DOI:10.17951/we.2025.11.1.11-20 | Wschód Europy • Восток Европы • East of Europe, vol. 11, 1 / 2025

Patryk Wosik
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
ORCID ID: https://orcid.org/0009-0004-9027-1425
e-mail: patrykpolitologia@wp.pl

Obrona przed niewidzialnymi wrogami: Polska w obliczu rosyjskich działań hybrydowych

1. Wstęp

Przyglądając się obecnej sytuacji politycznej na świecie, dostrzec możemy próbę zmiany ładu międzynarodowego. Obecny porządek hegemoniczny, w którym dotychczas rolę supermocarstwa sprawowały Stany Zjednoczone, ulega osłabieniu na rzecz ładu wielobiegunowego. Napaść zbrojna Federacji Rosyjskiej na Ukrainę, wojna handlowa między USA a Chinami, zainicjowana przez Donalda Trumpa, oraz kryzys wokół Tajwanu skłaniają do refleksji na temat bezpieczeństwa i potencjalnej wojny światowej. Odporność Rosji na sankcje i przestawienie gospodarki na tory wojenne skutkują coraz większą przewagą Putina i pogarszającą się sytuacją militarną na Ukrainie. Obecna napaść Federacji Rosyjskiej na Ukrainę ukazuje, że w przypadku konfliktu zbrojnego najważniejszym czynnikiem nie są wykresy dotyczące PKB, a zdolność do produkcji przemysłu zbrojeniowego. W czasach, gdy Donald Trump podczas jednego ze spotkań w kampanii wyborczej przed wyborami prezydenckimi w USA podważył fundamenty Paktu Północnoatlantyckiego, czyli Artykuł 5, społeczeństwo polskie musi być świadome realnego zagrożenia konfliktem zbrojnym z Federacją Rosyjską. W istocie, Vladimir Putin już prowadzi wojnę hybrydową przeciwko Polsce. Aby móc jej przeciwdziałać, społeczeństwo musi mieć jej świadomość, znać istotę oraz cel.

2. Zagrożenia hybrydowe

Chociaż nie istnieje jednoznaczna definicja działań hybrydowych, są to konflikty, w których jedna strona wykorzystuje zarówno metody konwencjonalne, jak i niekonwencjonalne, takie jak cyberataki, propagandę czy terroryzm, w celu osiągnięcia swoich celów. Możliwości realizacji działań hybrydowych wykazują się znacznym stopniem elastyczności i zróżnicowania. Obejmują one szeroki zakres obszarów, takich jak przestrzeń polityczna, dyplomatyczna, dezinformacyjno-propagandowa, gospodarcza, kulturalna,

społeczna oraz humanitarna. Charakteryzują się one nieustannymi zmianami, co pokazuje ich różnorodną strukturę[1].

Konflikty hybrydowe, według polskiego historyka Jacka Regina-Zacharskiego, to działania prowadzone na marginesie lub poza bezpośrednimi zagrożeniami dla państwa. Niemniej jednak, ich wpływ może generować długofalowe skutki, zwłaszcza dla państw demokratycznych, gdzie społeczeństwo odgrywa kluczową rolę w procesie wyborczym. Poprzez manipulację percepcją obywateli danego kraju możliwe jest wywieranie wpływu na struktury władzy i decyzje polityczne[2].

W latach 60. XX wieku pułkownik armii białej Rosji Jewgienij Messner stworzył pojęcie „wojen buntowniczych", które charakteryzowały się tożsamymi cechami z obecnymi wojnami hybrydowymi. Według Messnera, wojny buntownicze ukazywały się stanem rozmycia między pokojem a wojną, a celem ich było powodowanie poczucia chaosu, pogarszanie nastrojów społecznych i przeciągnie wrogiego społeczeństwa na swoją stronę[3].

Aby omówić koncepcję wojny hybrydowej, warto odwołać się do wypowiedzi Szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej, Walerego Gierasimowa. Gierasimow, analizując charakter wojen przyszłości, podkreśla wzrost znaczenia działań niemilitarnych, takich jak działania polityczne, ekonomiczne czy humanitarne, które są wspierane propagandą. Rosyjski wojskowy zwraca uwagę na zacieranie granic między różnymi poziomami działań wojennych oraz na łączenie środków militarnych z niemilitarnymi. Mimo że Gierasimow w swojej doktrynie nie używa bezpośrednio terminu „wojna hybrydowa", to opisując nowoczesne wojny, ukazuje istotę hybrydyzacji ekspansywnej polityki Rosji[4].

Współczesne konflikty zbrojne są nieodłącznie związane z zjawiskiem globalizacji, które sprawia, że państwa, firmy oraz jednostki ludzkie są coraz bardziej wzajemnie zależne na skalę światową. W ramach konfliktów międzypaństwowych, istotną rolę odgrywają współczesne media, które relacjonują przebieg wojen na żywo dla publiczności z różnych zakątków globu. Sposób, w jaki konflikty są przedstawiane, wpływa istotnie na opinie społeczną, która może wywierać presję na władze swojego państwa. W tym kontekście Federacja Rosyjska często podejmuje działania, które starannie maskuje jako legalne, pomimo znacznego sprzeciwu społeczności międzynarodowej. Wykorzystuje nieoznakowane jednostki wojskowe oraz wspiera lokalne struktury pa-

[1] Najwyższa Izba Kontroli, Hybrydowe zagrożenie (zapis konferencji prasowej) – https://www.nik.gov.pl/aktualnosci/dzialania-hybrydowe-zagrozenia.html?fbclid=IwAR1b_9pqFSyc6r3nGKn7rkt_iKmJ_x-nqWpu-Eri_NUa9sFnLNJatpZAr9s [dostęp: 1.03.2024].

[2] J. Regina-Zacharski, *Wojna w świecie współczesnym. Uczestnicy – cele – modele – teorie*, Łódź 2014, s. 320–321.

[3] P. Ochmann, J. Wojas, *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego" 2018, nr 2, s. 108.

[4] A. Gorzkowicz, *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1, s. 147.

ramilitarne. Vladimir Putin określił napaść zbrojną na Ukrainę jako „interwencję", co ma na celu nadać działaniom Rosji pozory legitymacji na arenie międzynarodowej[5].

Strategia działań hybrydowych opiera się na wykorzystaniu i podsycaniu wrażliwych tematów w celu destabilizacji społeczeństwa potencjalnego wroga. Zagrożenia te koncentrują się na słabościach przeciwnika, które wynikają z czynników takich jak historia, różnice ideologiczne czy uwarunkowania geostrategiczne. Rosjanie celowo wywołują wrażliwe tematy, takie jak zbrodnia wołyńska, aby pogorszyć relacje polsko-ukraińskie. Podszywają się za ukraińską społeczność w sieci, publikując kontrowersyjne treści na polskich forach, co ma na celu wywołanie negatywnych nastrojów społecznych wobec wsparcia Ukrainy.

3. Praktyka zagrożeń hybrydowych: rosyjskie działania przeciwko Polsce

Rosjanie od wielu lat angażują się w szereg działań hybrydowych, które mają na celu destabilizację Polski. Pierwszym z tych elementów jest dezinformacja, czyli świadome rozpowszechnianie fałszywych lub zmanipulowanych informacji. Rosjanie, dążąc do osiągnięcia polaryzacji społeczeństwa wroga, starają się wywołać podziały w państwie, prowadząc działania mające na celu podział społeczeństwa na dwa przeciwstawne obozy. Przykładem może być pandemia COVID-19, w której Rosja wykorzystywała propagandę zarówno z jednej, jak i drugiej strony, kreując narrację, która negowała istnienie pandemii, szerząc różne teorie spiskowe, takie jak „fake plandemia", oraz nawołując do bojkotu restrykcji sanitarnych. Jednocześnie prowadzili przeciwstawny przekaz sugerując, że powinno się zabierać prawa obywatelskie osobom, które nie chcą się zaszczepić. Działania te skutecznie powodowały destabilizację w państwie, tworząc atmosferę nieufności, podziałów społecznych i dezorientacji wśród obywateli. Rozpowszechnianie sprzecznych narracji i fałszywych informacji wpłynęło na pogorszenie relacji społecznych oraz zaognienie konfliktów światopoglądowych i politycznych[6].

Cyklicznym przykładem działań hybrydowych jest stosowanie dezinformacji w sieci po agresji Rosji na Ukrainę. Polskie media społecznościowe były zalewane fałszywymi informacjami dotyczącymi sytuacji na froncie. Udostępniano nagrania wojenne z przeszłości, podając je za aktualne walki na Ukrainie, co efektywnie prowadziło do dezorientacji i zamętu wśród odbiorców. W momencie wybuchu napaści zbrojnej, znaczny odsetek mężczyzn pochodzenia ukraińskiego, którzy pracowali w Polsce, zdecydował się powrócić do swojej ojczyzny w celu obrony jej. W tym samym czasie Rosjanie rozpoczęli szerzenie dezinformacji, twierdząc, że ukraińscy mężczyźni spędzają czas w polskich galeriach handlowych, siłowniach oraz starają się uwodzić polskie kobiety. W analogicznej sytuacji, kiedy do Polski przybyły ukraińskie kobiety i dzieci z powo-

[5] M. Pietraś, *Wojna hybrydowa Rosji na wschodzie Ukrainy w kontekście współczesnych stosunków międzynarodowych*, [w]: *Wojna hybrydowa Rosji przeciwko Ukrainie w latach 2014–2016*, red. W. Baluk, M. Doroszko, Lublin 2017, s. 27.

[6] P. Śledź, *Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19*, „Rocznik Strategiczny" 2020, nr 2, s. 391.

du ucieczki przed wojną, Rosjanie zainicjowali propagację informacji sugerujących, że „ukraińskie dzieci cieszą się przywilejami i posiadają większe uprawnienia w polskich placówkach edukacyjnych", a także, że „Polacy muszą oczekiwać dłużej w kolejkach do lekarzy". Celowość tych działań polegała na pogorszeniu relacji polsko-ukraińskich oraz na osłabieniu wsparcia i solidarności udzielanej Ukrainie. Dodatkowo, warto podkreślić, że postęp technologiczny dostarcza nowych narzędzi propagandowych. Sztuczna inteligencja (SI) wykazuje zdolność do generowania fałszywych treści informacyjnych poprzez analizę danych dotyczących preferencji, zachowań i poglądów społeczeństwa, co umożliwia ich skuteczne wykorzystanie w celach dezinformacji[7].

Kolejnym narzędziem hybrydowym Federacji Rosyjskiej jest oddziaływanie środkami prawnymi, co można było zaobserwować podczas kryzysu migracyjnego na granicy Białorusi z Unią Europejską poprzez stymulowanie nielegalnej migracji. Wojska rosyjskie i białoruskie transportowały migrantów z Bliskiego Wschodu w kierunku granicy Polski, wyznaczając szlaki nielegalnego przekroczenia. Ponadto te działania zostały połączone z dezinformacją, gdzie Rosjanie generowali propagandowe hasła, takie jak „stop islamizacji", oraz rozpowszechniali fałszywe informacje o przestępstwach popełnionych przez uchodźców już na terenie Polski. Z drugiej strony prowadzili narrację opartą na prawie międzynarodowym i potrzebie udzielenia pomocy uchodźcom, co w rzeczywistości było wykorzystywane przez Rosję do celów politycznych. Te działania skutkowały wzrostem napięć społecznych, prowadząc do konfliktów i radykalizacji poglądów oraz postaw jednostek. W kraju narodził się zatem znaczący spór ideologiczny, a społeczeństwo zaczęło się dzielić, nie zastanawiając się głęboko, kto stoi za całościowym kryzysem emigracyjnym i jakie cele są z nim związane.

W roku 2023 zainicjowano działania propagandowe bezpośrednio na terenie Polski. W dużych miastach zaczęły pojawiać się naklejki promujące Grupę Wagnera, czyli prywatną jednostkę wojskową związaną z rosyjskim wywiadem, działającą na rzecz Federacji Rosyjskiej. Na naklejkach umieszczony był kod QR, przekierowujący do formularza dołączenia do międzynarodowej organizacji przestępczej, z widocznym hasłem „jesteśmy tutaj". Celem tych działań było wywołanie wrażenia, że rosyjscy napastnicy operują na terenie Polski, mając na celu zastraszenie społeczeństwa polskiego.

W tym samym roku, miała miejsce seria incydentów naruszających integralność terytorialną Polski. Zaobserwowano dwa białoruskie helikoptery, które nielegalnie wtargnęły w przestrzeń powietrzną Polski. Ten incydent był oceniany jako prowokacyjny, mający na celu wywołanie w polskim społeczeństwie poczucia niepokoju i zagrożenia. 14 listopada w miejscowości Przewodów w województwie lubelskim doszło do uderzenia dwóch rakiet, które spowodowały śmierć dwóch osób. Trudność w analizie tego zdarzenia wynika z złożoności sytuacji, gdyż pojawiły się sugestie, że w Przewodowie spadły ukraińskie pociski obrony powietrznej. Podobny incydent miał miejsce 16 grudnia, kiedy to rosyjska rakieta spadła w okolicy Bydgoszczy. Te wydarzenia wywołały szeroką dyskusję na temat kompe-

[7] A. Majchrzak, *Rosyjska dezinformacja i wykorzystanie obrazów generowanych przez sztuczną inteligencję (deepfake) w pierwszym roku inwazji na Ukrainę*, „Media Biznes Kultura" 2023, nr 14, s. 76–78.

tencji i stanu wojska polskiego. W takich sytuacjach kryzysowych kluczowe jest, aby władze państwowe oraz odpowiednie instytucje transparentnie i szybko informowały społeczeństwo o zaistniałych wydarzeniach, w celu zapobieżenia rozprzestrzenianiu się paniki.

Następnym instrumentem wojny hybrydowej są ataki kinetyczne, inaczej dywersyjne, które wymierzone są w infrastrukturę strategiczną. W Polsce systematycznie dokonuje się aresztowań osób podejrzanych o prowadzenie działań szpiegowskich na rzecz Rosji. 31 stycznia 2024 roku funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego zatrzymali obywatela Ukrainy, który planował przeprowadzenie działań dywersyjnych, polegających na podpaleniu obiektów znajdujących się blisko infrastruktury strategicznej. Mężczyzna działał na zlecenie rosyjskich służb wywiadowczych.

W marcu 2024 roku trzy balony meteorologiczne opadły na obszarze Polski, miały one napisy w alfabecie cyrylicy, wskazujące na ich rosyjskie pochodzenie. Prawdopodobnie przemieszczały się z obwodu królewieckiego, który graniczy z Polską od północy. Rosjanie wykorzystali te balony jako narzędzie do przetestowania reakcji polskich sił obrony przeciwlotniczej. Generał Waldemar Skrzypczak, były dowódca Wojsk Lądowych, zauważył, że taka akcja wprowadza niepokój i chaos w Polsce, podkreślając, że stanowi to jedno z narzędzi wojny hybrydowej. Wskazuje to na rosnącą złożoność strategii hybrydowej stosowanej przez Rosję, gdzie używane są różnorodne instrumenty do osiągnięcia celów destabilizacyjnych[8].

W erze dynamicznego postępu technologicznego ataki cybernetyczne stają się potężnym narzędziem w wojny hybrydowej. Polska znajduje się na celowniku cyberprzestępców z Rosji. Z analizy raportu Microsoft Digital Defense wynika, że 36% rosyjskich ataków cybernetycznych skierowanych jest głównie przeciwko Stanom Zjednoczonym, Wielkiej Brytanii i Polsce. Badania wskazują, że każda organizacja, postać polityczna lub rząd wspierający Ukrainę lub wyrażający treści proukraińskie jest narażony na potencjalny atak hakerski[9].

W celach związanych z cyberprzestępczością Rosjanie systematycznie wykorzystują technikę phishingu, która polega na podszywaniu się pod instytucje lub osoby w celu zainfekowania komputera ofiary szkodliwym oprogramowaniem w celu wyłudzenia informacji. Przykładowo, podczas kampanii wyborczej w Stanach Zjednoczonych w 2016 roku, szef kampanii Hillary Clinton, John Podesta, stał się ofiarą tego rodzaju ataku. Nieświadomie kliknął złośliwy link zawarty w e-mailu, który wyglądem przypominał autentyczną wiadomość generowaną przez serwis Google. Następnie otworzył fałszywą stronę, stworzoną przez grupę hakerów, imitującą oficjalną witrynę Google, gdzie podał swoje poprawne dane logowania. Choć nadawcą wydawał się być system Google, to w rzeczywistości był to produkt działalności grupy hakerów phishingowych, którą później rząd USA powiązał z Rosją. W wyniku tego incydentu portal WikiLeaks opu-

[8] *Balony z napisami cyrylicą nad Polską* – https://www.rp.pl/konflikty-zbrojne/art39956821-balon-z-napisami-cyrylica-nad-polska-gen-waldemar-skrzypczak-nie-ma-sie-czym-przejmowac [dostęp: 11.03.2024].

[9] Raport Microsoft Digital Defense – https://news.microsoft.com/pl-pl/2023/10/09/raport-microsoft-digital-defense-84-wszystkich-cyberatakow-z-rosji-jest-wymierzonych-w-ukraine-lub-czlonkow-nato/ [dostęp: 10.03.2024].

blikował tysiące prywatnych e-maili niekorzystnych dla Demokratów, co wpłynęło na ostateczne wyniki wyborów[10]. Niezwykle istotne jest posiadanie świadomości dotyczącej zagrożeń związanych z atakami phishingowymi oraz dokładne sprawdzanie źródeł e-maili i wiadomości, zwłaszcza w przypadku pełnienia ważnej roli w strukturach państwowych oraz posiadania wrażliwych danych. Urzędnicy państwowi i politycy powinni być poddawani odpowiednim szkoleniom w tej dziedzinie.

Z analizy przeprowadzonej przez badaczy BlackBerry wynika, że obserwuje się wzrost liczby ataków cybernetycznych przeprowadzanych przez hakerów wspieranych przez państwo Rosyjskie. Raport przytacza liczne przykłady ataków na Polskę, w tym atak na stronę polskiego urzędu skarbowego przeprowadzony przez prorosyjską grupę hakerską o nazwie NoName057[11]. W Polsce atakowane są różne instytucje, począwszy od dziedziny medycznej po strony rządowe i instytucje bankowe. Ataki te często wykorzystują technikę DDoS (rozproszona odmowa usługi), gdzie osoby odpowiedzialne za nadużycia zalewają witrynę fałszywym ruchem, co skutkuje paraliżem strony i jej wyłączeniem. Taka agresja ma zdolność paraliżowania funkcjonowania państwa. W listopadzie 2023 roku doszło do skradzenia 44,5 gigabajtów danych z ogólnopolskiej sieci laboratoriów diagnostycznych (ALAB) przez cyberprzestępców. Dane obejmują wyniki badań, a także 187 tysięcy numerów PESEL i informacji dotyczących miejsc zamieszkania pacjentów. Wśród tych informacji znajdują się wrażliwe dane związane ze stanem zdrowia badanych. Tego rodzaju ataki na systemy medyczne mają poważne konsekwencje w aspekcie naruszenia prywatności i bezpieczeństwa. Kradzież danych osobowych, zwłaszcza takich jak numery PESEL, niesie za sobą ryzyko nadużycia tych informacji, co może prowadzić do różnych form przestępstw, takich jak kradzież tożsamości czy oszustwa finansowe. W kontekście zagrożeń hybrydowych naruszenie bezpieczeństwa danych w sektorze medycznym może wpłynąć na zaufanie społeczeństwa do instytucji zdrowotnych oraz osłabić system opieki zdrowotnej.

Aktualnie w Polsce odnotowuje się średnio 3,7 tysiąca ataków hakerskich tygodniowo, skierowanych przeciwko celom strategicznym oraz infrastrukturze. Firma CheckPoint, specjalizująca się w dziedzinie cyberbezpieczeństwa, raportuje, że obiekty, które znajdują się na celowniku hakerów, to przede wszystkim sektor finansowy i banki, gdzie notuje się średnio 1216 ataków tygodniowo, instytucje rządowe, na które przypada 1080 ataków tygodniowo, oraz szpitale, które doświadczają średnio 1699 ataków tygodniowo. Te liczby obrazują skalę zagrożenia, przed jakim stoi Polska w dziedzinie cyberbezpieczeństwa[12].

Jednym z instrumentów wojny hybrydowej prowadzonej przez Rosję jest szantaż nuklearny. Były prezydent Rosji, Dmitrij Miedwiediew, grozi że jeśli Ukraina będzie

[10] Inside story: How Russians hacked the Democrats' emails – https://apnews.com/article/technology-europe-russia-hacking-only-on-ap-dea73efc01594839957c3c9a6c962b8a [dostęp: 10.03.2024].

[11] Więcej cyberataków na rządy i usługi publiczne. Polska popularnym celem – https://cyberdefence24.pl/cyberbezpieczenstwo/wiecej-cyberatakow-na-rzady-i-uslugi-publiczne-polska-popularnym-celem [dostęp: 10.03.2024].

[12] Wojna w internecie: tysiące ataków na Polskę tygodniowo prorosyjskich hakerów – https://www.rp.pl/gospodarka/art38292191-wojna-w-internecie-tysiace-atakow-na-polske-tygodniowo-prorosyjskich-hakerow [dostęp: 10.03.2024].

kontynuować otrzymywanie broni z Europy, nieunikniona będzie konfrontacja nuklearna między Sojuszem Północnoatlantyckim a Rosją. Vladimir Putin wielokrotnie podkreślał gotowość Rosji do ataku nuklearnego. Działania te mają na celu zainstygnowanie strachu i zniechęcenie państw europejskich do udzielenia dalszego wsparcia Ukrainie.

Działania Rosji obejmujące broń jądrową poszerzyły się o nowy obszar, tj. przestrzeń kosmiczną. W roku 2024 Stany Zjednoczone doniosły o planach Rosji dotyczących umieszczenia broni atomowej na orbicie. Zastosowanie atomu miałoby polegać na oślepianiu satelitów, co skutkowałoby zakłóceniami w komunikacji sił zbrojnych oraz w systemie cywilnym GPS. Satelity kosmiczne zapewniają Zachodowi znaczną przewagę w monitorowaniu i komunikacji, co jest widoczne w trakcie konfliktu na Ukrainie. Mimo zapewnień prezydenta Rosji, Władimira Putina, że nie planuje on rozmieszczania broni nuklearnej w kosmosie, media społecznościowe zostały zalewane informacjami o zakłóceniach sieci i niedostępności Internetu w Polsce z powodu działań rosyjskich w kosmosie. Cała sytuacja wywołała dyskusję co do eskalacji postępowania Rosji[13].

4. Zwalczanie zagrożeń hybrydowych

W przeciwdziałaniu zagrożeniom hybrydowym kluczową rolę odgrywa państwo. Rząd dysponuje odpowiednimi instrumentami w postaci struktur wywiadowczych, kontrwywiadowczych oraz rozpoznania wojskowego, które są wspierane przez organy odpowiedzialne za utrzymanie porządku publicznego[14].

Istotą zwalczania zagrożeń hybrydowych jest ujawnianie celowo zmanipulowanych informacji i korygowanie ich w mediach publicznych. Istotne jest, aby władze rządzące regularnie informowały społeczeństwo o działaniach dezinformacyjnych podejmowanych przez Rosję. Edukacja społeczeństwa na temat zagrożeń wynikających z wojny hybrydowej przyczyni się do zwiększenia świadomości społecznej, co może skutkować większą odpornością obywateli na manipulacje z zewnątrz.

Ze względu na dążenia Rosji do ingerowania w relacje międzypaństwowe za pomocą wojny hybrydowej, współpraca międzynarodowa pełni istotną rolę w przeciwdziałaniu tym zagrożeniom. Słabości jednego kraju mogą generować negatywne efekty poza jego granicami. Na przykład atak na osłabiony segment międzynarodowego systemu transportowego może prowadzić do znaczących konsekwencji dla innych państw. Wobec tego od 2016 roku Unia Europejska oraz Organizacja Traktatu Północnoatlantyckiego (NATO) uznają zagrożenia hybrydowe za priorytetowy obszar ich współpracy. W efekcie 11 kwietnia 2017 roku utworzono Europejskie Centrum Doskonałości ds. Zwalczania Zagrożeń Hybrydowych. Jest to niezależne centrum przeznaczone dla praktyków i ekspertów, mające swoją siedzibę w Helsinkach. Według tych instytucji w obli-

[13] Widmo wojny w kosmosie. Jak Rosjanie mogą wykorzystać broń atomową? – https://www.rp.pl/konflikty-zbrojne/art39882411-widmo-wojny-w-kosmosie-jak-rosjanie-moga-wykorzystac-bron-atomowa [dostęp: 11.03.2024].

[14] H. Wyrębek, *Zagrożenia hybrydowe bezpieczeństwa informacyjnego państwa*, „Polityka i Społeczeństwo" 2023, nr 1, s. 325.

czu zagrożeń hybrydowych konieczne jest działanie z wyprzedzeniem, zarówno poprzez czynniki pasywne, jak budowanie odporności na szok i zaskoczenie, jak i aktywne, takie jak przygotowanie do ochrony struktur, które mogą paść ofiarą hybrydowych ataków[15].

Unia Europejska zidentyfikowała 22 obszary działań wobec zagrożeń hybrydowych, począwszy od podnoszenia świadomości do budowy odporności. W skład przedsięwzięcia wchodzi utworzenie unijnej komórki ds. syntezy informacji hybrydowych w celu gromadzenia informacji i danych wywiadowczych od państw członkowskich w celu wspólnego monitorowania zagrożeń. Zwiększenie odporności sektora energetycznego poprzez większą dywersyfikację źródeł i tras energii, wzmocnienie cyberbezpieczeństwa, podejmowanie działań w zakresie bezpieczeństwa transportu międzynarodowego oraz zwalczanie dezinformacji w sieci. Unia Europejska ma za cel zwiększenie zdolności wykrywania zagrożeń hybrydowych[16].

W styczniu 2018 roku Komisja Europejska powołała zaawansowaną grupę ekspertów (High-Level Group of Experts) w celu identyfikacji procesów zwalczania zagrożeń hybrydowych. W marcu tego samego roku opublikowany został specjalny raport, w którym zawarto następujące cele: Zwiększenie transparentności informacji publikowanych online; Promowanie edukacji z zakresu mediów oraz informacji; Wspieranie pozycji użytkowników oraz dziennikarzy w walce przeciwko dezinformacji; Promowanie dalszych badań nad wpływem dezinformacji w Europie oraz stworzenie odpowiednich narzędzi do przeciwdziałania fake newsom. Eksperci podkreślają, że w obliczu tendencji spadku zaufania społeczeństwa do polityków oraz instytucji publicznych w Europie dezinformacja, jako narzędzie hybrydowe Rosji, staje się coraz bardziej groźna. Teksty wygenerowane przez algorytmy sztucznej inteligencji są niemalże nie do odróżnienia od oryginałów. Administracje państwowe nie nadążają za rozwojem technologii i często padają ofiarą działań rosyjskich[17].

W Polsce obserwuje się brak adekwatnych narzędzi i instytucji odpowiedzialnych za prowadzenie skutecznej strategicznej komunikacji, mającej na celu przeciwdziałanie zagrożeniom hybrydowym ze strony Federacji Rosyjskiej. Warto rozważyć możliwość utworzenia specjalnej instytucji, której zadaniem byłoby zwalczanie tego rodzaju działań oraz prowadzenie edukacji społeczeństwa w tym obszarze.

5. Zakończenie

Podsumowując: współczesna sytuacja geopolityczna stawia Polskę w obliczu wyzwań bez precedensu, zwłaszcza w kontekście agresywnej wojny hybrydowej prowadzonej przez Federację Rosyjską. Zagrożenia hybrydowe wywierają nie tylko bezpośredni wpływ na stabilność i bezpieczeństwo państwa, lecz także na społeczeństwo, gospodar-

[15] Współpraca przeciwko zagrożeniom hybrydowym, NATO – https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html [dostęp: 13.03.2024].

[16] A Europe that Protects: Countering Hybrid Threats – https://www.eeas.europa.eu/node/46393_en [dostęp: 14.03.2024].

[17] Unia Europejska versus dezinformacja – syzyfowa praca? – https://pulaski.pl/komentarz-pulaskiego-unia-europejska-versus-dezinformacja-syzyfowa-praca/ [dostęp: 15.03.2024].

kę i struktury instytucjonalne. Jednakże poprzez świadome zrozumienie istoty tych zagrożeń oraz skuteczne podejmowanie działań obronnych i prewencyjnych Polska może przeciwdziałać tym wyzwaniom i budować bardziej odporną i bezpieczną przyszłość. Współpraca z partnerami międzynarodowymi, rozwój zdolności obronnych oraz promowanie świadomości społecznej stanowią kluczowe elementy w budowaniu skutecznej strategii bezpieczeństwa narodowego.

Streszczenie: Współczesna sytuacja geopolityczna stawia Polskę w obliczu potrzeby wszechstronnej refleksji nad jej bezpieczeństwem. Federacja Rosyjska prowadzi strategię wojny hybrydowej przeciwko Polsce, mającą na celu destabilizację oraz oderwanie kraju od zachodnich sojuszy. Aby skutecznie przeciwdziałać tym zagrożeniom, konieczne jest, aby społeczeństwo było świadome ich istoty i celów. W ramach niniejszego artykułu zastosowano metodę analizy dyskursu w celu zbadania treści medialnych pod kątem obecności elementów propagandy i dezinformacji, a także metodę obserwacji, która umożliwiła bezpośrednie monitorowanie i analizę działań hybrydowych oraz ich efektów w czasie rzeczywistym poprzez obserwację zachowań społecznych i politycznych. Niniejszy artykuł podejmuje próbę analizy oraz oceny istoty zagrożeń hybrydowych, które mają wpływ na obniżenie poziomu bezpieczeństwa państwa.
Słowa kluczowe: wojna hybrydowa, zagrożenia hybrydowe, dezinformacja, agresja rosyjska, bezpieczeństwo Polski, fake newsy, propaganda.

Defense Against Invisible Enemies: Poland in the Face of Russian Hybrid Warfare

Summary: The contemporary geopolitical situation poses Poland with the necessity of comprehensive reflection on its security. The Russian Federation employs a strategy of hybrid warfare against Poland, aiming for destabilization and detachment of the country from Western alliances. Effectively countering these threats requires societal awareness of their nature and objectives. This article attempts to analyze and evaluate the essence of hybrid threats impacting the state's security level.
Keywords: hybrid warfare, hybrid threats, disinformation, Russian aggression, Polish security, fake news, propaganda.

Bibliografia

Artykuły, monografie, opracowania

Gorzkowicz A., *Wojna hybrydowa na Ukrainie jako przykład współczesnych konfliktów zbrojnych*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1.

Majchrzak A., *Rosyjska dezinformacja i wykorzystanie obrazów generowanych przez sztuczną inteligencję (deepfake) w pierwszym roku inwazji na Ukrainę*, „Media Biznes Kultura" 2023, nr 14.

Ochmann P., Wojas J., *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego" 2018, nr 2.

Pietraś M., *Wojna hybrydowa Rosji na wschodzie Ukrainy w kontekście współczesnych stosunków międzynarodowych*, [w:] *Wojna hybrydowa Rosji przeciwko Ukrainie w latach 2014–2016*, red. W. Baluk, M. Doroszko, Lublin 2017.

Regina-Zacharski J., *Wojna w świecie współczesnym Uczestnicy – cele – modele – teorie*, Łódź 2014.

Śledź P., *Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19*, „Rocznik Strategiczny" 2020, nr 2.

Wyrębek H., *Zagrożenia hybrydowe bezpieczeństwa informacyjnego państwa*, „Polityka i Społeczeństwo" 2023, nr 1.

Źródła internetowe

A Europe that Protects: Countering Hybrid Threats – https://www.eeas.europa.eu/node/46393_en [dostęp: 14.03.2024].

Balony z napisami cyrylicą nad Polską – https://www.rp.pl/konflikty-zbrojne/art39956821-balon-z-napisami-cyrylica-nad-polska-gen-waldemar-skrzypczak-nie-ma-sie-czym-przejmowac [dostęp: 11.03.2024].

Inside story: How Russians hacked the Democrats' emails – https://apnews.com/article/technology-europe-russia-hacking-only-on-ap-dea73efc01594839957c3c9a6c962b8a [dostęp: 10.03.2024].

Najwyższa Izba Kontroli, Hybrydowe zagrożenie (zapis konferencji prasowej) – https://www.nik.gov.pl/aktualnosci/dzialania-hybrydowe-zagrozenia.html?fbclid=IwAR1b_9pqFSyc6r3nGKn7rkt_iKmJ_x-nqWpu-Eri_NUa9sFnLNJatpZAr9s [dostęp: 1.03.2024].

Raport Microsoft Digital Defense – https://news.microsoft.com/pl-pl/2023/10/09/raport-microsoft-digital-defense-84-wszystkich-cyberatakow-z-rosji-jest-wymierzonych-w-ukraine-lub-czlonkow-nato/ [dostęp: 10.03.2024].

Unia Europejska versus dezinformacja – syzyfowa praca? – https://pulaski.pl/komentarz-pulaskiego-unia-europejska-versus-dezinformacja-syzyfowa-praca/ [dostęp: 15.03.2024].

Widmo wojny w kosmosie. Jak Rosjanie mogą wykorzystać broń atomową? – https://www.rp.pl/konflikty-zbrojne/art39882411-widmo-wojny-w-kosmosie-jak-rosjanie-moga-wykorzystac-bron-atomowa [dostęp: 11.03.2024].

Więcej cyberataków na rządy i usługi publiczne. Polska popularnym celem – https://cyberdefence24.pl/cyberbezpieczenstwo/wiecej-cyberatakow-na-rzady-i-uslugi-publiczne-polska-popularnym-celem [dostęp: 10.03.2024].

Wojna w internecie: tysiące ataków na Polskę tygodniowo prorosyjskich hakerów – https://www.rp.pl/gospodarka/art38292191-wojna-w-internecie-tysiace-atakow-na-polske-tygodniowo-prorosyjskich-hakerow [dostęp: 10.03.2024].

Współpraca przeciwko zagrożeniom hybrydowym, NATO –https://www.nato.int/docu/review/pl/articles/2018/11/23/wspolpraca-przeciwko-zagrozeniom-hybrydowym/index.html [dostęp: 13.03.2024].