Polska wobec ewoluującej wojny hybrydowej

Kinga Kopońka

Termin „wojna hybrydowa" pojawił się w literaturze naukowej w latach 90. XX wieku, głównie w kręgach badawczy krajów anglosaskich. Pierwsze jego użycie miało miejsce w 1995 roku, kiedy Thomas R. Mockaitis zastosował go w swojej publikacji *British Counterinsurgency in the Post-imperial Era*[1]. W rozdziale zatytułowanym *A Hybrid War. The Indonesian Confrontation* autor analizował konfrontację indonezyjską (1950-1966), wskazując na specyficzną naturę tego konfliktu, łączącego tradycyjne operacje wojskowe z nieregularnymi formami walki[2]. W tej interpretacji wojna hybrydowa obejmowała szeroki wachlarz działań (partyzantka, terrorystyczne ataki czy sabotaż) mających na celu destabilizację przeciwnika i realizację celów strategicznych, które nie wymagały wojny konwencjonalnej podjętej na pełną skalę. Dodatkowo, działania te były wspierane przez operacje informacyjne, które miały na celu dalsze osłabienie morale przeciwnika i utrzymanie napięcia w regionie.

W swojej pracy magisterskiej z 2002 roku *Future War and Chechnya. A Case for Hybrid Warfare,* William Nemeth przedstawił wojnę hybrydową jako szczególny sposób prowadzenia działań wojennych, który łączył tradycyjne i nieregularne taktyki z nowoczesnymi metodami informacyjnymi[3]. Jego analiza skupiała się na wojnach czeczeńskich, w których bojownicy czeczeńscy stosowali asymetryczne metody walki przeciwko regularnym jednostkom rosyjskim[4.] Nemeth ukazał analogiczne do obserwacji Mockaitisa współistnienie nieregularnych działań z tradycyjnymi operacjami militarnymi[5]. W kontekście tych działań, wojna hybrydowa nie ograniczała się do konwencjonalnych starć wojskowych.

Nemeth skoncentrował się na analizie wojen czeczeńskich, ale jego badania miały istotny wpływ na przyszłe rozumienie konfliktów zbrojnych, zwłaszcza w kontekście rozwoju pojęcia wojny hybrydowej. Kluczowym elementem jego pracy była prognoza, zgodnie z którą wojny hybrydowe staną się jednym z głównych wyzwań bezpieczeństwa międzynarodowego w XXI wieku, szczególnie dla państw zachodnich. Przewidywał, że połączenie tradycyjnych działań militarnych z nieregularnymi formami walki, będą jednym z najistotniejszych zagrożeń. W

[1] T. R. Mockaitis, *British Counterinsurgency in the Post-imperial Era*, Manchester University Press, Manchster 1995.
[2] Tamże, s. 14.
[3] W. J. Nemeth, Future *War and Chechnya: A Case for Hybrid Warfare*, California: Naval Postgraduate School, Monterey, 2002
[4] Tamże, s. 34.
[5] Tamże, s. 57.

późniejszych latach okazało się, że doświadczenia z wojen czeczeńskich miały wpływ na współczesne działania wojenne, zwłaszcza w Rosji, gdzie elementy wojny hybrydowej zostały zaadaptowane w innych konfliktach[6]. Nemeth podkreślał również, że wojny hybrydowe stanowią zapowiedź nowych rodzajów konfliktów, które w dobie globalizacji i zaawansowanej technologii będą stawały się coraz bardziej powszechne.

W późniejszych latach podejścia do terminu wojny hybrydowej zaczęły się zmieniać w zależności od kontekstu geopolitycznego i ewolucji metod prowadzenia działań wojennych. Choć pierwotne analizy, koncentrowały się na połączeniu tradycyjnych i nieregularnych form walki, w kolejnych dekadach pojawiły się nowe aspekty, które rozwinęły i zaktualizowały wcześniejsze teorie. Zjawisko to zaczęło być postrzegane jako wielowymiarowe i dynamiczne, obejmujące nie tylko działania o militarnym charakterze, ale również intensywne wykorzystywanie technologii informacyjnych, cyberataków oraz operacji psychologicznych, kluczowych w konflikcie XXI wieku.

W rozwoju koncepcji wojny hybrydowej ogromną rolę odegrała publikacja Franka Hoffmana z 2007 roku *Conflict in the 21st Century. The Rise of Hybrid Wars*, będąca istotnym punktem zwrotnym. Hoffman zaznaczył, że wojny hybrydowe nie ograniczają się jedynie do łączenia tradycyjnych operacji wojskowych z nieregularnymi formami walki, lecz obejmują także szereg działań niekonwencjonalnych, w tym cyberataki oraz manipulacje informacyjne. Takie metody prowadzenia wojny mają zdolność do głębokiej destabilizacji państw i społeczeństw, często bez konieczności angażowania regularnych sił zbrojnych czy prowadzenia konfliktów zbrojnych na pełną skalę. Analiza Hoffmana poszerzyła rozumienie wojny hybrydowej, uwzględniając różnorodne podmioty (od państw, przez organizacje terrorystyczne, aż po grupy nieregularne), które mogą wykorzystywać te metody w realizacji swoich celów politycznych, strategicznych i militarnych[7] oraz nadała konfliktom bardziej złożony, wieloaspektowy charakter, co miało dalekosiężne konsekwencje zarówno dla teorii wojskowej, jak i dla analiz politycznych. upływem czasu, termin wojny hybrydowej został znacznie rozszerzony, obejmując szeroką gamę narzędzi i metod, które służą nie tylko destabilizacji militarnej, lecz także politycznej i społecznej. W rezultacie wojna hybrydowa przekształciła się w zjawisko, które wymaga opracowania nowych teorii oraz podejść do analizy współczesnych konfliktów zbrojnych.

---

[6] M. Banasik, *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej*, „Kwartalnik Bellona" 2016 685(2), s. 47-62.

[7] F. Hoffman, *Conflict in the 21st Century. The Rise of Hybrid Wars*, D.C.: Potomac Books, Washington 2007, s. 28.

W kolejnych latach koncepcja była rozwijana przez licznych ekspertów zajmujących się bezpieczeństwem międzynarodowym. Badania Philipa Karbera, Andreasa Kriegera oraz Andreja Manoilo wskazują na jej dalszą ewolucję, obejmującą elementy wojny gospodarczej, technologicznej oraz psychologicznej.

Jednym z kluczowych elementów współczesnej strategii wojskowej Federacji Rosyjskiej jest koncepcja wojny hybrydowej, szeroko omawiana przez generała Walerija Gierasimowa, szefa Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej. Chociaż nie stanowi ona oficjalnie zatwierdzonej doktryny wojskowej, jej założenia wywarły istotny wpływ na sposób prowadzenia konfliktów przez Rosję. Gierasimow przedstawił swoje tezy w artykule opublikowanym w lutym 2013 roku *The Value of Science in Prediction* na łamach czasopisma „Wojennyj Wiestnik", w którym zwrócił uwagę na ewolucję charakteru współczesnych konfliktów. Podkreślił on, że granica między stanem wojny a pokoju ulega zatarciu, a działania destabilizacyjne mogą być prowadzone bez formalnego wypowiedzenia wojny.[8]

Współczesna wojna hybrydowa to złożona strategia militarna, łącząca konwencjonalne i niekonwencjonalne środki walki, obejmując operacje militarne, ekonomiczne, cybernetyczne, dezinformacyjne oraz dyplomatyczne. Jej zasadniczym celem jest osiągnięcie strategicznych korzyści poprzez destabilizację przeciwnika, osłabienie jego struktur państwowych oraz manipulowanie opinią publiczną. Istotnym elementem tej strategii jest wykorzystanie nieregularnych formacji wojskowych, najemników i grup separatystycznych do prowadzenia działań bojowych, nieuznawanych formalnie za działania regularnych sił zbrojnych.

Wyrazistym przykładem implementacji strategii wojny hybrydowej przez Federację Rosyjską była aneksja Krymu w 2014 roku, podczas której zastosowano nieregularne formacje wojskowe, określane mianem „zielonych ludzików"[9], charakteryzujące się brakiem oficjalnych oznaczeń państwowych. Ich działania, obejmujące przejęcie kluczowej infrastruktury strategicznej Półwyspu Krymskiego, umożliwiły Rosji dokonanie de facto aneksji terytorium bez konieczności prowadzenia klasycznych działań zbrojnych.

Jednym z fundamentalnych narzędzi współczesnych strategii agresywnych są operacje dezinformacyjne oraz cyberataki, których celem jest osłabienie struktur państwowych oraz manipulowanie opinią publiczną. Federacja Rosyjska wykorzystuje szeroki wachlarz środków, obejmujących zarówno kontrolowane media państwowe, zorganizowane grupy internetowych

---

[8] W. Gierasimow, "The Value of Science in Prediction", Военно-промышленный курьер, 2017.

[9] NATO, *Ukraina: trzy lata później – powód do optymizmu*, NATO, 2017, (dostęp https://www.nato.int/docu/review/pl/articles/2017/03/10/ukraina-trzy-lata-pozniej-powod-do-optymizmu/index.html 07.03.2025 13:14).

agitatorów, jak i zaawansowane operacje psychologiczne prowadzone w mediach społecznościowych. Przykładem skutecznej operacji dezinformacyjnej była kampania propagandowa wymierzona w wybory prezydenckie w Stanach Zjednoczonych w 2016 roku, kiedy to rosyjskie grupy hackerskie, takie jak APT28 (Fancy Bear) i APT29 (Cozy Bear), dokonały ataków na serwery Komitetu Narodowego Partii Demokratycznej [10], wpływając na procesy demokratyczne jednego z najważniejszych światowych mocarstw.

Polska, jako państwo graniczące z Rosją i Białorusią oraz aktywny członek NATO i UE, znajduje się w szczególnym spektrum zainteresowania rosyjskich działań hybrydowych. Dezinformacja stanowi integralny element strategii Kremla, mającej na celu destabilizację wewnętrzną oraz osłabienie pozycji Polski na arenie międzynarodowej. W tym kontekście Rosja dysponuje rozbudowanym aparatem propagandowym, stosującym zaawansowane techniki manipulacji informacyjnej w celu wpływania na społeczne postrzeganie rzeczywistości. Przykładem skuteczności tych działań była kampania dezinformacyjna po katastrofie smoleńskiej w 2010 roku, w której rosyjskie media konsekwentnie rozpowszechniały fałszywe narracje na temat przyczyn tragedii. Celem tych działań było podsycanie napięć wewnętrznych w Polsce oraz wpływanie na jej relacje międzynarodowe. W ramach tej kampanii powielano tezy podważające oficjalne ustalenia dotyczące przyczyn katastrofy, sugerując między innymi udział osób trzecich lub rzekome zamachowe tło wydarzenia. Przekazy te były dystrybuowane zarówno poprzez rosyjskie media państwowe, takie jak RT czy Sputnik, jak i poprzez anonimowe konta w mediach społecznościowych oraz portale internetowe, co wpisywało się w szerszą strategię działań hybrydowych Kremla. Kampania ta miała na celu nie tylko destabilizację wewnętrzną Polski, ale także pogorszenie relacji polsko-zachodnich poprzez sianie wątpliwości wśród sojuszników Polski co do jej stabilności i wiarygodności.

Oprócz dezinformacji i cyberataków, do kluczowych wyzwań należą działania o charakterze ekonomicznym, energetycznym oraz prowokacje militarne w pobliżu granic Polski. Przykładem takich działań są manipulacje dostawami gazu ziemnego przez Gazprom, które doprowadziły do kryzysu energetycznego w Europie w 2021 roku. Ponadto w tym samym roku Rosja i Białoruś zorganizowały sztuczny kryzys migracyjny na granicy z Polską, sprowadzając migrantów z Bliskiego Wschodu i kierując ich na terytorium UE w celu wywołania destabilizacji politycznej oraz wewnętrznych napięć społecznych w krajach unijnych.

[10] R. S. Meller, *Report on the investigation into Russian interference in the 2016 presidential election (Vol. 1 of 2). U.S. Department of Justice,* 2019, (dostęp: https://www.justice.gov/storage/report.pdf 07.03.2025 17:08).

W związku z tym widać, że Polska XXI wieku, stoi w obliczu rosnących zagrożeń, które nie ograniczają się jedynie do tradycyjnych form konfliktów militarnych. Współczesne zagrożenia hybrydowe, takie jak wojny informacyjne, cyberataki, a także presja ekonomiczna i militarna, stanowią poważne wyzwania, wymagające reakcji na poziomie krajowym oraz międzynarodowym. W odpowiedzi na te zagrożenia Polska nie tylko rozwija zdolności obronne i cyberbezpieczeństwo, ale również angażuje się w szereg inicjatyw międzynarodowych, mających na celu przeciwdziałanie zagrożeniom hybrydowym oraz wzmocnienie swojej pozycji strategicznej w regionie Europy Środkowo-Wschodniej.

Pierwszym kluczowym elementem odpowiedzi Polski na współczesne zagrożenia hybrydowe jest wzmocnienie zdolności obronnych. Modernizacja technologiczna, rozwój systemów wczesnego ostrzegania, a także zwiększenie wydatków na obronność są niezbędnymi działaniami mającymi na celu wzmocnienie bezpieczeństwa narodowego. Ważnym krokiem w tym kierunku było utworzenie Wojsk Obrony Cyberprzestrzeni w 2018 roku, które pełnią centralną rolę w przeciwdziałaniu cyberatakom oraz w ochronie krytycznej infrastruktury państwowej. W ramach rozwoju cyberbezpieczeństwa, Polska inwestuje w szkolenie kadr oraz rozwój technologii służących do wykrywania, neutralizowania i zapobiegania zagrożeniom w cyberprzestrzeni.

W 2022 roku rozpoczęto realizację programu „Tarcza Wschód", mającego na celu wzmocnienie obronności na wschodnich granicach kraju. Program zakłada budowę nowych fortyfikacji, infrastruktury obronnej, a także rozwój współpracy z sojusznikami NATO w celu przeciwdziałania potencjalnym agresjom. Rozbudowa infrastruktury obronnej na wschodnich rubieżach Polski stanowi element długofalowej strategii obronnej, mającej na celu nie tylko zminimalizowanie ryzyka militarnych działań w tym regionie, ale także wzmocnienie poczucia bezpieczeństwa wśród obywateli oraz sojuszników.

W obliczu rosnących zagrożeń hybrydowych, Polska uznaje rozwój systemu cyberbezpieczeństwa za niezbędny element strategii obronnej. Cyberataki, takie jak ataki typu ransomware, DDoS czy próby wykradania wrażliwych danych, stanowią istotne zagrożenie. W odpowiedzi na te wyzwania, Polska utworzyła Narodowe Centrum Cyberbezpieczeństwa w ramach NASK. Celem NCB jest koordynacja działań związanych z ochroną infrastruktury krytycznej, instytucji publicznych i sektora prywatnego, oraz reagowanie w cyberprzestrzeni.

NCB pełni kluczową rolę w systemie krajowego cyberbezpieczeństwa, monitorując zagrożenia oraz wspierając sektory publiczny i prywatny w zakresie ochrony przed cyberatakami. Współpracuje z międzynarodowymi instytucjami, takimi jak Centrum Doskonałości NATO ds. Cyberbezpieczeństwa, aby zapewnić skoordynowaną obronę. Działania edukacyjne i

współpraca z uczelniami wyższymi pozwalają na kształtowanie kompetentnych kadr w tym zakresie.

W ramach swojej polityki obronnej, Polska aktywnie angażuje się w międzynarodowe inicjatywy. Jednym z najważniejszych przykładów tej współpracy jest działalność Centrum Eksperckiego NATO ds. Komunikacji Strategicznej z siedzibą w Rydze. Centrum pełni kluczową rolę w analizie i przeciwdziałaniu dezinformacji, której celem jest destabilizacja państw członkowskich NATO. Szczególnym obszarem działalności STRATCOM COE jest monitorowanie i neutralizowanie działań związanych z rosyjską dezinformacją, która w ostatnich latach stała się istotnym narzędziem w realizacji strategii hybrydowej. Centrum prowadzi także szeroką działalność edukacyjną, organizując szkolenia i warsztaty dla przedstawicieli rządów, wojskowych oraz instytucji odpowiedzialnych za bezpieczeństwo narodowe, mające na celu zwiększenie świadomości i zdolności do obrony przed zagrożeniami informacyjnymi.

Polska jest także aktywnym członkiem Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych z siedzibą w Helsinkach, które wspiera państwa Unii Europejskiej w opracowywaniu i wdrażaniu strategii obrony przed zagrożeniami hybrydowymi. Centrum to specjalizuje się w analizie zagrożeń, takich jak cyberataki, wojna informacyjna, a także ingerencje w procesy demokratyczne. Hybrid CoE dostarcza cenne narzędzia i wiedzę, które umożliwiają państwom członkowskim UE szybsze i skuteczniejsze reagowanie na zagrożenia hybrydowe.

Angażowanie się Polski w te inicjatywy pozwala na rozwój wspólnych strategii obrony przed zagrożeniami hybrydowymi oraz zwiększa zdolności kraju do reagowania na wysoce złożone i zmieniające się zagrożenia w cyberprzestrzeni. Przykłady te stanowią istotny element międzynarodowej polityki obronnej Polski, przyczyniając się do wzmocnienia bezpieczeństwa narodowego oraz stabilności regionu Europy Środkowo-Wschodniej.

W kontekście współpracy międzynarodowej, Polska aktywnie angażuje się, uczestnicząc w ćwiczeniach NATO oraz we wspólnych inicjatywach UE. Integracja systemów obrony cybernetycznej, wymiana informacji wywiadowczych oraz wspólne szkolenia są fundamentami skutecznej obrony przed zagrożeniami, które nie uznają granic narodowych.

Kluczowe elementy strategii obronnej to modernizacja armii, rozwój technologii obronnych, w tym systemów wczesnego ostrzegania, a także intensyfikacja działań w zakresie ochrony cyberprzestrzeni. Utworzenie Wojska Obrony Cyberprzestrzeni, realizacja programu „Tarcza Wschód” oraz zaangażowanie w międzynarodowe inicjatywy, takie jak STRATCOM COE i

Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych, świadczą o kompleksowym podejściu Polski do wyzwań związanych z zagrożeniami hybrydowymi. W obliczu rosnącej presji ze strony działań Rosji, Polska musi utrzymać wysoki poziom gotowości obronnej, jednocześnie rozwijając współpracę międzynarodową i przeciwdziałając zagrożeniom informacyjnym, które stanowią jedno z kluczowych wyzwań XXI wieku.

Bibliografia:

Banasik M., *Wojna hybrydowa w teorii i praktyce Federacji Rosyjskiej*, „Kwartalnik Bellona" 2016 685(2), s. 47-62.

Chudoba M., *Zagrożenia Hybrydowe - Wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej*, w: *Studia Bezpieczeństwa Narodowego, Instytut Bezpieczeństwa i Obronności,* t. 29, 2023, s. 121–140 (dostęp online: https://doi.org/10.37055/sbn/173489).

Gierasimow W., *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, "Military-Industrial Kurier 2013", tłum. Robert Coalson, "Military Review. January-February 2016".

Gierasimow W., *The Value of Science in Prediction*, "Военно-промышленный курьер 2013".

Grabowska K., *Próba wyjaśnienia pojęcia i istoty wojen hybrydowych*, w: *Świat Idei i Polityki*, t. 14, Wydawnictwo Adam Marszałek, Toruń 2015, (Rocznik Instytutu Nauk Politycznych Uniwersytetu imienia Kazimierza Wielkiego w Bydgoszczy), s. 259–282.

Hoffman F.G., *Conflict in the 21st Century. The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007.

Mockaitis T. R., *British Counterinsurgency in the Post-imperial Era,* Manchester University Press, Manchester 1997.

Meller R. S., *Report on the investigation into Russian interference in the 2016 presidential election (Vol. 1 of 2). U.S. Department of Justice*, 2019, (dostęp: https://www.justice.gov/storage/report.pdf 07.03.2025 17:08).

NATO, Ukraina: trzy lata później – powód do optymizmu, NATO, 2017, (dostęp https://www.nato.int/docu/review/pl/articles/2017/03/10/ukraina-trzy-lata-pozniej-powod-do-optymizmu/index.html 07.03.2025 13:14).

Nemeth W. J., *Future War and Chechnya. A Case for Hybrid Warfare,* California: Naval Postgraduate School, Monterey 2002.