międzynarodowych

Rozwój technologiczny i cywilizacyjny sprawiają, że współczesne zbiorowości funkcjonują w ramach społeczeństwa informacyjnego. Oprócz wykorzystywania systemów komputerowych w codziennych czynnościach i wspomagania działalności obywateli oraz tworzonych przez nich organizacji cyberprzestrzeń stała się naturalnym obszarem funkcjonowania państw. Skala przepływu informacji powoduje, że działania w tej sferze stanowią wsparcie dla tradycyjnej działalności w ramach przestrzeni wyznaczanych granicami państwowymi, w tym tradycyjnych stosunków politycznych, gospodarczych i militarnych. Mowa przy tym zarówno o działaniach pożądanych, polegających na wspieraniu komunikacji, jak i niepożądanych, czyli wykorzystywaniu globalnej sieci i jej zasobów jako narzędzia wpływu w polityce zagranicznej, na przykład przez rozpowszechnianie nieprawdziwych informacji i manipulowanie obywatelami innego państwa. W tym sensie cyberprzestrzeń nie jest już tylko infrastrukturą komunikacyjną, lecz kolejną – obok lądu, morza, powietrza i kosmosu – domeną rywalizacji państw. W polskiej literaturze zwraca się uwagę, że przesunięcie rywalizacji mocarstw do domeny technologicznej i informacyjnej nie jest zjawiskiem nowym, lecz stanowi naturalne następstwo dążeń do maksymalizacji przewagi strategicznej w warunkach globalizacji. Cyberprzestrzeń stała się nie tylko polem walki o bezpieczeństwo informacyjne, ale także instrumentem wpływu politycznego i gospodarczego[1]. Przeniesienie ciężaru rywalizacji do sfery cyfrowej wpisuje się w logikę realizmu w stosunkach międzynarodowych (jest to konkurencja o zasoby i przewagi strategiczne), ale także w podejścia liberalne (ze względu na rosnącą współzależność i znaczenie reżimów lub reguł). Na poziomie prakseologicznym – w duchu ujęć proponowanych w polskiej literaturze – cyberprzestrzeń można traktować jako zbiór środków i działań dobieranych przez państwa, aby maksymalizować skuteczność własnej polityki w warunkach ograniczeń, kosztów i niepewności.

Celem niniejszego opracowania jest zobrazowanie roli i znaczenia cyberprzestrzeni w relacjach rosyjsko-amerykańskich z uwzględnieniem szans i zagrożeń specyficznych dla tego obszaru, jak również strategii

1 Zob. *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, red. M. Górka, Difin, Warszawa 2014.

państw w zakresie cyberbezpieczeństwa oraz mechanizmów przeciwdziałania zagrożeniom w tej sferze. Artykuł lokuje się na styku badań nad bezpieczeństwem międzynarodowym i analiz strategicznych, uzupełniając lukę między opisem doktryn a empirycznym obrazem operacji w domenie cyfrowej (w tym operacji wpływu, działań na infrastrukturze krytycznej i cyberszpiegostwa). Wkładem tekstu do stanu badań jest zestawienie i porównanie kluczowych dokumentów strategicznych USA i Rosji z ostatnich dwóch dekad oraz osadzenie ich w ramie analitycznej, która pozwala ocenić kierunki i intensywność rywalizacji.

Badania na ten temat potwierdzają, że rola cyberprzestrzeni w polityce zagranicznej znacząco wzrosła, co znajduje odzwierciedlenie w rozwijanych współcześnie koncepcjach strategicznych oraz mechanizmach zapewniania bezpieczeństwa. Szczególnie interesującym przedmiotem obserwacji jest obecnie wpływ cyberprzestrzeni na politykę zagraniczną i dynamikę relacji międzynarodowych. Omawia się w tym zakresie aspekty teoretyczne i empiryczne. Pytania badawcze sformułowane na potrzeby rozważań prowadzonych w niniejszym artykule dotyczą po pierwsze, głównych strategii państw w zakresie wykorzystywania cyberprzestrzeni jako narzędzia polityki zagranicznej, a po drugie, sposobu, w jaki cyberprzestrzeń wpływa na kształtowanie się rywalizacji lub współpracy w ramach środowiska międzynarodowego oraz mechanizmów i instrumentów stosowanych w celu przeciwdziałania zagrożeniom w cyberprzestrzeni i umacniania bezpieczeństwa. W szczególności analizie poddane zostaną: ewolucja rosyjskich koncepcji informacyjnego przeciwstawiania się i ich implementacja w praktyce, przejście USA od ujęć defensywnych do strategii *defend forward* i *persistent engagement* oraz skuteczność mechanizmów dyplomacji cybernetycznej (GGE, OEWG i kanałów dwustronnych). Artykuł wykorzystuje triadę relacji państw według Klausa Knorra (współpraca – rywalizacja – walka) jako porządkującą typologię scenariuszy, a do oceny dynamiki posługuje się analizą kosztów i korzyści (*cost – benefit*) oraz kryteriami prakseologicznymi skuteczności czy efektywności działania.

Zmiennymi albo wyznacznikami operacjonalizującymi rywalizację w dalszych partiach tekstu są m.in.: intensywność incydentów cybernetycznych o znaczeniu strategicznym (liczba i charakter ataków na infrastrukturę krytyczną i cele rządowe), poziom jawnych i niejawnych działań wpływu (skala operacji informacyjnych i ich mierzalne skutki), kierunek i treść aktualizowanych dokumentów strategicznych (doktryn, strategii

i wytycznych resortowych), stopień instytucjonalizacji dialogu i mechanizmów *de-confliction* (norm, kanałów komunikacji i reżimów), oraz postawa i zdolności aktorów trzecich (NATO, UE i Chin), wpływające na kalkulacje Stanów Zjednoczonych i Rosji.

Pod względem źródłowym praca opiera się na dokumentach strategicznych USA i FR z lat 2000–2023, literaturze naukowej i analitycznej (m.in. raportach RAND, CSIS, RUSI, IISS i CCDCOE) oraz dorobku polskich autorów zajmujących się prakseologią stosunków międzynarodowych i bezpieczeństwem informacyjnym. Odwołania do głośnych przypadków empirycznych (Estonii z 2007 r., Gruzji z 2008, Ukrainy z lat 2015–2016 i 2022, wyborów w USA w 2016 i 2020 oraz kampanii „Solar Winds") służą jako studia ilustracyjne dla weryfikacji tendencji zidentyfikowanych w strategiach.

Ewolucja cyberrelacji USA i Rosji od czasów zimnej wojny po współczesność

W ujęciu problemowym geneza ARPANET pełni tu funkcję tła – wskazuje bowiem technologiczne źródła domeny, ale o właściwej ewolucji cyberrelacji decydują konkretne interakcje polityczno-strategiczne po 1991 r. (incydenty, doktryny, instytucje i praktyki operacyjne). Poniższy szkic historyczny zachowuje zatem genezę omawianego zjawiska jako kontekst i przechodzi do osiowych epizodów kształtujących dynamikę stosunków amerykańsko-rosyjskich w cyberprzestrzeni.

Można zaryzykować tezę, że samo istnienie internetu zawdzięczamy zimnej wojnie[2]. Po zakończeniu drugiej wojny światowej w ośrodku badawczym RAND Corporation opracowano koncepcję utworzenia rozproszonej sieci komunikacyjnej, podporządkowaną ówczesnemu bipolarnemu podziałowi świata oraz zagrożeniu konfliktem nuklearnym między mocarstwami. Nowe rozwiązanie miało zapewniać możliwość utrzymania komunikacji

2 Zob. M. Pudełko, *Prawdziwa historia internetu na świecie*, wyd. 4, IT Start, Piekary Śląskie 2020; N. Packard, *Internet Prehistory: ARPANET Chronology*, „Cogent Social Sciences" 2023, vol. 9, issue 2; R. Cohen-Almagor, *Internet History*, „International Journal of Technoethics" 2011, vol. 2, No. 2; A. Targowski, *From the Cold War to Internet Cathedral*, „International Journal of Information and Communication Technology Education" 2005, vol. 1, issue 2; J. Galbreath, *The Internet: Past, Present, and Future*, „Educational Technology" 1997, vol. 37, No. 6.

na wypadek zniszczenia części infrastruktury. Istotnym impulsem do jego wdrożenia było wystrzelenie przez ZSRR rakiety i umieszczenie na orbicie okołoziemskiej pierwszego sztucznego satelity – Sputnika. Wydarzenie do wywołało w USA szeroką dyskusję na temat konieczności przyspieszenia badań i poszukiwania możliwości zintensyfikowania współpracy między ośrodkami badawczo-rozwojowymi. Ten wątek, ważny dla historii technologii, wyznacza jedynie punkt „zero" późniejszej rywalizacji cyfrowej.

W związku z eskalującym napięciem na linii Waszyngton–Moskwa propozycja ta spotkała się z dużym zainteresowaniem i uzyskała dofinansowanie w Agencji ds. Zaawansowanych Projektów Badawczych (ARPA). Sieć, która miała połączyć komputery w najistotniejszych ośrodkach badawczo-rozwojowych USA, uruchomiona została 29 września 1969 r. Nazwano ją ARPANET, a przez kolejne dekady funkcjonowania włączano następne uczelnie i ośrodki badawcze. Środowisko to było stale udoskonalane i rozwijane, by można było do niego dołączać komputery tworzone w nowych architekturach. W związku z dużym zróżnicowaniem podłączanych systemów komputerowych od początku lat osiemdziesiątych zaczęto wprowadzać jednolite standardy, zastosowane wówczas protokoły transmisji danych przypominają te współczesne, a pojawiające się potrzeby przyczyniły się do powstania powszechnych dziś usług sieciowych. Po wprowadzeniu WWW wszelkie zmiany możemy uznać za kosmetyczne, natomiast główny nacisk kładzie się na przyspieszanie i zwiększanie przepustowości łącz oraz upowszechnianie dostępu do sieci[3]. Dalsza część niniejszej sekcji skupia się już na relacjach USA z Rosją w cyberprzestrzeni po zakończeniu zimnej wojny.

Po rozpadzie ZSRR stosunki amerykańsko-rosyjskie przeżywały okres względnej konwergencji interesów, a cyberprzestrzeń nie była jeszcze autonomicznym polem rywalizacji. Dyskurs na temat bezpieczeństwa koncentrował się na kontroli zbrojeń, transformacji ustrojowej i integracji gospodarczej, a kwestie cyfrowe pojawiały się marginalnie (w wymiarze przestępczości komputerowej i ochrony sieci rządowych).

Ataki DDoS na Estonię w 2007 r. (wymierzone w instytucje państwowe, banki i media) pokazały, że cyberoperacje mogą zakłócić funkcjonowanie państwa bez przekraczania progu użycia siły w klasycznym rozumieniu.

3 Z. Nowakowski, I. Protasowicki, *Bezpieczeństwo informacyjne a cyber terroryzm*, „Zeszyty Naukowe WSIZiA" 2009, nr 1 (9), s. 323–324.

Rok 2008 przyniósł skoordynowane działania w trakcie konfliktu rosyjsko-gruzińskiego, a na Zachodzie zintensyfikował debatę o kolektywnej obronie w cyberprzestrzeni w ramach NATO. Rosja umacniała w tym okresie własną koncepcję informacyjnego przeciwstawiania się, łącząc środki techniczne z operacjami psychologicznymi.

Aneksji Krymu i konfliktowi w Donbasie towarzyszyły działania w domenie cyfrowej, w tym operacje na infrastrukturze energetycznej Ukrainy („Black Energy" i „Industroyer"), które unaoczniły przejście od zakłóceń informacyjnych do fizycznych skutków w systemach OT/ICS. Równolegle intensyfikowane były operacje wpływu wymierzone w państwa zachodnie.

Wybory prezydenckie w USA w 2016 r. na trwałe wprowadziły do agendy politycznej problem ingerencji informacyjnej i manipulacji społecznej w wyniku działań podmiotów powiązanych z Rosją, w tym Agencji Badań Internetowych (ABI). W 2020 r. ujawniono operację „Solar Winds", czyli kampanię skierowaną przeciwko łańcuchowi dostaw poprawek oprogramowania wykorzystywanego m.in. przez podmioty zaliczane do infrastruktury krytycznej, którą przypisywano aktorom państwowym działającym przeciwko instytucjom USA i ich partnerom. Potwierdziło to rosnącą dojrzałość cyberwywiadowczą po stronie rosyjskiej. Jednocześnie odnotowana została przy tej sprawie aktywność jednostek GRU (np. Sandworm) oraz ugrupowań przypisywanych rosyjskiemu wywiadowi zagranicznemu (np. Cozy Bear / APT29).

Odpowiedzią Stanów Zjednoczonych była stopniowa ewolucja od paradygmatu reaktywnego do podejścia *persistent engagement* i *defend forward*, które akcentuje proaktywne zakłócanie wrogich kampanii jeszcze przed bramą. W praktyce obejmowało to działania U.S. Cyber Command (m.in. ofensywne operacje wymierzone w infrastrukturę podmiotów ingerujących w procesy wyborcze), rozwój współdzielenia informacji wywiadowczych oraz wzmacnianie odporności sektorów publicznego i prywatnego.

Wraz z eskalacją konfliktu zbrojnego w Ukrainie od 2022 r. obserwowano intensyfikację aktywności rosyjskich grup APT w regionie, a także operacje zakłócające, w tym przeciw łączności satelitarnej na początku inwazji. Po stronie USA i sojuszników wzrosła rola obrony kolektywnej w cyberprzestrzeni (NATO uznało cyber za domenę operacyjną), a także koordynacji reagowania na incydenty transgraniczne. Praktyka ta utrwaliła stan permanentnej rywalizacji poniżej progu otwartego konfliktu.

Rosyjskie doktryny i strategia cyberbezpieczeństwa

Już w latach dziewięćdziesiątych koncepcje strategiczne Federacji Rosyjskiej miały dość konfrontacyjny charakter. Zapowiadano w nich sprzyjanie tworzeniu wielobiegunowego świata przez wzmacnianie pozycji ekonomicznej i politycznej państw ściśle współpracujących z Rosją. Z drugiej strony Moskwa jawnie sprzeciwiała się umacnianiu porządku międzynarodowego wokół organizacji pod przywództwem państw zachodnich, ze szczególnym naciskiem na USA. Interesy Federacji Rosyjskiej miały polegać na równoprawnej i obopólnie korzystnej współpracy międzynarodowej. Zaznaczono, że kraj ten stoi w obliczu szerokiego spektrum wewnętrznych i zewnętrznych zagrożeń dla bezpieczeństwa narodowego, wśród których wskazywano na niezadowalający stan gospodarki narodowej, mankamenty systemu organizacji władzy państwowej i społeczeństwa obywatelskiego, pogłębiającą się w tym społeczeństwie polaryzację, kryminalizację kontaktów społecznych, wzrost poczucia zagrożenia przestępczością zorganizowaną i terroryzmem, a także niesprzyjające warunki geopolityczne. Co ciekawe, w strategii z omawianego okresu odrzucano jednostronne rozwiązywanie problemów geopolitycznych z wykorzystaniem siły wojskowej i z pominięciem standardów wyznaczanych przez prawo międzynarodowe[4]. Doświadczenia z 2014 i 2022 r. dowodzą jednak, że Federacja Rosyjska miała bardzo elastyczne podejście do realizacji własnych strategii w tym zakresie, zatem próba przewidzenia jej przyszłych zachowań na scenie międzynarodowej przez ten pryzmat może się okazać wysoce nieskuteczna. Istotnym punktem odniesienia pozostają kolejne edycje 'Doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej' z lat 2000 i 2016, które stanowią ramy koncepcyjne dla jej cyberpolityki. W doktrynie z 2000 r. szczególną uwagę poświęcono zagrożeniom dla jednolitej przestrzeni informacyjnej państwa. Dokument z 2016 r. rozszerzył te ujęcia, wskazując na cyberprzestrzeń jako domenę walki ideologicznej i narzędzie destabilizacji porządku wewnętrznego. Ich uzupełnieniem były kolejne 'Strategie bezpieczeństwa narodowego' z 2009, 2015 i 2021 r., w któ-

4 Z. Nowakowski, H. Szafran, R. Szafran, *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw*, Fundacja Niepodległości, Rzeszów 2009, s. 188–194.

rych podkreślono potrzebę integracji działań obronnych, wywiadowczych i propagandowych w domenie cyfrowej.

Już od początku XXI w. Federacja Rosyjska konsekwentnie rozwijała koncepcję cyberbezpieczeństwa jako integralnego elementu swojej strategii bezpieczeństwa narodowego. W takich dokumentach, jak 'Strategia bezpieczeństwa narodowego Federacji Rosyjskiej' z 2021 r. cyberprzestrzeń uznana została za kluczowy obszar rywalizacji międzynarodowej, w którym Rosja dostrzega zarówno zagrożenia, jak i możliwości projekcji własnej siły[5].

Rosyjskie podejście do cyberbezpieczeństwa opiera się na koncepcji informacyjnego przeciwstawiania się (*информационное противоборство*), która obejmuje zarówno działania techniczne, jak i psychologiczne. W ramach tej doktryny cyberoperacje są ściśle zintegrowane z działaniami wojskowymi, wywiadowczymi oraz propagandowymi, co pozwala na realizację celów strategicznych poprzez destabilizację przeciwnika i kontrolę nad własnym społeczeństwem[6]. W praktyce podejście to zmaterializowało się w działaniach określanych w literaturze jako wojny nowej generacji – opisywanych m.in. w „Przeglądzie Bezpieczeństwa Wewnętrznego" z lat 2014–2018. Ich istotą jest łączenie klasycznych środków militarnych z instrumentami informacyjnymi, cybernetycznymi i psychologicznymi, by osiągnąć przewagę strategiczną przy relatywnie niskich kosztach.

Federacja Rosyjska wykorzystuje swoje zdolności cybernetyczne do prowadzenia operacji ofensywnych, takich jak ataki na infrastrukturę krytyczną innych państw, kampanie dezinformacyjne oraz cyberszpiegostwo. Przykładem może być wykorzystanie technologii zakłócających systemy GPS w regionie Bałtyku, co jest interpretowane jako element rosyjskiej strategii wojny hybrydowej mającej na celu destabilizację Zachodu. Do katalogu działań należy również zaliczyć operacje typu APT (*advanced persistent threat*), które przypisywane są rosyjskim służbom, m.in. APT28 / Fancy Bear

5 Zob. *Указ Президента Российской Федерации от 02.07.2021 г. № 400 „О Стратегии национальной безопасности Российской Федерации"*, „Консультант плюс" [online, dostęp: 16 II 2025]: <https://www.consultant.ru/document/cons_doc_LAW_389271/>.

6 B. Lily, J. Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, [w:] *2020 12th International Conference on Cyber Conflict*, ed. T. Jančárková [i in.], NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2020, s. 130–147.

z ramienia GRU czy APT29 / Cozy Bear z ramienia SWR, odpowiedzialne za wiele kampanii cyberszpiegowskich wobec instytucji NATO, UE i USA. Ataki te charakteryzują się długotrwałością, wieloetapowością i ukierunkowaniem na pozyskanie wrażliwych danych strategicznych. Jednocześnie Rosja rozwija własną infrastrukturę cyberbezpieczeństwa, w tym systemy nadzoru elektronicznego, np. SORM, oraz promuje ideę suwerenności cyfrowej, dążąc do kontroli nad krajowym segmentem internetu i ograniczenia wpływów zagranicznych technologii[7].

Koncepcja suwerenności cyfrowej stanowi jedną z osi rosyjskiej polityki informacyjnej – zakłada stworzenie krajowych odpowiedników usług (np. Runet jako alternatywę dla globalnego internetu), możliwość odłączenia się od sieci światowej oraz kontrolę przepływu treści. Z punktu widzenia Moskwy jest to narzędzie ochrony systemu politycznego przed zewnętrzną ingerencją, a zarazem instrument umożliwiający sprawniejsze prowadzenie operacji ofensywnych.

Podsumowując, należy stwierdzić, że rosyjskie doktryny cyberbezpieczeństwa charakteryzuje kilka cech wspólnych: integracja cyberprzestrzeni z wojną informacyjną i psychologiczną, postrzeganie domeny cyfrowej jako narzędzia rywalizacji geopolitycznej i ideologicznej, dążenie do kontroli wewnętrznej poprzez suwerenność cyfrową, a także gotowość do stosowania ofensywnych środków technicznych i wywiadowczych w warunkach konfliktu poniżej progu wojny. Elementy te, konsekwentnie rozwijane od pierwszych lat XXI w., czynią z Rosji jednego z najaktywniejszych i najbardziej agresywnych aktorów w globalnej cyberprzestrzeni.

Amerykańskie podejście do cyberobrony i cyberodstraszania

W kluczowych punktach amerykańskie doktryny z analogicznego okresu są zbieżne ze stanowiskiem Federacji Rosyjskiej. Po zakończeniu zimnej wojny USA poświęciły szczególną uwagę procesom transformacji ustrojowej w Nowej Europie. Powolny rozpad Układu Warszawskiego wywoływał konieczność przebudowy architektury geopolitycznej, w skutek czego

7 T. Wang [i in.], *SORM-Enhanced Inverse Reliability Analysis for Geotechnical Multiobjective Reliability-Based Design Optimization*, „International Journal for Numerical and Analytical Methods in Geomechanics" 2025, vol. 49, issue 1, s. 185–200.

zajęcie dominującej pozycji w nowym układzie sił stało się dla Stanów Zjednoczonych celem strategicznym. Stanowisko to podtrzymywane było w kolejnych dokumentach strategicznych z 1991, 1994 i 1996 r. Z ich perspektywy gwarantem stabilizacji na kontynencie europejskim miały być postępujące procesy integracyjne, natomiast pod względem militarnym rolę sprawczą koncentrowano wokół Sojuszu Północnoatlantyckiego. Katalizatorem współpracy miał być program „Partnerstwo dla Pokoju", zainicjowany w ramach NATO w styczniu 1994 r. W strategii bezpieczeństwa USA z 1997 r. ustawodawca uznał, że kontynuacja reform demokratycznych i rynkowo-ekonomicznych ma istotne znaczenie także dla bezpieczeństwa USA. Wówczas jeszcze Rosja przedstawiana była jako pełnoprawny uczestnik budowy zintegrowanej i demokratycznej Europy. Od początku XXI w. Amerykanie jasno wskazują, że w swojej polityce zagranicznej wybierają przywództwo nad izolacjonizmem i zajmowanie się wyzwaniami geopolitycznymi zamiast pozostawiania ich przyszłym pokoleniom. Sygnalizują także intencje związane z rolą, jaką USA przyjmuje na arenie stosunków międzynarodowych, dążąc do kształtowania światowego ładu poprzez wpływanie na bieżące wydarzenia[8].

W 2003 r. opublikowano *National Strategy to Secure Cyberspace* – pierwszy dokument kompleksowo ujmujący zagrożenia cyfrowe dla bezpieczeństwa narodowego. W 2008 r. wdrożono *Comprehensive National Cybersecurity Initiative*, która położyła nacisk na modernizację ochrony sieci federalnych oraz zacieśnienie współpracy z sektorem prywatnym. Począwszy od 2011 r. pojawiły się kolejne dokumenty *Department of Defense Cyber Strategy*, w których cyberprzestrzeń uznano za pełnoprawną domenę operacyjną. Strategia z 2015 r. zarysowała pojęcie cyberodstraszania, a ta z 2018 przyjęła koncepcję *defend forward* i *persistent engagement*, czyli działań wyprzedzających i aktywnego zakłócania kampanii wroga[9]. W ramach tej doktryny cyberoperacje są ściśle zintegrowane z działaniami wojskowymi, wywiadowczymi oraz dyplomatycznymi, co pozwala na realizację celów strategicznych poprzez destabilizację przeciwnika i kontrolę nad własnym społeczeństwem.

8 Z. Nowakowski, H. Szafran, R. Szafran, *Bezpieczeństwo...*, s. 245–251.

9 M. Smeets, *U.S. Cyber Strategy of Presidential Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection*, „Intelligence and National Security" 2020, vol. 35, No. 3, s. 444–453.

Szczególne znaczenie miało powstanie w 2009 r. i rozwój U.S. Cyber Command, które w 2018 uzyskało status pełnego dowództwa bojowego. Od tego momentu USA zaczęły wprost deklarować gotowość prowadzenia operacji ofensywnych, co znalazło wyraz m.in. w działaniach przeciwko rosyjskim grupom ingerującym w wybory w 2018 r. (*hunt forward operations*).

W amerykańskim podejściu widoczna jest także ewolucja środków prawnych i instytucjonalnych. *Cybersecurity Information Sharing Act* z 2015 r. stworzył ramy do prowadzenia między sektorem prywatnym a rządem wymiany informacji o zagrożeniach. W 2023 r. administracja Joe Bidena ogłosiła nową *National Cybersecurity Strategy*, która akcentuje odpowiedzialność dostawców technologii za bezpieczeństwo produktów (*secure by design*), zwiększa rolę współpracy międzynarodowej i przewiduje bardziej zdecydowane działania ofensywne wobec wrogich podmiotów[10].

Jednocześnie USA rozwijają własną infrastrukturę cyberbezpieczeństwa, w tym systemy nadzoru elektronicznego, oraz promują ideę suwerenności cyfrowej, dążąc do kontroli nad krajowym segmentem internetu i ograniczenia wpływów zagranicznych technologii. W tym kontekście warto zauważyć, że amerykańska strategia cyberbezpieczeństwa kładzie duży nacisk na współpracę międzynarodową oraz budowanie sojuszy na rzecz przeciwdziałania wspólnym zagrożeniom w cyberprzestrzeni.

W amerykańskich strategiach cyberprzestrzeń definiowana jest jako przestrzeń globalna, w której bezpieczeństwo można osiągnąć wyłącznie poprzez współpracę z sojusznikami i partnerami. kluczowymi partnerami USA są tu zaś NATO oraz UE. Szczególną wagę przywiązuje się do art. 5 *Traktatu waszyngtońskiego*, który od 2014 r. formalnie obejmuje również poważne cyberataki. W praktyce oznacza to, że Stany Zjednoczone traktują cyberprzestrzeń jako wymiar odstraszania zbiorowego – uzupełniający klasyczne środki konwencjonalne i nuklearne. Ponadto współpraca w ramach mającej siedzibę w Tallinnie NATO CCDCOE oraz inicjatywy UE (np. *European Cybersecurity Act*) postrzegane są jako elementy wzmacniania odporności Sojuszu.

10 Zob. *The National Cybersecurity Strategy*, „The White House" [online], March 2023 [dostęp: 3 IV 2025] <https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/>.

Operacje wywierania wpływu i dezinformacja jako narzędzia polityki zagranicznej

Operacje związane z wywieraniem wpływu i dezinformacja stanowią istotne narzędzia polityki zagranicznej, wykorzystywane przez państwa do kształtowania opinii publicznej i wpływania na procesy polityczne w innych krajach. W kontekście prowadzonych rozważań warto zauważyć, że to przede wszystkim Rosja zintensyfikowała swoje działania w tym zakresie, wykorzystując zaawansowane techniki informacyjne do realizacji celów strategicznych. Działania te osadzone są w doktrynie informacyjnego przeciwstawiania się, która łączy środki technologiczne z operacjami psychologicznymi, mającymi na celu destabilizację struktur społecznych i osłabienie zaufania do instytucji demokratycznych. Rosyjskie podejście zakłada długofalowe oddziaływanie poprzez złożone kampanie dezinformacyjne, obejmujące zarówno kanały tradycyjne, jak i media społecznościowe, co umożliwia dotarcie do szerokich grup odbiorców. Kluczową cechą tych operacji jest ich adaptacyjny charakter – zdolność do szybkiego modyfikowania narracji oraz eksploatowania lokalnych podziałów społeczno-politycznych w państwach będących celem oddziaływania[11]. W literaturze, np. raportach RAND, CSIS czy Hybrid CoE, podkreśla się, że dezinformacja pełni dla Rosji funkcję broni asymetrycznej – jest relatywnie tania, trudna do jednoznacznego przypisania oraz skuteczna w erodowaniu spójności Zachodu. Instrument ten jest również sprzężony z wywiadowczymi i ofensywnymi działaniami w cyberprzestrzeni, co zwiększa jego zasięg strategiczny.

Przykładem zachowania Federacji Rosyjskiej mogą być próby wywierania wpływu na amerykańskie wybory prezydenckie w 2016 i 2020 r. Pierwsza z tych elekcji stała się celem szeroko zakrojonej kampanii dezinformacyjnej prowadzonej przez różne jednostki inspirowane działaniami Kremla. Zgodnie z raportem specjalnego prokuratora Roberta Muellera rosyjska ABI prowadziła w mediach społecznościowych kampanię mającą na celu wsparcie kandydatury Donalda Trumpa oraz dyskredytację Hillary Clinton. Działania te obejmowały tworzenie fałszywych kont, organizowanie wydarzeń politycznych oraz rozpowszechnianie dezinformacji na takich platformach jak „Facebook"

11 F. Bryjka, T. Chłoń, R. Kupiecki, *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe „Scholar", Warszawa 2022, s. 161–186.

i „Twitter"[12]. Według danych Biura Dyrektora Wywiadu Narodowego (ODNI) oraz analiz amerykańskich *think tanków* działania te miały charakter skoordynowany i były wspierane przez kampanie hakerskie, takie jak włamania do skrzynek mailowych Demokratów (*DNC hack*), co ilustruje synergiczne wykorzystanie narzędzi technicznych i psychologicznych.

W wyborach prezydenckich w 2020 r. Rosja kontynuowała swoje działania dezinformacyjne, choć w zmienionej formie. Zamiast prowadzenia bezpośrednich ataków hakerskich skupiono się na kampaniach wpływu w mediach społecznościowych, mających na celu podważenie zaufania do procesu wyborczego oraz wsparcie określonych narracji politycznych. Raport ODNI potwierdza, że Rosja dążyła do osłabienia kampanii Bidena poprzez rozpowszechnianie dezinformacji[13]. Co istotne, narracje były bardziej zniuansowane: koncentrowały się nie na bezpośrednim wsparciu jednego kandydata, lecz na podważeniu zaufania do całego procesu demokratycznego, co wpisuje się w długofalowy cel strategiczny Rosji – erozję wiarygodności instytucji amerykańskiego państwa.

Rosyjskie kampanie dezinformacyjne w przestrzeni anglojęzycznej nie ograniczają się do samych Stanów Zjednoczonych. Niezależnie od celu charakteryzują się wykorzystaniem zaawansowanych technologii oraz zrozumieniem lokalnych kontekstów społeczno-politycznych. Przykładem mogą być inspirowane przez Kreml działania przeciwko Wielkiej Brytanii. Sieć Prawda (znana również jako Portal Kombat) prowadzi zautomatyzowane strony internetowe publikujące treści w językach angielskim, walijskim i szkockim gaelickim. Celem tych działań jest podważenie zaufania do instytucji demokratycznych, osłabienie poparcia dla Ukrainy oraz szerzenie prorosyjskich narracji. Sieć opiera się na treściach pochodzących z rosyjskich mediów państwowych, „Telegramu" oraz kanałów *influencerów* powiązanych z Kremlem[14]. Opisywane działania mają charakter długofa-

12 Zob. tzw. raport Muellera: R. S. Meller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1, U.S. Department of Justice, Washington, March 2019.

13 A. Greenberg, *Foreign Meddling Flooded the 2020 Election – but Not by Hackers*, „Wired" [online], 16 III 2021 [dostęp: 5 IV 2025]: <https://www.wired.com/story/odni-russia-iran-2020-election-interference/>.

14 J. Judah, F. Hamilton, *Russia Using AI to Target Britons with Flood of Fake News*, „The Times" [online], 29 IV 2025 [dostęp: 5 IV 2025]: <https://www.thetimes.com/uk/defence/article/russia-ai-disinformation-pravda-fake-news-plbwwn7v0>.

lowy i są elementem szerszej strategii w polityce zagranicznej Federacji Rosyjskiej. Ich celem nie jest krótkotrwałe wspieranie określonej narracji, ale systematyczne podważanie zaufania do instytucji demokratycznych w państwach Zachodu. Realizację tych zadań powierzono m.in. ABI, czyli funkcjonującej na polecenie Putina farmie trolli, która prowadzi zorganizowane kampanie dezinformacyjne i ingeruje w przebieg oraz wyniki wyborów[15]. Podobne kampanie odnotowano także w innych krajach europejskich, np. w 2017 r. we Francji i w 2017 oraz 2021 w Niemczech, gdzie Rosja starała się wpływać na wyniki wyborów poprzez wzmacnianie partii skrajnych i podsycanie nieufności wobec unijnych instytucji.

Badania przeprowadzone przez Hybrid CoE wskazują, że rosyjskie kampanie dezinformacyjne są skuteczne w eksploatowaniu społecznych i politycznych słabości w krajach docelowych. Poprzez promowanie takich narracji jak *russkij mir* czy słowiańska jedność Rosja wpływa na postawy społeczne w takich krajach jak Gruzja, Ukraina, Słowacja, Czechy, Węgry i Serbia, zniechęcając je do integracji z Zachodem[16]. Wyniki badań prowadzą do wniosku, że skuteczność tych operacji nie polega na przekonaniu odbiorców do określonej narracji, lecz na zasianiu wątpliwości i wywołaniu dezorientacji. W tym sensie celem nie jest wygranie sporu informacyjnego, ale doprowadzenie do sytuacji, w której odbiorcy nie ufają żadnym źródłom informacji. To stanowi największe zagrożenie dla demokracji liberalnych.

Infrastruktura krytyczna jako cel działań ofensywnych

Infrastruktura krytyczna stanowi fundament funkcjonowania współczesnych państw, obejmując takie sektory jak energetyka, transport czy opieka zdrowotna. W dobie rosnącej cyfryzacji i integracji systemów informatycznych jest ona coraz bardziej narażona na działania ofensywne w cyberprzestrzeni. Cyberataki na te sektory mogą prowadzić do poważnych zakłóceń w świadczeniu podstawowych usług, wpływając negatywnie na bezpieczeństwo wewnętrzne oraz stabilność społeczną państw.

15 F. Bryjka, *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych*, „Sprawy Międzynarodowe" 2022, t. 75, nr 2, s. 76.

16 A. Hoyle, J. Šlerka, *Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns*, Hybrid CoE, [b.m.w.] March 2024 (Hybrid CoE Working Paper, 29), s. 11–24.

Sektor energetyczny jest jednym z głównych celów cyberataków ze względu na jego kluczowe znaczenie dla funkcjonowania państwa. Przykładem jest atak *ransomware* na Colonial Pipeline w maju 2021 r., który doprowadził do czasowego wstrzymania dostaw paliw na wschodnim wybrzeżu Stanów Zjednoczonych, powodując ich niedobory i wzrost cen[17]. Innym przypadkiem jest masowa awaria zasilania, która dotknęła Hiszpanię i Portugalię w kwietniu 2025 r., skutkująca zakłóceniami w transporcie i opiece zdrowotnej oraz śmiercią kilku osób[18].

Systemy transportowe, w tym lotnictwo, kolej i transport miejski, są coraz częściej celem cyberataków. W 2024 r. odnotowano znaczny wzrost liczby naruszeń danych w sektorze transportu, a precyzyjnie 3205 incydentów, co stanowi wzrost o 78 proc. w porównaniu do roku poprzedniego[19]. Ataki te mogą prowadzić do opóźnień, zakłóceń w harmonogramach oraz zagrożeń dla bezpieczeństwa pasażerów.

Szczególnie wrażliwy na cyberataki jest sektor opieki zdrowotnej – ze względu na przechowywanie wrażliwych danych pacjentów oraz konieczność ciągłego działania systemów medycznych. W maju 2017 r. atak *ransomware* Wanna Cry sparaliżował działanie Narodowej Służby Zdrowia w Wielkiej Brytanii, prowadząc do odwołania tysięcy wizyt i operacji[20]. Podobnie w marcu 2025 r. atak na szpital w Australii skutkował wyciekiem danych ponad 2 tys. pacjentów.

Cyberataki na infrastrukturę krytyczną mają bezpośredni wpływ na bezpieczeństwo wewnętrzne państw. Zakłócenia w dostawach energii, transporcie czy opiece zdrowotnej mogą prowadzić do paniki społecznej,

17 *US Invokes Emergency Powers after Cyber-Attack on Fuel Pipeline*, „The Guardian" [online], 10 V 2021 [dostęp: 7 IV 2025]: <https://www.theguardian.com/us-news/2021/may/10/us-invokes-emergency-powers-after-cyberattack-shuts-crucial-fuel-pipeline>.

18 S. Jones, *Pedro Sánchez Vows to Find the Cause of Huge Power Cut in Spain and Portugal*, „The Guardian" [online], 29 IV 2025 [dostęp: 30 IV 2025]: <https://www.theguardian.com/world/2025/apr/29/spain-portugal-returning-normal-experts-cause-blackout>.

19 Zob. S. Bowcut, *Digital Safeguards: Navigating Cybersecurity in Transportation*, „Cybersecurity Guide" [online], 3 IV 2025 [dostęp: 7 IV 2025]: <https://cybersecurityguide.org/industries/transportation/>.

20 J. Kroustek, *WannaCry Ransomware That Infected Telefonica and NHS Hospitals Is Spreading Aggressively, with over 50,000 Attacks so far Today*, „Avast" [online], 12 V 2017 [dostęp: 7 IV 2025]: <https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today>.

spadku zaufania do instytucji publicznych oraz destabilizacji gospodarczej. Według raportu RAND Corporation skoordynowane ataki na infrastrukturę krytyczną mogą ograniczyć zdolności decyzyjne państwa, zakłócić mobilizację wojskową oraz narzucić społeczeństwu znaczące koszty[21].

Przykładami ataków na infrastrukturę krytyczną są działania przeciwko ukraińskiemu sektorowi energetycznemu z 2015 i 2016 r.[22], atak Not Petya z 2017[23], atak na sieć wodociągową w USA z 2021[24], zakłócanie sygnału GPS i systemów lotniczych w krajach bałtyckich w latach 2018–2024[25] czy atak „Solar Winds" z 2020[26]. W obliczu wzrostu zagrożenia takimi operacjami konieczne jest wdrażanie kompleksowych strategii bezpieczeństwa cybernetycznego, obejmujących zarówno środki techniczne, jak i organizacyjne, które zapewnią ciągłość działania kluczowych sektorów oraz ochrony obywateli.

21 B. R. Kane [i in.], *Defending the United States against Critical Infrastructure Attacks. Exploring a Hypothetical Campaign of Cascading Impacts*, RAND Corporation, [b.m.w.] 2024 (Inverted Rook Research Report), s. 3–10.

22 Atak przeprowadzony przez grupę Sandworm, wskutek którego ok. 230 tys. mieszkańców zachodniej Ukrainy przez kilka godzin nie miało dostępu do energii elektrycznej. W drugiej fali ataku na sieci elektroenergetyczne wykorzystano złośliwe oprogramowanie *Industroyer*.

23 Atak przeprowadzony przez grupę Sandworm z wykorzystaniem autorskiego szkodliwego oprogramowania *Not Petya*, którego celem były przede wszystkim podmioty ukraińskie, ale ostatecznie doprowadził do paraliżu systemów informatycznych takich jak firm Maersk i Merck oraz wielu instytucji rządowych na świecie. Straty szacuje się na ok. 10 mld dol.

24 Powiązani z Rosją hakerzy (w tym grupa APT28 / Fancy Bear) wykorzystali luki w systemie SCADA używanym przez sieć wodociągową w Oldsmar na Florydzie i podjęli próbę podniesienia poziomu wodorotlenku sodu stosowanego do regulacji pH do wartości przeszło stukrotnie przekraczającej bezpieczną.

25 Federacja Rosyjska wielokrotnie zakłócała sygnał GPS w regionie Bałtyku i Arktyki, zwłaszcza w czasie ćwiczeń organizowanych przez Sojusz Północnoatlantycki, utrudniając nie tylko działania sił zbrojnych, lecz także funkcjonowanie żeglugi i lotnictwa cywilnego, m.in. Norwegii, Finlandii i Szwecji.

26 Jako element rozbudowanej kampanii grupa APT29 / Cozy Bear zainfekowała aktualizację oprogramowania *Orion* firmy Solar Winds zajmującej się produkcją oprogramowania do zarządzania siecią i infrastrukturą oraz ich monitoringu. Dzięki wykorzystaniu zagrożenia typu *code injection* szkodliwe oprogramowanie trafiło do ok. 18 tys. odbiorców, m.in. Agencji Bezpieczeństwa Narodowego oraz departamentów Skarbu, Energetyki i Handlu, umożliwiając hakerom przechwycenie danych z zainfekowanych systemów.

Dyplomacja cybernetyczna – dialog czy gra pozorów?

Dyplomacja cybernetyczna stała się kluczowym narzędziem w zarządzaniu relacjami międzynarodowymi w przestrzeni wirtualnej. Jej celem jest nie tylko zapobieganie konfliktom, ale także budowanie zaufania i ustanawianie norm postępowania w cyberprzestrzeni. Skuteczność tych działań budzi jednak kontrowersje, zwłaszcza w kontekście eskalujących napięć między państwami o konkurencyjnych interesach cyfrowych. Istotą cyberdyplomacji jest przeniesienie klasycznych narzędzi dyplomatycznych (dialogu, mediacji i tworzenia reżimów międzynarodowych) do sfery cyfrowej, w której problemami szczególnymi są atrybucja ataków, brak jasnych reguł odpowiedzialności i trudność w wyznaczeniu progów eskalacji.

W odpowiedzi na rosnące zagrożenia w cyberprzestrzeni państwa podejmują próby ustanawiania bezpośrednich kanałów komunikacji, które pozwolą szybko reagować na incydenty i zapobiegać eskalacji konfliktów. Przykładem jest inicjatywa CATALINK, proponująca utworzenie trójstronnego kanału komunikacji kryzysowej między Stanami Zjednoczonymi, Wielką Brytanią i Francją. Celem tego mechanizmu jest umożliwienie szybkiej wymiany informacji i koordynacji działań w sytuacjach kryzysowych, zwłaszcza w kontekście zagrożeń nuklearnych i cybernetycznych[27]. Podobne kanały komunikacji rozwija NATO, które od 2014 r. traktuje cyberprzestrzeń jako domenę operacyjną. W ramach Sojuszu prowadzone są konsultacje w sprawie reagowania na incydenty cybernetyczne, a takie ćwiczenia jak „Locked Shields" w Estonii służą testowaniu mechanizmów koordynacji między państwami członkowskimi.

Podobne mechanizmy testowane były w relacjach między Stanami Zjednoczonymi a Chinami. W 2015 r. oba państwa osiągnęły porozumienie dotyczące zwalczania cyberprzestępczości i ustanowiły wspólny mechanizm dialogu[28]. W kolejnych latach jednak, w wyniku rosną-

27 D. Zhukov, *The Phone-a-Friend Option: Use Cases for a U.S.-U.K.-French Crisis Communication Channel*, Institute for Security and Technology, [b.m.w.] June 2024: <https://securityandtechnology.org/wp-content/uploads/2024/10/CATALINK-P3.pdf> [dostęp: 16 II 2025].

28 M. Xu, Ch. Lu, *China–U.S. Cyber-Crisis Management*, „China International Strategy Review" 2021, vol. 3, issue 1: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8237537/pdf/42533> [dostęp: 10 IV 2025].

cych napięć politycznych i gospodarczych, wiele z tych kanałów komunikacji zostało zawieszonych, co utrudniło skuteczne zarządzanie kryzysami w cyberprzestrzeni. Również w relacjach USA z Rosją podejmowano próby tworzenia dialogu eksperckiego i mechanizmów deeskalacji, m.in. w ramach *cyberhotline* i spotkań roboczych w latach 2013–2017. Wybuch konfliktu w Ukrainie w 2014 r. i ingerencje w amerykańskie wybory znacząco ograniczyły jednak zaufanie, co doprowadziło do faktycznego zamrożenia tych inicjatyw.

Analiza skuteczności dwustronnych i wielostronnych mechanizmów kontroli eskalacji w cyberprzestrzeni wskazuje na mieszane rezultaty. Inicjatywy takie jak Grupa Ekspertów Rządowych ONZ ds. Rozwoju w Dziedzinie Informacji i Telekomunikacji (GGE) mają potencjał, by w przyszłości znacząco przyczynić się do ustanowienia podstawowych norm zachowania państw w cyberprzestrzeni. Z drugiej strony nie sposób zignorować ryzyka, że brak wiążących porozumień i różnice w interpretacji istniejących norm ostatecznie ograniczą ich skuteczność. Wyniki prac GGE i Open-Ended Working Group (OEWG) pokazały, że możliwe jest osiągnięcie częściowego konsensusu – np. co do zakazu ataków na infrastrukturę krytyczną w czasie pokoju – lecz brak mechanizmów egzekucyjnych sprawia, że normy te mają przede wszystkim charakter deklaratywny[29].

Ponadto różnice w podejściu do suwerenności cyfrowej i zarządzania internetem między państwami demokratycznymi a autorytarnymi utrudniają osiągnięcie konsensusu w kwestiach kluczowych dla bezpieczeństwa cybernetycznego. W rezultacie wiele inicjatyw dyplomatycznych w cyberprzestrzeni pozostaje na etapie deklaracji, bez realnego wpływu na zachowania państw. Państwa demokratyczne promują model otwartego internetu i wielostronnego zarządzania (*multi-stakeholder approach*), podczas gdy Rosja i Chiny forsują koncepcję suwerenności cyfrowej oraz większej roli organizacji międzyrządowych kosztem podmiotów prywatnych. Ten rozdźwięk sprawia, że cyberdyplomacja coraz częściej przybiera charakter gry pozorów – oficjalnie deklaruje wolę współpracy, lecz faktycznie utrwala podziały w systemie międzynarodowym.

29 B. Hogeveen, *The UN Norms of Responsible State Behaviour in Cyberspace. Guidance on Implementation for Member States of ASEAN*, Australian Strategic Policy Institute, [b.m.w.] March 2022.

Scenariusze stosunków amerykańsko-rosyjskich w sferze cyber

Relacje między Stanami Zjednoczonymi a Federacją Rosyjską w obszarze cyberbezpieczeństwa charakteryzują się dynamicznym napięciem, wynikającym z odmiennych interesów strategicznych, asymetrii w postrzeganiu zagrożeń oraz braku trwałych mechanizmów kontroli eskalacji. Analiza możliwych ścieżek rozwoju tych stosunków wskazuje na trzy główne scenariusze: intensyfikację konfliktu, utrwalenie stanu zimnej cyberwojny oraz próbę resetu poprzez dyplomację cyfrową.

Konstrukcja scenariuszy opiera się na klasyfikacji współpraca – rywalizacja – walka[30], uzupełnionej o podejście prakseologiczne, które pozwala uchwycić logikę działań państw w warunkach ograniczonych zasobów i wysokiej niepewności[31]. Przy ich tworzeniu wykorzystano takie wskaźniki jak: częstotliwość cyberincydentów o charakterze strategicznym, poziom wzajemnego zaufania w dialogu dyplomatycznym, stanowisko organizacji międzynarodowych (NATO, UE czy OUBZ) oraz aktywność aktorów trzecich (zwłaszcza Chin).

Intensyfikacja konfliktu – eskalacja w cieniu konwencjonalnych napięć

W obliczu trwających napięć geopolitycznych, szczególnie związanych z wojną w Ukrainie, istnieje ryzyko eskalacji działań cybernetycznych między USA a Rosją. Rosyjskie służby wywiadowcze, takie jak GRU, prowadzą kampanie sabotażu i dezinformacji, które nasilają się w Europie i Stanach Zjednoczonych. Przykładami są ataki na systemy energetyczne i transportowe, które mogą prowadzić do poważnych zakłóceń w funkcjonowaniu państw.

Stany Zjednoczone z kolei poprzez działania U.S. Cyber Command podejmują ofensywne operacje mające na celu neutralizację zagrożeń, co może prowadzić do dalszego zaogniania konfliktu. Brak skutecznych mechanizmów komunikacji i kontroli eskalacji zwiększa ryzyko niezamierzonych konsekwencji, które mogą doprowadzić do rozszerzenia zasięgu konfliktu.

30 M. Sułek, *Prakseologiczna teoria stosunków międzynarodowych*, „Przegląd Strategiczny" 2012, nr 1, s. 39–40.

31 Tenże, *Trzy działy prakseologii*, „Rocznik Naukowy Wydziału Zarządzania w Ciechanowie" 2008, t. 2, z. 1–2, s. 53–69.

W tym scenariuszu cyberprzestrzeń staje się areną eskalacji równoległej do konfrontacji konwencjonalnej, a granica między operacjami poniżej progu wojny a działaniami mogącymi wywołać odpowiedź militarną ulega zatarciu. Szczególnie podatnym celem pozostaje infrastruktura krytyczna, zakłócenie funkcjonowania której może mieć nie tylko skutki gospodarcze, ale i humanitarne.

Zimna cyberwojna – trwała rywalizacja bez otwartego konfliktu

Alternatywnym scenariuszem jest utrwalenie stanu zimnej cyberwojny, charakteryzującej się stałą rywalizacją w cyberprzestrzeni bez otwartego konfliktu zbrojnego. Obie strony angażują się w działania wywiadowcze, dezinformacyjne i sabotażowe, starając się jednocześnie unikać bezpośrednich konfrontacji, które mogłyby prowadzić do eskalacji.

W tym kontekście inicjatywy takie jak dialog cybernetyczny między USA a Rosją, które mają na celu ustanowienie norm i zasad postępowania w cyberprzestrzeni, mogą się przyczynić do ograniczenia ryzyka eskalacji. Skuteczność tych działań zależy jednak od wzajemnego zaufania i gotowości do przestrzegania ustalonych zasad.

Zimna cyberwojna opiera się na logice wzajemnego odstraszania – obie strony tolerują określony poziom cyberszpiegostwa i działań dezinformacyjnych, starając się utrzymać kontrolę nad eskalacją. Rywalizacja toczy się głównie w sferach wywiadu, wpływu i technologii, z przewagą działań poniżej progu prawa międzynarodowego. Ten scenariusz wydaje się obecnie najbardziej realistyczny w krótkiej i średniej perspektywie.

Reset relacji – dyplomacja cyfrowa jako narzędzie stabilizacji

Trzeci scenariusz zakłada możliwość resetu relacji poprzez dyplomację cyfrową, mającą na celu ustanowienie trwałych mechanizmów współpracy i kontroli eskalacji w cyberprzestrzeni. Przykładem takich działań jest zawieszenie ofensywnych operacji cybernetycznych przez USA w celu stworzenia przestrzeni dla negocjacji z Rosją.

Skuteczność dyplomacji cyfrowej jest ograniczają jednak brak zaufania między stronami oraz różnice w postrzeganiu suwerenności cyfrowej i zarządzania internetem. Ponadto działania Rosji w zakresie cyberataków i dezinformacji podważają wiarygodność jej zaangażowania w dialog i współpracę.

Warunkiem realizacji tego scenariusza byłaby zmiana kontekstu politycznego, np. deeskalacja konfliktu w Ukrainie, wypracowanie nowych mechanizmów bezpieczeństwa europejskiego czy presja ze strony aktorów trzecich, jak Chiny czy UE, na stabilizację stosunków. W praktyce reset wydaje się obecnie mało prawdopodobny, ale nie można go wykluczyć w dłuższej perspektywie.

* * *

W ostatnich miesiącach dało się zauważyć, że NATO intensyfikuje działania w zakresie obrony cybernetycznej, uznając cyberprzestrzeń za domenę operacyjną i rozwijając zdolności do przeciwdziałania zagrożeniom[32].

Mniej aktywna w sferze cyberbezpieczeństwa OUBZ może z kolei stanowić platformę dla Rosji, pozwalając koordynować działania z państwami członkowskimi. Na równowagę sił wpływa również współpraca Moskwy z Pekinem w zakresie technologii i cyberbezpieczeństwa, tworząc alternatywne bloki wpływów w cyberprzestrzeni.

Unia Europejska, jako aktor trzeci, dąży do wzmocnienia swojej odporności na cyberzagrożenia poprzez rozwój wspólnej polityki cyberbezpieczeństwa i współpracę z partnerami międzynarodowymi. Jej działania mają na celu nie tylko ochronę własnych systemów, ale także promowanie norm i standardów w cyberprzestrzeni.

Uwzględnienie roli aktorów trzecich pokazuje, że scenariusze relacji amerykańsko-rosyjskich w cyberprzestrzeni nie rozgrywają się w próżni i są kształtowane przez szerszy układ sił globalnych. NATO i UE wzmacniają ramy obrony zbiorowej, OUBZ i współpraca rosyjsko-chińska mogą konsolidować alternatywny blok, a rosnąca presja normatywna ze strony organizacji międzynarodowych, jak ONZ, OEWG czy GGE, tworzy dodatkowe ramy, nawet jeśli ich skuteczność pozostaje ograniczona.

Podsumowanie

Cyberprzestrzeń jako nieodłączny element współczesnych stosunków międzynarodowych staje się kluczową domeną rywalizacji strategicznej pomiędzy państwami. Dynamiczny rozwój technologii informacyjno-komu-

32 G. Van Epps, *Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain*, „Connections The Quarterly Journal" 2013, vol. 12, No. 4, s. 15–50.

nikacyjnych sprawił, że przestrzeń ta przestała być jedynie narzędziem wspomagającym funkcjonowanie państw i społeczeństw, a stała się pełnoprawnym polem prowadzenia polityki zagranicznej – zarówno w wymiarze współpracy, jak i konfrontacji.

Historycznie relacje amerykańsko-rosyjskie w obszarze cyberprzestrzeni osadzone są w szerszym kontekście zimnowojennej rywalizacji, której spuścizną są struktury sieciowe tworzone w celach strategicznych. Przemiany ustrojowe po 1991 r. nie zniosły napięcia geopolitycznego, a cyberprzestrzeń stopniowo przekształciła się w nową arenę konfrontacji. Obie strony – zarówno Federacja Rosyjska, jak i Stany Zjednoczone – uczyniły z cyberbezpieczeństwa jeden z kluczowych komponentów swoich doktryn bezpieczeństwa narodowego.

Federacja Rosyjska postrzega przedmiotową domenę jako obszar operacyjny, który umożliwia asymetryczne oddziaływanie na przeciwnika. Kluczową rolę odgrywa tu koncepcja informacyjnego przeciwstawiania się, obejmująca zarówno środki techniczne (cyberataki czy sabotaż infrastruktury krytycznej), jak i psychologiczne (operacje wpływu i dezinformację). Państwo to aktywnie rozwija swoje zdolności w zakresie cyberszpiegostwa, prowadzenia wojen hybrydowych i zakłócania funkcjonowania instytucji demokratycznych w państwach zachodnich.

Analogicznie Stany Zjednoczone wypracowały ofensywną strategię *persistent engagement* i *defend forward*, która zakłada neutralizację zagrożeń w cyberprzestrzeni jeszcze poza własnym terytorium. Amerykańska polityka cyberobronna integruje środki wojskowe, wywiadowcze i dyplomatyczne, a jej celem jest nie tylko ochrona interesów narodowych, lecz również kształtowanie globalnego ładu poprzez rozwój norm i sojuszy w zakresie cyberbezpieczeństwa.

Wysoce istotnym wymiarem rywalizacji cybernetycznej są operacje wpływu i dezinformacja. Przypadki ingerowania Rosji w wybory prezydenckie w USA w latach 2016 i 2020 dowodzą skuteczności tego typu działań oraz ich potencjału destabilizującego. Zaawansowane kampanie informacyjne oparte na rozbudowanych sieciach fałszywych tożsamości i zautomatyzowanych źródeł treści przyczyniają się do erozji zaufania społecznego, pogłębiania podziałów i utrudniania konsolidacji instytucji demokratycznych.

Celem ataków cybernetycznych pozostaje infrastruktura krytyczna – sektory energetyczny, transportowy i zdrowotny. Zakłócenia w tych obszarach mogą prowadzić do realnych strat ekonomicznych i społecznych,

a także paraliżować funkcjonowanie państwa. Zdolności do obrony i redundancji infrastruktury stanowią dziś zatem istotny komponent suwerenności cyfrowej państw.

W obliczu eskalujących napięć między USA a Rosją można wyróżnić trzy potencjalne scenariusze rozwoju sytuacji: eskalację konfliktu z dalszym rozwojem ofensywnych zdolności cybernetycznych, utrwalenie stanu zimnej cyberwojny z zachowaniem zasad wzajemnego odstraszania oraz próbę resetu relacji poprzez dyplomację cyfrową. Każdy z tych wariantów obarczony jest ryzykiem i zależy od szeregu czynników, w tym gotowości do budowania mechanizmów zaufania i przestrzegania norm międzynarodowych.

Bibliografia

Bowcut S., *Digital Safeguards: Navigating Cybersecurity in Transportation*, „Cybersecurity Guide" [online], 3 IV 2025 [dostęp: 7 IV 2025]: <https://cybersecurityguide.org/industries/transportation/>.

Bryjka F., *Grupa Wagnera – paramilitarne narzędzie rosyjskich operacji hybrydowych*, „Sprawy Międzynarodowe" 2022, t. 75, nr 2.

Bryjka F., Chłoń T., Kupiecki R., *Dezinformacja międzynarodowa. Pojęcie, rozpoznanie, przeciwdziałanie*, Wydawnictwo Naukowe „Scholar", Warszawa 2022.

Cohen-Almagor R., *Internet History*, „International Journal of Technoethics" 2011, vol. 2, No. 2.

Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, red. M. Górka, Difin, Warszawa 2014.

Galbreath J., *The Internet: Past, Present, and Future*, „Educational Technology" 1997, vol. 37, No. 6.

Greenberg A., *Foreign Meddling Flooded the 2020 Election – but Not by Hackers*, „Wired" [online], 16 III 2021 [dostęp: 5 IV 2025]: <https://www.wired.com/story/odni-russia-iran-2020-election-interference/>.

Hogeveen B., *The UN Norms of Responsible State Behaviour in Cyberspace. Guidance on Implementation for Member States of ASEAN*, Australian Strategic Policy Institute, [b.m.w.] March 2022.

Hoyle A., Šlerka J., *Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns*, Hybrid CoE, [b.m.w.] March 2024 (Hybrid CoE Working Paper, 29).

Jones S., *Pedro Sánchez Vows to Find the Cause of Huge Power Cut in Spain and Portugal*, „The Guardian" [online], 29 IV 2025 [dostęp: 30 IV 2025]: <https://www.theguardian.com/world/2025/apr/29/spain-portugal-returning-normal-experts-cause-blackout>.

Judah J., Hamilton F., *Russia Using AI to Target Britons with Flood of Fake News*, „The Times" [online], 29 IV 2025 [dostęp: 5 IV 2025]: <https://www.thetimes.com/uk/defence/article/russia-ai-disinformation-pravda-fake-news-plbwwn7v0>.

Kane B. R., Webber S., Tucker K. H., Wallace S., Chang J., McCarthy D., Murphy D., Egel D., Wingfield T., *Defending the United States against Critical Infrastructure Attacks. Exploring a Hypothetical Campaign of Cascading Impacts*, RAND Corporation, [b.m.w.] 2024 (Inverted Rook Research Report).

Kroustek J., *WannaCry Ransomware That Infected Telefonica and NHS Hospitals Is Spreading Aggressively, with over 50,000 Attacks so far Today*, „Avast" [online], 12 V 2017 [dostęp: 7 IV 2025]: <https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000--attacks-so-far-today>.

Lily B., Cheravitch J., *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, [w:] *2020 12th International Conference on Cyber Conflict*, ed. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2020.

Meller R. S., III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, vol. 1, U.S. Department of Justice, Washington, March 2019.

The National Cybersecurity Strategy, „The White House" [online], March 2023 [dostęp: 3 IV 2025] <https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/>.

Nowakowski Z., Protasowicki I., *Bezpieczeństwo informacyjne a cyber terroryzm*, „Zeszyty Naukowe WSIZiA" 2009, nr 1 (9).

Nowakowski Z., Szafran H., Szafran R., *Bezpieczeństwo w XXI wieku. Strategie bezpieczeństwa narodowego Polski i wybranych państw*, Fundacja Niepodległości, Rzeszów 2009.

Packard N., *Internet Prehistory: ARPANET Chronology*, „Cogent Social Sciences" 2023, vol. 9, issue 2.

Pudełko M., *Prawdziwa historia internetu na świecie*, wyd. 4, IT Start, Piekary Śląskie 2020.

Smeets M., *U.S. Cyber Strategy of President Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection*, „Intelligence and National Security" 2020, vol. 35, No. 3.

Sułek M., *Prakseologiczna teoria stosunków międzynarodowych*, „Przegląd Strategiczny" 2012, nr 1.

Sułek M., *Trzy działy prakseologii*, „Rocznik Naukowy Wydziału Zarządzania w Ciechanowie" 2008, t. 2, z. 1–2.

Targowski A., *From the Cold War to Internet Cathedral*, „International Journal of Information and Communication Technology Education" 2005, vol. 1, issue 2.

[Twenty-twenty] 2020 12th International Conference on Cyber Conflict, ed. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2020.

Ukaz Prezidenta Rossijskoj Federacii ot 02.07.2021 g. № 400 „O Strategii nacional'noj bezopasnosti Rossijskoj Federacii", „Konsul'tant plûs" [online, dostęp: 16 II 2025]: <https://www.consultant.ru/document/cons_doc_LAW_389271/>.

US Invokes Emergency Powers after Cyber-Attack on Fuel Pipeline, „The Guardian" [online], 10 V 2021 [dostęp: 7 IV 2025]: <https://www.theguardian.com/us-news/2021/may/10/us-invokes-emergency-powers-after-cyberattack-shuts-crucial-fuel-pipeline>.

Van Epps G., *Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain*, „Connections The Quarterly Journal" 2013, vol. 12, No. 4.

Wang T., Wang Zh., Zhang Zh., Liao W., Ji J., *SORM-Enhanced Inverse Reliability Analysis for Geotechnical Multiobjective Reliability-Based Design Optimization*, „International Journal for Numerical and Analytical Methods in Geomechanics" 2025, vol. 49, issue 1.

Xu M., Lu Ch., *China–U.S. Cyber-Crisis Management*, „China International Strategy Review" 2021, vol. 3, issue 1: <https://pmc.ncbi.nlm.nih.gov/articles/PMC8237537/pdf/42533> [dostęp: 10 IV 2025].

Zhukov D., *The Phone-a-Friend Option: Use Cases for a U.S.-U. K.-French Crisis Communication Channel*, Institute for Security and Technology, [b.m.w.] June 2024: <https://securityandtechnology.org/wp-content/uploads/2024/10/CATALINK-P3.pdf> [dostęp: 16 II 2025].