

Klaudia WIZIMIRSKA-NAPORA

Dowództwo Wielonarodowego Korpusu Północny-Wschód Szczecin

Polskie Towarzystwo Stosunków Międzynarodowych

k.wizimirska@gmail.com

<https://orcid.org/0000-0002-3141-069X>

<https://doi.org/10.34739/dsd.2024.01.02>



ZAGROŻENIA HYBRYDOWE W KONTEKŚCIE WOJEN BUNTOWNICZYCH WZGLĘDEM PAŃSTW NATO W REGIONIE MORZA BAŁTYCKIEGO

ABSTRAKT: Artykuł przedstawia wybrane czynniki destabilizujące bezpieczeństwo międzynarodowe, skupione w ramach zagrożeń hybrydowych względem wybranych państw NATO w regionie Morza Bałtyckiego na podstawie koncepcji wojen buntowniczych J. Messnera. Wprowadzone przez autora ograniczenia geograficzne są konieczne ze względu na szeroki i zróżnicowany zakres oddziaływania agresji przy użyciu metod hybrydowych na państwa członkowskie NATO. Poszukując odpowiedzi na pytanie, z jakimi metodami działań hybrydowych mamy obecnie do czynienia w regionie Morza Bałtyckiego, opierając się na koncepcji wojen buntowniczych, przeanalizowano literaturę przedmiotu, informacje medialne oraz oficjalne wypowiedzi i poglądy ekspertów zajmujących się problematyką bezpieczeństwa międzynarodowego. Przedstawiono założenia koncepcji wojen buntowniczych oraz zarys narzędzi dotyczących zagrożeń hybrydowych względem państw NATO w rejonie Morza Bałtyckiego. Konkluzja poprzedzona procedurą badawczą złożoną z analizy logicznej, abstrahowania, klasyfikacji oraz wnioskowania pozwala wstępnie uchwycić podjęte cele badawcze na tle syntetycznej charakterystyki opisywanych zagrożeń hybrydowych. Wyniki przeprowadzonych badań wskazują, że koncepcja Messnera stanowi pierwowzór dla współczesnych wojen hybrydowych i punkt odniesienia dla lepszego zrozumienia tego zjawiska. Ponadto wybrane kraje Morza Bałtyckiego (Estonia, Łotwa, Litwa, Finlandia i Polska) w ramach NATO nie są obecnie w pełni przygotowane do przeciwdziałania zagrożeniom hybrydowym. Wynika to nie tylko ze złożoności zagrożeń, ale również z trudności ich jednoznacznego rozpoznania i klasyfikacji. Jednocześnie autor kieruje uwagę badaczy zajmujących się tą problematyką na konieczność podjęcia dyskusji na temat kierunków rozwoju NATO oraz opracowania odpowiedniej strategii dostosowanej do charakteru zagrożeń hybrydowych, co pozwoli na powzięcie odpowiedzialności Sojuszu za bezpieczeństwo jego członków.

SŁOWA KLUCZOWE: wojny buntownicze, działania hybrydowe, konflikty międzynarodowe, bezpieczeństwo, sojusz północnoatlantycki

HYBRID THREATS IN THE CONTEXT OF REBELLION WARS AGAINST NATO STATES IN THE BALTIC SEA REGION

ABSTRACT: The article presents selected factors destabilizing international security, grouped within hybrid threats towards selected NATO countries in the Baltic Sea region, based on the concept of rebellious wars by J. Messner. The geographical limitations introduced by the author are necessary due to the wide and varied scope of impact of aggression using hybrid methods on NATO member states. Searching for answers to the question of what methods of hybrid operations we are currently dealing with in the Baltic Sea region, based on the concept of rebellious wars, the literature on the subject, media information and official statements and views of experts dealing with international security issues were analyzed. The assumptions of the concept of rebel wars and an outline of tools regarding hybrid threats towards NATO countries in the Baltic Sea region are presented. The conclusion, preceded by a research procedure

consisting of logical analysis, abstraction, classification and inference, allows for a preliminary capture of the undertaken research goals against the background of the synthetic characteristics of the described hybrid threats. The results of the conducted research indicate that Messner's concept is a prototype for modern hybrid wars and a reference point for a better understanding of this phenomenon. Moreover, selected Baltic Sea countries (Estonia, Latvia, Lithuania, Finland and Poland) within NATO are currently not fully prepared to counter hybrid threats. This results not only from the complexity of the threats, but also from the difficulty of their unambiguous recognition and classification. At the same time, the author directs the attention of researchers dealing with this issue to the need to discuss the directions of NATO's development and develop an appropriate strategy adapted to the nature of hybrid threats, which will allow the Alliance to assume responsibility for the security of its members.

KEYWORDS: rebellion wars, hybrid activities, international conflicts, security, North Atlantic Alliance

WPROWADZENIE

Na podstawie teorii Jewgienija Messnera (1891-1974) prowadzenia działań zbrojnych nazywaną koncepcją wojen buntowniczych, która stanowi pierwowzór dla idei konfliktów asymetrycznych i wojen hybrydowych (jakie znamy z drugiej połowy lat dziewięćdziesiątych XX wieku i początku wieku obecnego), przeprowadzono analizę zagrożeń hybrydowych dla państw NATO regionu Morza Bałtyckiego. Należy w tym miejscu wyjaśnić, że koncepcja Messnera była szeroko rozwijana przez oficerów sił zbrojnych i służb specjalnych najważniejszych mocarstw świata podczas zimnej wojny, a swój renesans przeżywa od początku XXI wieku¹.

Teoria wojen buntowniczych nie cieszyła się dotychczas szczególnym zainteresowaniem, aż do czasu kryzysu krymskiego i możliwości zaobserwowania zastosowania tej koncepcji w praktyce w państwie sąsiadującym z naszym krajem². Ponadto działania Rosji w zakresie zagrożeń hybrydowych, prowadzone równoległe z jej wojną przeciwko Ukrainie, stwarzają istotne wyzwania zarówno dla bezpieczeństwa regionalnego, jak i międzynarodowego. W ciągu ostatniego roku Rosja zaczęła bardziej agresywnie wykorzystywać swoje środki z zestawu narzędzi w zakresie zagrożeń hybrydowych, szczególnie w regionie Morza Bałtyckiego. Bliskość krajów tego regionu do Rosji i Białorusi stwarza warunki do wykorzystywania metod wojny hybrydowej. Rosja stosuje różnorodną taktykę, wprowadzając metody takie jak: dezinformacja, cyberataki, presja psychologiczna, zinstrumentalizowana migracja i akty sabotażu, mające na celu wywarcie nacisku i destabilizację tych państw³.

J. Messner wskazywał na zacieranie się granicy między stanem pokoju a wojną, podobnie jak na ograniczenie różnic między regularnymi i nieregularnymi pododdziałami wojskowymi, formacjami paramilitarnymi, bezpieczeństwaowymi formacjami militarnymi czy doraźnie uzbrojonymi grupami społecznymi. Ten rosyjski strateg podkreślał też, że podstawową formą walki

¹ L. Sykulski, *Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera*, „Przegląd Geopolityczny” 2015, t. 11, s. 103.

² K. Kraj, *Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i Praktyka” 2012, nr 3, s. 33-39.

³ H. Praks, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, “Hybrid CoE Working Paper” 2024, May, 32, s. 5.

w wojnach buntowniczych są działania nieregularne, m.in. dywersja, terror, partyzantka czy powstanie. Jako przykład takich działań podawał on np. Polskę z okresu drugiej wojny światowej (1939-1945), zwłaszcza powstanie warszawskie⁴.

Koncepcja wykorzystania zrewoltowanych grup społecznych celem destabilizacji danego państwa, jak również użycia jego terytorium do wojen zastępczych, jest tematem szeroko opisywanym w dyskursie strategicznym na arenie międzynarodowej. Poprzez wojnę zastępczą należy rozumieć rodzaj konfliktu zbrojnego, w którym strony toczą walki na obszarze państwa trzeciego. Natomiast forma zaangażowania może mieć charakter otwarty w formule oficjalnej interwencji lub ukryty w formie udziału formacji bez oznak państwowych⁵.

Już nie tylko działania Federacji Rosyjskiej w Ukrainie, ale także wydarzenia określane mianem arabskiej wiosny lub tzw. kolorowych rewolucji noszą znamiona praktycznego wykorzystania koncepcji wojen buntowniczych, poszerzonej o osiągnięcia nowych technologii ery informacyjnej⁶.

Pierwotna koncepcja Messnera została wzbogacona o nowe rozwiązania tzw. wojen sieciowych, najnowsze osiągnięcia technologii wojen informacyjnych, sieciocentryczne systemy prowadzenia działań zbrojnych i wszystko to, co obejmuje określenie zagrożeń asymetrycznych i hybrydowych⁷. Tak więc katalog zagrożeń dla bezpieczeństwa międzynarodowego systematycznie poszerza się i generuje kolejne problemy, nie tylko dotyczące zapobiegania konfliktom i zagrożeniom, ale także trudności w zakresie rozpoznawania, klasyfikowania i interpretowania współczesnych zagrożeń.

Stąd też podjęty problem badawczy, zawarty w tytule niniejszej publikacji. Pytanie badawcze dotyczy wpływu metod i technik wykorzystywanych w obszarze działań hybrydowych na bezpieczeństwo państw NATO w regionie Morza Bałtyckiego. Tym samym celem poznawczym jest zidentyfikowanie narzędzi stosowanych w ramach wojen hybrydowych i zasygnalizowanie prawidłowości zachodzących podczas wystąpienia ataku hybrydowego w odniesieniu do koncepcji wojen buntowniczych. Na tej podstawie możliwe będzie prognozowanie kolejnych przemian w rozwoju technik w obszarze konfliktów hybrydowych celem przygotowania się do przeciwstawiania się i zapobiegania im.

Hipotezą badawczą będzie zatem następujące założenie: wielość i złożoność działań hybrydowych jest tak wysoka, że dokonywać się będą przemiany w przygotowaniu i prowadzeniu konfliktów na arenie międzynarodowej. Co za tym idzie, należy nie tylko określić kierunki rozwoju technik i narzędzi działań hybrydowych, ale też skupić się na określeniu odpowiednio przystosowanej strategii kolektywnej obrony Sojuszu względem zagrożeń hybrydowych.

W pierwszej kolejności poddano analizie pojęciowej tzw. wojny buntownicze, które stanowią pierwowzór dla współczesnych działań hybrydowych. Następnie prawidłowości w ich

⁴ K. Kraj, *Miatieżwojna Jewgienija Messnera*, „e-Terroryzm” 2012, nr 2, s. 16-17.

⁵ L. Sykulski, *op. cit.*, s. 104.

⁶ Vide P. Towle, *The strategy of war by proxy*, „The RUSI Journal” 1981, vol. 126, s. 21-26.

⁷ M. Kaldor, *New & Old Wars: Organized Violence in a Global Era*, Stanford 2001; Z. Policikiewicz, *Właściwości przyszłych wojen oraz ich implikacje społeczne*, „Zeszyty Naukowe WSOWL” 2012, nr 1, s. 94-111.

występowaniu oraz cechy charakterystyczne poddano analizie logicznej w odniesieniu do obecnej sytuacji na arenie międzynarodowej. Zidentyfikowane prawidłowości porównano, aby określić, które z nich są częściej spotykane, a które stanowią rzadkość lub wyjątek. Następnie podjęto się klasyfikacji badanego zjawiska zachodzącego w stosunku do państw regionu Morza Bałtyckiego. Na końcu wysunięto własne propozycje poprzez wnioskowanie, aby podsumować całość syntetyczną oceną wraz z rekomendacjami.

W celu realizacji założonych celów zastosowano dostępne narzędzia z zastrzeżeniem, że z powodu ograniczeń zasobów mogą one odbiegać od standardów reprezentowanych przez instytucje państwowe lub społeczne, dysponujące istotnie (w porównaniu z jednostką fizyczną) większymi zasobami, zarówno ludzkimi, jak i materialnymi.

Autor zakłada, że nie mogą one być porównywalne pod względem kompleksowości z analizami np. SG WP. Pozyskane dane pochodzą z wywiadu „białego” na podstawie źródeł otwartych z jednoznacznym wykluczeniem źródeł niejawnych i wojskowych. Podczas badań wykorzystywane były informacje o charakterze ogólnodostępnym oraz wiedza i doświadczenie autora. Główne źródła informacji opublikowane zostały też w Internecie.

Podczas analizy często posługiwano się przyjmowanymi założeniami. Obecna sytuacja na arenie międzynarodowej, z naciskiem na państwa NATO, poddana była analizie i omówieniu, w wyniku czego starano się formułować wnioski i rekomendacje, które posiadają cechy prawdopodobieństwa (realności), pozwalają zachować spójność i ciągłość rozważań oraz prognozowanych działań (w tym potencjalnego ryzyka).

WOJNY BUNTOWNICZE A WSPÓŁCZESNE ZAGROŻENIA HYBRYDOWE

Za jednego z najważniejszych prekursorów teorii wojen hybrydowych uważa się byłego rosyjskiego wojskowego Jewgienija Messnera. Autor koncepcji „wojen buntowniczych” był ciekawą postacią. Urodzony u schyłku XIX wieku, służbę wojskową odbywał począwszy od armii carskiej poprzez „białe” wojska generała Denikina. Po ich ewakuacji z terenów Ukrainy udał się na emigrację do Królestwa Serbii, Chorwatów i Słoweńców, tam w 1941 roku pełnił urząd dyrektora Niemieckiego Biura Informacyjnego. Został profesorem wojskowości, służył w Wydziale Propagandowym „Południowy Wschód” Wehrmachtu, skąd kierował sekcją rosyjską. W latach 1943-1944 redagował pismo *Russkoje dielo*, a od połowy marca 1945 roku w stopniu majora stał na czele oddziału propagandowego sztabu I Rosyjskiej Armii Narodowej gen. Borysa A. Smysłowskiego. Po wojnie udał się na emigrację do Argentyny, gdzie sformułował nową koncepcję działań zbrojnych, którą nazwał wojnami buntowniczymi (ros. *miatieżnyje wojny, miatieżwojny*)⁸.

Jak wspomniano wcześniej, wojna buntownicza to przede wszystkim zacieranie się granic między stanem pokoju i stanem wojny. Messner uznawał wojnę za nieodłączną część życia

⁸ W. Pokora, *Wojna hybrydowa nie jest patentem Putina*, <https://kurierygalicyjski.com/wojna-hybrydowa-nie-jest-patentem-putina/> (6.06.2024).

ludzi. Pisał chociażby, że wojna to jedna z form walki o istnienie i dopóki nie zniszczą jej inne formy, będzie tolerowana przez prawa życia. Podkreślał przy tym, że zarówno rewolucja przemysłowa, jak i pojawienie się geopolityki jako naukowego i praktycznego sposobu analizy politycznej skutkowało opracowaniem nowych strategii wojskowych⁹. Wynika więc z tego, że metody i techniki prowadzenia działań wojennych dostosowują się do dynamicznie zmieniającej się areny stosunków międzynarodowych. W takim rozumieniu współczesna wojna może mieć charakter ograniczenia koalicyjny lub nieograniczenia koalicyjny, czyli światowy. Podkreślić należy, że każda ze stron konfliktu może mieć jawnych i tajnych uczestników. Taki charakter wojny powoduje, że ze względu na dużą ich liczbę obserwujemy rozmycie celów podejmowanej walki.

Z takiego punktu widzenia ważne jest podkreślenie i uświadomienie sobie, że działania wojenne, na co zwracał uwagę Messner, prowadzone są na cztery sposoby. Możemy mieć do czynienia z wojną, w której regularne wojska walczą z wojskami innego kraju. Wojna została wcześniej wypowiedziana i toczy się zgodnie z określonymi zasadami prawa. Jednak możemy również spotkać się z półwojną, agresjo-dyplomacją (np. zimna wojna) i dyplomacją. W takim przypadku zaciera się granica, o której wspomniano powyżej, trudno jest zatem dostrzec podział na formalny stan pokoju a stan wojny. Społeczeństwa żyją w nieświadomości faktu toczącej się wojny. Tak rozumiana wojna hybrydowa to nic innego, jak łamanie artykułu 1. Konwencji haskiej z 1907 roku, która mówi o tym, że dwa kraje mające podjąć kroki wojenne uprzednio niedwuznacznie zawiadamiają o tym fakcie, wypowiadając wojnę lub stawiając ultimatum z warunkowym wypowiedzeniem wojny. Jak zapisano na kartach niedawnej przeszłości, ani w Gruzji w 2008 roku, ani w Ukrainie w 2014 taki fakt nie miał miejsca¹⁰.

Biorąc pod rozwagę trzy obszary prowadzenia walki: siły, przestrzeń i czas, a jednocześnie bazując na teorii wojen buntowniczych, można wysunąć wniosek, iż w wojnie hybrydowej zmianie ulegają wszystkie trzy aspekty. Tradycyjnym przeciwnikiem nie są wrogie siły zbrojne, a staje się nim społeczeństwo, naród. Ponadto znaczenie tradycyjnej przestrzeni walki nabiera innego kształtu, przybierając formę przestrzeni mentalnej, sfery świadomości ludzi i ich wyobrażeń dotyczących przestrzeni. Czas natomiast ulega szerokiemu rozmyciu, gdyż często nie jesteśmy w stanie stwierdzić, kiedy jest początek, a kiedy koniec wojny.

Messner przewidywał również wzrost znaczenia „elektronicznego mózgu” oraz nowoczesnych technologii, które pozwalałyby na ograniczenie liczby sztabowców, nawet przy wzrastającej liczbie walczących stron (żołnierzy, bojowników, rebeliantów)¹¹.

Strategia prowadzenia wojny buntowniczej według Messnera to przede wszystkim działania zbrojne podejmowane przez ludność cywilną, a głównym czynnikiem wpływającym na tego typu działania są metody psychologiczno-informacyjne. Rosyjski strateg uważał, że kluczowym zadaniem w wojnie buntowniczej jest zjednoczenie narodu i przeciągnięcie na swoją

⁹ L. Sykulski, *op. cit.*, s. 105-106.

¹⁰ W. Pokora, *op. cit.*

¹¹ L. Sykulski, *op. cit.*, s. 106.

stronę części narodu państwa wrogiego. Zatem głównym elementem wojny buntowniczej jest „psychologiczna obróbka” wszystkich warstw społecznych. Istotnym czynnikiem jest tutaj także wywołanie uczucia strachu, aż do poziomu paniki. Ponadto uwagę przykuwają również działania psychologiczne skierowane na podważenie zaufania i szacunku do władzy państwowej oraz wiary we własne siły zbrojne, w tym zdolności do obrony kraju. Jak podkreślał autor teorii wojen buntowniczych, „wojna buntownicza to wojna wszystkich przeciw wszystkim, przy czym wrogiem może być rodak, a sojusznikiem obcokrajowiec”¹².

Analizując obecną sytuację na arenie międzynarodowej, nie można nie zwrócić uwagi na analogię do powyższych słów Messnera. Nie można też pominąć kwestii geopolitycznych. „Wszystko jest wojną”¹³ – tak brzmi tytuł istotnej publikacji w kwestiach bezpieczeństwa, ale omawiającej szczególnie działania dezinformacyjne w rosyjskim myśleniu strategicznym. Stan bezpieczeństwa jest odzwierciedleniem złożonej struktury funkcjonowania państwa w środowisku geopolitycznym. Wielowymiarowość i złożoność czynników, które mają wpływ na powstanie zagrożeń oraz zmiany, jakie zachodzą nieustannie w środowisku politycznym, ekonomicznym, społecznym i informacyjnym, są źródłem powstawania zagrożeń międzynarodowych i dla bezpieczeństwa każdego kraju, jak i sojuszy¹⁴.

W ostatnich latach to właśnie Federacja Rosyjska, po aneksji Krymu i ataku na Ukrainę, jest uznawana za agresora i zagrożenie dla suwerennych państw. Rosyjski teoretyk wojskowości Swieczin podkreśla, że wojna nie jest niczym innym niżli realizacją przy użyciu siły zbrojnej wcześniej sformułowanych celów politycznych. Ta faza, jeszcze zanim wybucha otwarty konflikt, jest w jego opinii kluczowa dla osiągnięcia końcowego sukcesu. W pierwszej fazie wojny, jak w przypadku wojen buntowniczych, mamy do czynienia zwłaszcza z działaniami hybrydowymi nastawionymi na rozmycie stanu wojny i niewojny po to, aby skutecznie przeprowadzić mobilizację sił zbrojnych, ale i gospodarki, a także maksymalnie wykorzystać możliwości związane z wywarceniem presji, zastraszeniem potencjalnego przeciwnika, uzyskaniem większego pola manewru dla zabiegów dyplomatycznych celem osiągnięcia pożądaných celów politycznych przy jednoczesnym ukryciu własnych zamiarów i zatuszowaniu winy¹⁵. Powyższy pogląd ukształtował się i upowszechnił już w latach 20. i na początku lat 30. ubiegłego stulecia w rosyjskiej myśli wojskowej i jest aktualny do dziś. Stanowi istotny punkt wyjścia dla zrozumienia czynników decydujących o działaniach agresora, jednocześnie alarmując społeczność międzynarodową, że zagrożenie może nadejść na długo przed wybuchem otwartego konfliktu.

Zagrożenia lokalne są szczególnie ważne, ale i nie poddają się prostej klasyfikacji. Ma to związek z lokalną specyfiką teatru działań wojennych, wojenno-polityczną oraz strategiczną sytuacją stron konfliktu na początku działań zbrojnych oraz wielością celów i różnorodnością

¹² *Ibidem*, s. 107-108.

¹³ M. Budzisz, *Wszystko jest wojną*, Rosyjska Kultura Strategiczna, Warszawa 2021.

¹⁴ M. Kopczeński, K. Wizimirski-Napora, *Świat hybrydowy a bezpieczeństwo międzynarodowe*, [w:] J. Nowicka (red.), *Spółczesność jako uczestnik bezpieczeństwa. Wybrane zagadnienia*, Warszawa 2022, s. 104-109.

¹⁵ B. Balcerowicz, *Siły zbrojne w państwie i stosunkach międzynarodowych*, Warszawa 2006, s. 118-139.

stosowanych metod¹⁶. Analogicznie rzecz się ma w przypadku działań hybrydowych. Dotyczą one dwóch płaszczyzn – wojskowej i dyplomatycznej. Charakteryzuje je relatywnie niska stawka polityczna, która spowodowała ich użycie i wymusza precyzyjne (o mniejszej skali zaangażowania, nieeskalujące) użycie sił zbrojnych. Stąd to kolejny element, który zwraca uwagę – przykładanie przez państwo agresora wielkiej wagi do tego, aby nadać atakowi pozory legalności i międzynarodowej prawomocności, ale również potrzeba podjęcia starań o zbudowanie lokalnych sojuszy wojskowych po to, aby konflikt nie nosił znamion bilateralnego sporu¹⁷. Tak było w przypadku „specjalnej operacji wojskowej”, pod której pozorem Federacja Rosyjska zaatakowała Ukrainę w 2022 roku.

Wraz z upadkiem starego ładu międzynarodowego związanego z dwubiegunowym podziałem świata oraz jesienią ludów, która zapoczątkowała w latach 1989-1991 rewolucyjne przemiany w systemie bezpieczeństwa europejskiego, powstała niezagospodarowana przestrzeń w Europie Środkowo-Wschodniej. Transformacje ustrojowe w państwach byłego bloku wschodniego, rozwiązanie Rady Wzajemnej Pomocy Gospodarczej, Układu Warszawskiego oraz rozpad Związku Socjalistycznych Republik Radzieckich doprowadziły do pojawienia się nowych wyzwań, zagrożeń i szans dla całej Europy¹⁸. Osłabiona Rosja i dominująca w tym czasie rola Stanów Zjednoczonych we wszystkich sferach działalności w stosunkach międzynarodowych doprowadziły do próby asymilacji narodów Europy Środkowo-Wschodniej ze strukturami najpotężniejszego i najbardziej wpływowego w tym rejonie strategicznego sojuszu polityczno-militarnego – Organizacji Traktatu Północnoatlantyckiego (ang. North Atlantic Treaty Organization – NATO)¹⁹. Wysiłki na rzecz integracji z Sojuszem w państwach takich jak Polska, Węgry czy Czechy, a także ewolucja systemu bezpieczeństwa międzynarodowego raz na zawsze zmieniły oblicze Europy.

O ile na przełomie lat 80. i 90. XX wieku wydarzenia w Europie Środkowo-Wschodniej miały duży wpływ na porządek światowy, o tyle obecnie jest on kształtowany w innych regionach świata. Niemniej jednak ten obszar świata nie stracił na znaczeniu. Problemem NATO, oprócz rozbieżności w stanowiskach państw członkowskich dotyczących finansowania Sojuszu, jest brak zgodności w rozwiązywaniu konfliktu w Ukrainie oraz jej destabilizacja pod względem gospodarczym i politycznym²⁰. Państwa Europy Środkowo-Wschodniej widzą w tej wojnie preludium do ekspansji rosyjskiej na państwa byłego bloku wschodniego i dlatego podejmują działania, które mają na celu wzmocnienie wschodniej flanki Sojuszu przez obecność amerykańskich wojsk na swoim terytorium.

¹⁶ M. Budzisz, *op. cit.*, s. 75.

¹⁷ C. Kennedy, T. Waldman, *Ways of War in the 21st Century*, Chapter 7, University of Hull, 2017, s. 96-98.

¹⁸ A. Orzelska-Stączek, *Bezpieczeństwo Europy Środkowo-Wschodniej w perspektywie ładu globalnego*, [w:] *System euroatlantycki w wielobiegunowym ładzie międzynarodowym*, red. J. Fiszer, P. Olszewski, Warszawa 2013, s. 113-114.

¹⁹ A. Olech, A. Rogozińska, *Zagraniczne obiekty wojskowe jako system wzmacniania międzynarodowego potencjału militarnego Federacji Rosyjskiej*, Warszawa 2021, s. 127.

²⁰ A. Rogozińska, *Doświadczenia wojny hybrydowej na Ukrainie w kontekście bezpieczeństwa państw bałtyckich*, „Horyzonty Bezpieczeństwa” 2017, nr 19, s. 89-92.

Przynależność do NATO stwarza wprawdzie szansę na zapewnienie bezpieczeństwa, ale rodzi jednocześnie zagrożenia i wyzwania dla tego bezpieczeństwa²¹. Przynależność państw opisanego regionu do Sojuszu jest jednym z najważniejszych determinantów ich bezpieczeństwa. Rodzą się jednak wątpliwości, czy przy obserwowanej postawie państw członkowskich Sojuszu, NATO rzeczywiście podejmie działania zbrojne przeciw agresorowi w przypadku ewentualnej agresji militarnej na obszarze kraju członkowskiego. Art. 5, który mówi o kolektywnej obronie, to wprawdzie jedna z najważniejszych podstaw i wartość dodana o nieocenionej wadze, lecz ocenia się, że nie należy upatrywać w niej *ultima ratio* zapewnienia bezpieczeństwa. Taka ocena wynika z faktu, że mamy do czynienia z coraz większym podziałem pomiędzy członkami Sojuszu, który dotyczy m.in. ekonomicznych i politycznych interesów poszczególnych państw. Doskonałym przykładem będzie tutaj konflikt między Turcją a Grecją, gdy jedno państwo członkowskie – Turcja – niemalże dokonało zbrojnej interwencji w innym państwie członkowskim – Grecji – podczas gdy pozostałe państwa członkowskie pozostały bezradne, bo ważniejsze okazało się mieć w składzie Sojuszu silną Turcję niż zadbać o interes mniej atrakcyjnej strategicznie Grecji. Dlatego właśnie podczas budowania poprawnego stanu bezpieczeństwa nie można liczyć wyłącznie na stanowiska i gwarancje sojusznicze, ale należy tworzyć własny system obronny i potencjał, który oczywiście powinien być zintegrowany z Sojuszem. Przynależność do NATO, z uwagi na art. 3, powoduje konieczność rozwoju interoperacyjności pomiędzy państwami członkowskimi celem stworzenia warunków do właściwej i adekwatnej gotowości do budowania zdolności obronnych opartych na współdziałaniu na arenie międzynarodowej. Należy zatem skorzystać z dostępu do najnowszych technologii wojskowych celem modernizacji i zwiększania zdolności bojowych sił zbrojnych regionu²².

Niedawne badania nad wojnami w Afganistanie i Iraku pokazują, jak kosztowne mogą być wojny totalne pod względem strat ludzkich, gospodarczych, a także społecznych i politycznych, niezależnie od tego, jak odmienne są możliwości skonfliktowanych stron. Wraz ze wzrostem kosztów państwa coraz częściej decydują się na podjęcie wojny hybrydowej poniżej progu konfliktu zbrojnego, realizując swoje cele w zakresie bezpieczeństwa o sumie zerowej. Centralne miejsce zajmuje w tym przypadku ludność cywilna. Współczesne platformy cyfrowe i media społecznościowe pozwalają aktorom hybrydowym z dużą łatwością wpływać na obecną sytuację międzynarodową. Dobrym przykładem są rosyjskie kampanie dezinformacyjne w Internecie, niektóre z nich bardzo subtelne, aczkolwiek poważne, skierowane przeciwko niektórym państwom zachodnim²³.

²¹ Vide, *Rola NATO w kształtowaniu systemu bezpieczeństwa Europy Wschodniej*, „Przegląd Geopolityczny” 2020, nr 31, s. 115.

²² E. Rumer, *The Primakov (Not Gerasimov) Doctrine in Action*, Carnegie Endowment for International Peace, 2019, s. 17-23.

²³ A. Bilal, *Wojna hybrydowa – nowe zagrożenia, złożoności i „zaufanie” jako antidotum*, NATO Review, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html> (18.04.2024).

Co więcej, od rosyjskiej agresji na Ukrainę w 2014 roku wysiłki NATO koncentrują się głównie na odbudowie zdolności do prowadzenia dużej operacji obronnej w ramach art. 5. Niemniej jednak, konsekwentnie realizowane przez Rosję działania hybrydowe takie jak: ingerencja w wybory w USA w 2016 r., atak z użyciem broni chemicznej w Wielkiej Brytanii, próby zablokowania członkostwa Czarnogóry w NATO, sprawiły, że wzmocnienie odporności na niemilitarne zagrożenia stało się istotnym uzupełnieniem wojskowej adaptacji Sojuszu do nowych wyzwań²⁴.

Kolejny aspekt w ramach rozpatrywania kwestii zagrożeń hybrydowych dotyczy obecności chińskiego kapitału w portach państw członkowskich NATO. To ryzyko cyberataków, szpiegostwa i wykradania wrażliwych danych. Przedsiębiorstwa z Chińskiej Republiki Ludowej pozostają akcjonariuszami w wielu europejskich portach, a władze Sojuszu nie są w stanie określić limitów bezpośrednich inwestycji rządu chińskiego. To efekt nadmiernie wolnorynkowej polityki i zbyt małej liczby narzędzi kontroli. Ryzyko cybernetyczne to efekt dostępu chińskich przedsiębiorstw do systemów komunikacyjnych i sieci lokalnych, co może stwarzać większe ryzyko dla Europy, a zwłaszcza w odniesieniu do sił zbrojnych państw członkowskich²⁵.

Przeгляд obecnej sytuacji wskazuje również, że w wyniku zbrojnej agresji Rosji na Ukrainę wstrząsom podlega cała przestrzeń euroatlantycka. Daje się zauważyć tendencja do działań ukierunkowanych na destabilizację funkcjonowania morskiej infrastruktury krytycznej. Zwiększona aktywność Rosji na akwenach jest związana z mapowaniem przez Moskwę infrastruktury natowskiej oraz przeprowadzaniem akcji sabotażowych w celu zastraszenia zachodnich rządów i społeczeństw²⁶.

Mimo iż wojna hybrydowa jest wciąż spornym tematem debat akademickich i politycznych, skuteczne reagowanie na zagrożenia hybrydowe stało się najwyższym priorytetem dla NATO i jego członków. Wrogie państwa coraz częściej stosują kombinacje taktyk hybrydowych, aby zrealizować swoje strategiczne interesy, często po to, by pozostać poniżej progu konfliktu zbrojnego. W związku z tym zagrożenia hybrydowe należy traktować jako pilne i wielopoziomowe wyzwanie. Przykłady takich działań to m.in. dezinformacja, ingerencja polityczna, wojna cybernetyczna czy kradzież technologii²⁷. Ponadto w sferze gospodarczej zagrożenia hybrydowe stanowią wyzwanie dla bezpieczeństwa energetycznego, infrastruktury krytycznej, bezpośrednich inwestycji zagranicznych i badań nad wysoce zaawansowanymi technologiami. Takie wyzwania mogą nie mieć bezpośrednich implikacji militarnych, natomiast mogą istotnie wpływać na odporność Sojuszu²⁸.

²⁴ K. Załęski, *Siły zbrojne. Teoria i praktyka funkcjonowania*, Warszawa 2018, s. 153-164.

²⁵ R. Shirreff, *2017 Wojna z Rosją. Przeróżający scenariusz wydarzeń w Europie*, Poznań 2016, s. 321-327.

²⁶ R. Borkowski, *Konflikty współczesnego świata*, Kraków 2011, s. 87-92.

²⁷ D. Snetselaar, *Bezpieczeństwo wiedzy – wnioski dla NATO*, NATO Review, <https://www.nato.int/docu/review/pl/articles/2022/09/30/bezpieczenstwo-wiedzy-wnioski-dla-nato/index.html> (18.04.2024).

²⁸ P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych*, Ośrodek Studiów Wschodnich, <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych> (18.04.2024).

ZAGROŻENIA HYBRYDOWE JAKO ŚRODEK CIĘŻKOŚCI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTW REGIONU MORZA BAŁTYCKIEGO

Pięć krajów uwzględnionych w tym artykule – Estonia, Łotwa, Litwa, Finlandia i Polska – to kraje wybrane przez autora na podstawie kilku kryteriów geograficznych, historycznych i społecznych. Po pierwsze, kraje te są jedynymi państwami członkowskimi UE, które mają granicę lądową z Rosją (w przypadku NATO Norwegia również ma 195 km odcinka granicy z Rosją w Arktyce). Łączna granica tych państw z Rosją rozciąga się na długości ponad 2300 kilometrów. Trzy z nich – Łotwa, Litwa i Polska – dzieli także granicę z Białorusią, dodając kolejne 1250 kilometrów. Po drugie, wszystkie te kraje na różnych etapach swojej historii znajdowały się pod panowaniem rosyjskim lub sowieckim. A jak wiadomo, rosyjska propaganda lubi usprawiedliwiać swoją agresję, mówiąc o „historycznych granicach Rosji”. Ponadto kraje analizowane w tym artykule są wielokrotnie wymieniane, w różnym stopniu, w (odwetowych) rosyjskich narracjach jako możliwe późniejsze cele po Ukrainie. Co więcej, wszystkie pięć krajów znajduje się w regionie Morza Bałtyckiego, które ma znaczenie strategiczne dla Rosji. Morze Bałtyckie jest kluczową bramą dla rosyjskiego handlu morskiego, zwłaszcza dla eksportu ropy. W październiku 2023 r. ponad połowa całkowitego eksportu rosyjskiej ropy pochodziła z Rosji. Eksport ten stanowi główne źródło dochodów Kremla, umożliwiając napędzanie jego maszyny wojennej²⁹. Morze Bałtyckie jest także szlakiem pomiędzy silnie zmilitaryzowanymi rosyjskimi placówkami obwodu królewieckiego a Rosją. Po trzecie, Estonia i Łotwa mają największą liczbę etnicznych Rosjan i obywateli Rosji w UE proporcjonalnie do ich populacji. Kraje te były również na czele międzynarodowego wsparcia dla Ukrainy, wszystkie znajdują się w pierwszej dziesiątce państw na świecie wspierających Ukrainę. Wreszcie ze względu na duży napływ uchodźców z Ukrainy to właśnie te kraje zostały dotknięte największymi zmianami, szczególnie Polska, która przyjęła największą liczbę ukraińskich uchodźców w stosunku do ich populacji³⁰.

Główne narzędzia rosyjskich działań hybrydowych w regionie Morza Bałtyckiego skupiają się na: dezinformacji oraz operacjach wywierania wpływu, instrumentalizacji diaspor oraz instytucji powiązanych z Rosją, sabotażu, wandalizmie oraz działalności wywiadowczej, a także cyberatakach, instrumentalizacji migracji, atakach na infrastrukturę krytyczną i komunikacyjną.

W rosyjskim systemie dezinformacji nastąpiła mobilizacja znacznych zasobów przeciwko narodom europejskim w celu zalewania różnych sieci mediów społecznościowych manipulacyjnymi narracjami. W marcu 2024 r. Czechy i Polska odkryły sieć szerzącą rosyjską propagandę i wywierającą wpływy na całym świecie, w tym w Parlamencie Europejskim. Choć ogólny nacisk na tę dezinformację i wywieranie wpływu wydaje się skierowany na większe kraje Europy, takie jak Niemcy czy Francja, to podobne komunikaty również zostały

²⁹ I. Levi, *October 2023 - Monthly analysis on Russian fossil fuel exports and sanctions*, Centre for Research on Energy and Clean Air, 23 November 2023, <https://energyandcleanair.org/october-2023-monthly-analysis-on-russian-fossil-fuel-exports-and-sanctions/> (19.04.2024).

³⁰ Data from the UNHCR Operational Data Portal at <https://data.unhcr.org/en/situations/ukraine> (19.04.2024).

rozpowszechnione w krajach omawianych w tym artykule. Podczas gdy główne narracje są wspólne, istnieją także wyraźne przesłania stosowane w kontekście narodowym poszczególnych państw. Kraje bałtyckie opisuje się jako podżegaczy wojennych i rusofobiczne przyczółki „Kolektywu Zachód”. Twierdzi się, że stoją w obliczu problemów ekonomicznych, a upadek społeczny jest nieuchronny z powodu ich rządów, które kierują wszystkie swoje pieniądze na Ukrainę, lekceważąc interesy własnych obywateli. Kraje bałtyckie starają się utrudniać Rosji prowadzenie działań informacyjnych poprzez ograniczanie dostępu do rosyjskiej telewizji i innych źródeł propagandy. To doprowadziło Rosję do przeniesienia uwagi w swoich działaniach propagandowych na media społecznościowe. Obejmuje to wykorzystywanie grup skrajnych, zwłaszcza skrajnie prawicowych alternatywnych ekosystemów medialnych, które starają się przeciwstawiać mediom głównego nurtu, znajdując odpowiednie przekazy z rosyjskiej propagandy i wzmacniając je bez utrzymywania standardów dziennikarskich, nazywając siebie patriotami³¹.

Rosja ma długą historię instrumentalizowania rosyjskojęzycznych diaspor w celach strategicznych. Jest to narzędzie umożliwiające rozszerzenie swoich wpływów poza własne granice, dzieląc tym samym społeczeństwa w innych krajach. Rosja nie jest zainteresowana ich integracją, ale trzymaniem pod swoją kontrolą. Wyciekły dokumenty z rosyjskiej administracji prezydenckiej z końca 2021 r., które zawierają informacje, że Rosja zatrudnia osoby w celu utrzymania swoich wpływów w regionie Morza Bałtyckiego, w tym skupia się szczególnie na finansowaniu prorosyjskich organizacji i instytucji, wspierających wysiłki na rzecz utrzymywania szkół języka rosyjskiego czy sprzeciwiania się rozbiórce pomników sowieckich³².

Sabotaż, działalność wywrotowa i inne działania „cieniowe” mające na celu destabilizację są istotnymi częściami rosyjskiej wojny niekonwencjonalnej lub hybrydowej. Do początku 2024 r. doszło w Europie do kilku niespodziewanych wydarzeń, które zakłóciły zachodnie dostawy na Ukrainę. Uważa się, że było to częściowo spowodowane chęcią zarządzania eskalacją w stosunkach z NATO, ale także z powodu braku zdolności do kontynuowania operacji przez wojska rosyjskie. Po zyskaniu na czasie, wiosną 2024 r. Rosja aktywnie dążyła do odbudowania zdolności do podjęcia kolejnych działań zaczepnych. Należy zauważyć, że rosyjskie służby wywiadowcze mają dostęp do bardzo znaczących zasobów materialnych i ludzkich. Masowe wypędzenia setek agentów rosyjskiego wywiadu pracujących pod przykrywką dyplomatyczną w całej Europie zakłócił aparat wsparcia, przez który Rosja prowadzi wiele swoich operacji. Rosyjskie służby systematycznie rekrutują nowych agentów spośród obywateli Rosji, którzy uciekli za granicę, i próbują rekrutować obcokrajowców. Od jesieni 2023 r. w krajach bałtyckich zaobserwowano wyraźny wzrost działalności rosyjskich służb wywiadowczych, w tym aktów wandalizmu i ataków terrorystycznych. Doniesienia o zatrzymaniu osób podejrzanych o popełnienie tych

³¹ H. Praks, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, Hybrid CoE Working Paper 32, May 2024, s. 9.

³² I. Makaraityte, *Secret Kremlin in document reveals Russia's plans for Baltic states*, LRT, 1 May 2023, <https://www.lrt.lt/en/news-in-english/19/1973471/secret-kremlin-document-reveals-russia-s-plans-for-baltic-states-lrt-investigation> (04.06.2024).

czynów pokazują, że rosyjskie służby wydają się zatrudniać osoby ze środowisk przestępczych lub borykające się z trudnościami ekonomicznymi³³.

Rosyjski wywiad korzysta z aktywistów-hakerów o szerokim spektrum działania w zakresie różnych narzędzi cybernetycznych. Wzmoczona aktywność prokremlowskiej grupy hakerów towarzyszyła inwazji na Ukrainę. Przyznały się one do odpowiedzialności za uderzenie w kraje wspierające Ukrainę rozproszonymi atakami typu „odmowa usługi” (ang. *Distributed Denial of Service* – DDoS). W raporcie opublikowanym przez Europejską Agencję ds. Cyberbezpieczeństwa ENISA w grudniu 2023 r. zwrócono uwagę, że 50 proc. ataków DDoS było powiązanych z agresywną wojną Rosji przeciwko Ukrainie³⁴. Tego typu cyberataki, mające na celu zakłócenie codziennego życia, są obecnie codziennością w krajach regionu Morza Bałtyckiego i ich skala oraz złożoność stale rośnie. „W porównaniu z przeszłością ataki ideologiczne stały się znacznie bardziej ukierunkowane, dlatego też zaobserwowaliśmy wzrost liczby takich zdarzeń. Cyberatak jest jak przedłużenie zagranicznej dyplomacji” – pisze Estoński Urząd ds. Systemu Informatycznego w swoim najnowszym „Roczniku Cyberbezpieczeństwa”³⁵.

Rosja wraz ze wspierającą ją Białorusią wykorzystuje migrację jako narzędzie wpływu i wywierania presji na sąsiednie kraje. Posługują się w tym celu osobami ubiegającymi się o azyl lub poszukującymi lepszego życia za granicą. Sprawa jest dwutorowa – nie chodzi tylko o liczbę osób próbujących przedostać się przez granicę, ale także o fakt, że Rosja i władze białoruskie decydują, kto jest popychany do granic obcych krajów, a także gdzie i kiedy to następuje. Białoruś posługuje się instrumentalizacją migracji na Łotwę, Litwę i do Polski na dużą skalę od 2021 r. Wszystkie trzy państwa od tego czasu stawiają płoty i inną infrastrukturę ochrony granicy z Białorusią i zaczęły stosować rygorystyczne środki zapobiegające nielegalnemu przekraczaniu granicy. Utrudniło to ten proceder i pomogło w utrzymaniu kontrolowanych przejść. Jednakże sąsiedzi Białorusi w dalszym ciągu spotykają się z ciągłą presją migracyjną, która jest ukierunkowana i wspierana na miejscu przez białoruskie służby. Większość nielegalnych prób przekroczenia granicy w 2023 r. miało miejsce na granicach Białorusi z Polską i Łotwą. Liczba osób, które próbowały przekroczyć obie granice, podwoiła się w porównaniu z rokiem poprzednim³⁶. Trasa nielegalnych migrantów zazwyczaj zaczyna się w Moskwie, skąd przybywają na Białoruś w zorganizowany sposób, a następnie próbują przedostać się do sąsiednich krajów UE z pomocą białoruskich służb specjalnych. Białoruskie służby graniczne są znane z wielokrotnego pokazywania agresywnych zachowań na granicy, m.in. niszcząc

³³ J. Watling, *The Threat from Russia's Unconventional Warfare beyond Ukraine 2022–24*, RUSI, February 2024, <https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf> (04.06.2024).

³⁴ ENISA, *ENISA Threat Landscape for DoS Attacks*, 6 December, 2023, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks> (05.06.2024).

³⁵ Estonian Information System Authority, *Number of cyber incidents increased by a quarter in a year*, 5 February, 2024, <https://www.ria.ee/en/news/information-system-authority-number-cyber-incidents-increased-quarter-year> (4.06.2024).

³⁶ D. Tilles, *Polish border guard report shows scale of migrant pressure from Belarus*, Notes from Poland, 02 January 2024, <https://notesfrompoland.com/2024/01/02/polish-border-guard-report-shows-scale-of-migrant-crisis-from-belarus/> (05.06.2024).

infrastrukturę ochrony granic sąsiadujących krajów i angażując się w inne działania naruszające bezpieczeństwo. Jesienią 2023 roku na granicy łotewsko-rosyjskiej Rosja była bliska ogłoszenia swego rodzaju stanu nadzwyczajnego. W październiku tego roku władze rosyjskie nagle zdecydowały, że obywatele Ukrainy pragnący wjechać do Rosji z krajów UE mogą to zrobić jedynie przez lotnisko Szeremietiewo w Moskwie lub przez małą granicę w miejscowości Vientuli na trasie łotewsko-rosyjskiej. W odpowiedzi rząd łotewski, nie mając innego wyjścia, zamknął przejście graniczne całkowicie. Gdyby pozostało otwarte, mogłoby to doprowadzić, w wyniku wprowadzenia nowej rosyjskiej procedury, do masowego napływu obywateli Ukrainy przez przejście graniczne z bardzo ograniczoną infrastrukturą i potencjałem, co groziłoby poważnymi konsekwencjami dla sytuacji humanitarnej oraz porządku publicznego³⁷.

Infrastruktura energetyczna i komunikacyjna są uważane za jeden z najbardziej prawdopodobnych celów, gdyby Rosja zdecydowała się na eskalację działań wywrotowych w regionie Morza Bałtyckiego. Położenie geograficzne Finlandii i krajów bałtyckich ogranicza możliwości łączenia infrastruktury energetycznej i komunikacyjnej z resztą Europy, przy czym wiele z tych połączeń przebiega przez wody międzynarodowe Morza Bałtyckiego. To czyni je bardziej podatnymi na groźbę lub nawet dokonanie sabotażu. Jak zauważyli wyżsi urzędnicy NATO, podwodna sieć kabli i rur wokół wód europejskich nie została zbudowana z myślą o wojnie hybrydowej. Konwencja ONZ o prawie morza (UNCLOS) stwarza warunki do zabezpieczenia obiektów wrażliwych pod względem bezpieczeństwa, ale poważnie ogranicza prawo do interwencji w wody międzynarodowe. Jednocześnie Rosja jest wyraźnie mniej zaniepokojona niż inne kraje w kwestii przestrzegania prawa międzynarodowego. Działalność Rosji i jej zainteresowanie mapowaniem morskiej infrastruktury energetycznej i komunikacyjnej w całej Europie jest dobrze znana. Pojawiło się wiele raportów o podejrzanym obecności różnych statków powiązanych z Rosją w bliskości infrastruktury morskiej (krytycznej), w tym na Morzu Bałtyckim³⁸. Nowe technologie, takie jak drony morskie, skutecznie rozmieszczone przez Ukrainę na Morzu Czarnym, już wkrótce mogą zostać przyjęte przez Rosję jako prowokacja, co zwiększy obawę odwetu.

Działania związane z zagrożeniem hybrydowym, jakie stosuje Rosja, rozpoczęły się równoległe z wojną z Ukrainą. Tym samym zaczęto kwestionować porządek bezpieczeństwa regionalnego i międzynarodowego. Rosja stała się bardziej agresywna wobec Zachodu w ogóle, a cała piątka krajów regionu Morza Bałtyckiego opisana w tym artykule pod wieloma względami szczególnie narażona jest na wrogie działania Rosji. Ich położenie na wschodnim krańcu UE, geograficzna bliskość Rosji i jej wasalnej Białorusi oraz różne powiązania, jakie miały

³⁷ A. Sytasa, *Latvia says Russia trying to disrupt border with Ukraine passport ruling*, Reuters, 13 October 2023, <https://www.reuters.com/world/europe/latvia-says-russia-trying-disrupt-border-with-ukraine-passport-ruling-2023-10-13/> (05.06.2024).

³⁸ S. Hedlund, *Nordic media take aim at Russian threats*, Gisreportsonline, 7 June 2023, <https://www.gisreportsonline.com/russia-nordic-threats/>; S. Kaushal, *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*, RUSI Commentary, 25 May 2023, <https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure> (05.06.2024).

z nią te państwa, generują możliwości wrogiego wyzysku. Jednak to również czyni je cennymi sensorami umożliwiającymi identyfikację rosnących zagrożeń. Rosja zastosowała różne narzędzia, aby wywierać presję i destabilizować te narody, celując w szerzenie strachu i paniki oraz podważanie odporności społecznej. Taki stan rzeczy doskonale koreluje z założeniami koncepcji Messnera. Taktyka ta obejmuje ciągle szerzenie dezinformacji, tj. w tym przypadku zatrudnianie agentów wywiadu, wykorzystanie narzędzi cybernetycznych, wywieranie presji psychologicznej, angażowanie się w ataki fizyczne i wandalizm, a także stosowanie zinstrumentalizowanej presji migracyjnej. Rosja w zakresie zagrożeń hybrydowych podejmuje obecnie działania, których wcześniej nie widziano. Wykorzystuje również szczególnie słabe punkty systemowe w różnych krajach. W regionie Bałtyku na przykład rekrutuje i wykorzystuje agentów z miejscowej ludności rosyjskojęzycznej. W Polsce, gdzie ludność rosyjska jest nieliczna, celem są nowo przybyli Ukraińcy. Rosja również wykorzystuje wiedzę nt. krajowych przepisów i procedur. Zaczęto używać zinstrumentalizowanej presji migracyjnej przeciwko Finlandii, która wcześniej przyjęła bardziej liberalną politykę wobec osób ubiegających się o azyl. Pomimo rosnących wysiłków Rosji, jej taktyka w regionie Morza Bałtyckiego nie przyniosła jeszcze znaczących wyników. Świadomość społeczeństwa dotycząca zagrożenia ze strony Rosji ciągle rośnie i rozwinęto w tym zakresie pewną odporność. Silny konsensus polityczny i społeczny we wszystkich pięciu krajach do przeciwstawienia się rosyjskiej agresji i wsparcie Ukrainy w znacznym stopniu przyczynia się do ich obrony. Organy bezpieczeństwa wewnętrznego państw wykazały się także determinacją w zapobieganiu i powstrzymywaniu ataków z użyciem zagrożeń hybrydowych. Obecnie Rosji brakuje znaczącego wpływu na politykę wewnętrzną tych państw. Odkąd Finlandia dołączyła do NATO w 2023 r., wszystkie wskazane kraje są jego członkami. Sojusz prezentuje konwencjonalną postawę obronną w regionie, niemniej jednak w najbliższym czasie może okazać się ona niewystarczająca, a jej wzmocnienie nieuchronne. Wszystkie pięć krajów pokazało, że chociaż taktyka zagrożeń hybrydowych stanowi ciągle zagrożenie, to ważne jest, aby nie okazywać podatności na tę chorobę presji rosyjskiej, lecz zamiast tego wykazać się zdecydowaniem. Zachowując pewność siebie, wewnętrzną spójność i czujność, narody mogą skutecznie przeciwdziałać zagrożeniom i łagodzić ich skutki. Politycy muszą być gotowi do podjęcia proaktywnych działań i trudnych decyzji dotyczących wyzwań związanych z bezpieczeństwem członków Sojuszu, nawet jeśli pociągają one za sobą istotne konsekwencje, takie jak zamknięcie granic. Rosja będzie nadal testować reakcje docelowych narodów i ich sojuszników, odpowiednio dostosowując swój zestaw narzędzi dotyczących zagrożeń hybrydowych. Będzie szukać nowych luk do wykorzystania i nowych sposobów na podważenie stabilności. W tym kontekście ważne jest dla UE, NATO i ich krajów członkowskich utrzymywanie gotowości do ścisłego monitorowania sytuacji i stawiania oporu.

Działania hybrydowe cechuje łączenie różnych środków wywierania nacisku i uzależniania kraju od potencjału agresora. Na przykładzie tego, co się stało w ciągu ostatnich kilku

lat, można wyróżnić najważniejsze cechy zagrożeń hybrydowych dla państw NATO regionu Morza Bałtyckiego w odniesieniu do wydarzeń, które mają miejsce „obok nas”³⁹:

1. Asymetryczne oddziaływanie w sferze psychologicznej, ideologicznej, dyplomatycznej i ekonomicznej;
2. Prowadzenie operacji specjalnych mających na celu wprowadzenie w błąd liderów politycznych i wojskowych;
3. Manipulowanie zachowaniami społecznymi i próba wyizolowania niezadowolonego segmentu społeczeństwa (zastraszanie, podstęp, szantaż, przekupywanie);
4. Destabilizowanie państwa przy pomocy tajnych służb. Podżeganie do bezprawnych działań, wywoływanie chaosu, paniki i nieposłuszeństwa wobec władz;
5. Ustanowienie strefy zakazu lotów, wprowadzenie blokady lądowej i morskiej. Użycie prywatnych pododdziałów, wspólnie z lokalną opozycją;
6. Rozpoczęcie operacji militarnej poprzedzonej działaniami wywrotowymi;
7. Socjocentryczne uderzenia z kosmosu, lądu, powietrza i morza, połączone z kilkudniowym obezwładnieniem R/E i użyciem robotów. Odcięcie wody pitnej, żywności itp.;
8. Użycie komponentu lądowego wraz z wojskami specjalnymi i obrony terytorialnej do ostatecznej likwidacji fizycznego oporu;
9. Dywersja obliczona na osłabienie narodu będącego przeciwnikiem. Obróbka psychologiczna, podważenie wewnętrznej solidarności społecznej, nadwątlenie i zniszczenie autorytetu władzy, wywołanie konfliktów w elitach, zastraszenie, wywołanie paniki, uczynienie zaatakowanego państwa niezdolnym do oporu;
10. Znaczący wzrost roli działań z zakresu rozpoznania wywiadowczego, prowadzonych jeszcze przed wejściem w fazę intensywniejszych posunięć. Prawidłowe rozpoznanie słabych i mocnych stron potencjalnego przeciwnika, stopień inwigilacji środowisk opinio-twórczych, uzyskanie możliwości wpływu na dyskurs publiczny – opinię publiczną, narzucanie swojej wizji porządku politycznego, wiedza na temat infrastruktury krytycznej, systemu finansowego itp.;
11. Walka w przestrzeni mentalnej – wojna informacyjna. Zniszczenie międzynarodowej reputacji przeciwnika, pozbawienie go legitymacji, a w efekcie doprowadzenie do politycznej izolacji i braku możliwości zawierania międzynarodowych sojuszy i koalicji;
12. Zaskoczenie, oszustwo – maskowanie operacyjne – to wszystko to, co pozwoli wprowadzić przeciwnika w błąd odnośnie do własnych intencji, ale także utrzymanie planów w tajemnicy, użycie nowych broni i rodzajów uzbrojenia, a także sposobów prowadzenia walki. To także użycie pozorowanych struktur, komunikatów lub innych środków prowadzących do wprowadzenia w błąd. To głęboka dezinformacja, określana jeszcze przez KGB jako „działania aktywne”, które mają na celu przeniknąć umysły przeciwnika,

³⁹ A. Lanoszka, M.A. Hunzeker, *Conventional Deterrence and Landpower in Northeastern Europe*, Strategic Studies Institute, US Army War College, 2019, s. 17-22.

z góry przewidzieć jego niepożądane działania, wprowadzić w błąd, przechwycić z jego rąk inicjatywę i zakłócić jego akcje dywersyjne⁴⁰.

Uogólniając, można stwierdzić, że zgodnie z koncepcją Messnera, obecnie w środku ciężkości zagrożeń hybrydowych jest społeczeństwo, ostateczne zwycięstwo nie może być odniesione bez komponentu lądowego, a w sytuacji gdy klasyczne działania militarne nie przyniosą efektów, strona skłonna użyć BMR lub innych środków walki wykorzysta każdą przewagę. Natomiast istotą funkcjonowania każdego państwa i całego Sojuszu będzie jego strategiczna odporność⁴¹.

Utrzymujący się stabilny trend w kierunku konfliktów hybrydowych i asymetrycznych jest bardzo niebezpieczny. Celem takich ataków już nie jest przejęcie kontroli nad terytorium, ale są one raczej zorientowane na wywieranie wpływu na źródła decydujące o warunkach egzystencji społeczeństwa, suwerenności i integralności państw. Agresorzy wykorzystują luki w obszarze bezpieczeństwa, słabość w procesie zarządzania kryzysowego i brakujące zasoby obronne. Dochodzi do użycia środków i narzędzi spoza koszyka wojny konwencjonalnej⁴². Działania hybrydowe zawierają w sobie zarówno elementy wojny regularnej, jak i nieregularnej. Ponadto ukazują proces wprowadzania do walki zbrojnej niewojskowych metod i struktur organizacyjnych oraz ideowego charakteru. Użyte podczas takich konfliktów narzędzia bardzo szybko ulegają modyfikacji i przystosowaniu do zmieniających się warunków. Te czynniki sprawiają, że zaciera się granica między środkami konwencjonalnymi a niekonwencjonalnymi. Na przykładzie tych konfliktów można stwierdzić, że działania agresora są widoczne w wielu sferach (PEMSII⁴³). Z uwagi na tak obszerny zasięg działań mamy do czynienia z kreowaniem nastrojów społeczeństwa, mniejszości narodowych czy religijnych. To skłania do oceny, iż zagrożenia hybrydowe są efektem globalizacji oraz dążenia do dominacji państw i ich liderów⁴⁴.

Bezpośrednie zagrożenie dla bezpieczeństwa obywateli państw NATO i całej międzynarodowej społeczności stwarza terroryzm. Grupy terrorystyczne dzięki otwartym granicom przenikają na obszary o istotnym znaczeniu dla Sojuszu i podejmują na nich działania. Ponadto, w ocenie ekspertów, ataki cybernetyczne mogą stanowić istotny aspekt zagrożeń asymetrycznych. Prawdopodobnie zagrożenia cybernetyczne zagrożą w przyszłości systemowi bezpieczeństwa i stabilności całego obszaru Sojuszu⁴⁵.

Rozwój nowych technologii także powoduje powstanie nieznanych dotąd zagrożeń dla systemu bezpieczeństwa.

⁴⁰ H. Romerstein, *Disinformation as a KGB Weapon in the Cold War*, „Journal of Intelligence History” 2001, s. 54-67.

⁴¹ A. Dębczak, C. Pawlak, J. Keplin, *Analityczny model oceny hybrydowości współczesnych konfliktów*, „Zeszyty Naukowe AON”, 2015, nr 2, s. 52.

⁴² B. Panek, *Bezpieczeństwo Europy w II i III dekadzie XXI wieku. Zagrożenia i wyzwania*, Warszawa 2020, s. 17.

⁴³ To metoda zwana generalną segmentacją otoczenia. Zawiera czynniki: polityczne, ekonomiczne, militarne, społeczne, infrastruktury i informacyjne.

⁴⁴ T.L. Friedman, *The Lexus and the Olive Tree: Understanding Globalization*, Picador, New York 2012, s. 7-8.

⁴⁵ M.A. Miniats, *War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine*, Bard Digital Commons, NY 2019, s. 46-47.

Nowym globalnym zagrożeniem jest wykorzystanie przestrzeni kosmicznej do celów militarnych. Sojusz powinien być gotowy także na zagrożenia wynikające z degradacji środowiska naturalnego i ograniczenia zasobów⁴⁶.

NATO dostrzega fakt, że kryzysy i konflikty poza jego granicami mogą stwarzać bezpośrednie zagrożenie dla bezpieczeństwa terytorium i społeczeństw Sojuszu. Dlatego przewiduje się, że zasadniczym zadaniem NATO w najbliższym okresie będzie opanowanie sytuacji kryzysowej, stabilizacja działań oraz wspieranie procesu odbudowy upadających krajów. NATO przewiduje, że wśród zagrożeń bezpieczeństwa nie należy ignorować zagrożeń konwencjonalnych. Ponieważ wiele państw w coraz większym stopniu zależnych jest od dróg tranzytowych, na których głównie opiera się międzynarodowy handel i bezpieczeństwo energetyczne, nie należy wykluczać rozwoju piractwa, ataków na sieci dostarczające energię i zorganizowanych międzynarodowych działań przestępczych.

Potencjalnie zagrożenie dla transportu, sieci dostaw energii oraz elementów infrastruktury krytycznej stanowią organizacje i struktury pozapaństwowe. W tej sytuacji istnieje groźba pojawienia się klasycznych konfliktów zbrojnych. Trudnym do rozwiązania problemem, jednocześnie powodującym wzrost zagrożenia NATO, będzie proliferacja broni oraz środków jej przenoszenia⁴⁷.

Skuteczność Sojuszu, oprócz sprzecznych interesów jej członków, ograniczają niedostateczne środki finansowe na przeciwdziałanie zagrożeniom hybrydowym. Negatywnie wpływa na nią także brak woli państw członkowskich do zwiększania wymiany informacji wrażliwych, dotyczących np. ochrony infrastruktury krytycznej czy cyberbezpieczeństwa. Przykład nasilenia wymierzonych w Zachód kampanii dezinformacyjnych w związku z pandemią COVID dowodzi, że NATO powinno poświęcić tej problematyce jeszcze większą uwagę.

Rozmieszczenie rosyjskiej broni nuklearnej na Białorusi oraz przemieszczenie części najeźników do tego kraju⁴⁸ to ważne sygnały, że NATO będzie musiało zmierzyć się z jeszcze bardziej wieloaspektowym zagrożeniem na wschodzie niż wcześniej. Rosja, zmieniając Białoruś w de facto wasala, zyskuje cały zestaw nowych narzędzi o charakterze hybrydowym, konwencjonalnym i nuklearnym dla kontrolowanej eskalacji przeciwko NATO. Stanowi to wyzwanie dla podejścia Sojuszu do obrony i odstraszania, w tym w wymiarze nuklearnym, ale także do budowania odporności na zagrożenia hybrydowe⁴⁹.

Głównym wyzwaniem dla Sojuszu pozostaje Rosja, ale dostrzegana jest również rosnąca rola Chin. Z oczywistych względów Rosja pozostaje największym wyzwaniem dla bezpieczeństwa europejskiego. Z punktu widzenia Polski kluczowe są działania podejmowane w Europie Środkowo-Wschodniej – od agresji wojskowej na Ukrainie, poprzez tworzenie zamrożonych

⁴⁶ R. Kopeć, P. Mazur, *Odstraszanie militarne w XXI wieku. Polska – NATO – Rosja*, Kraków 2017, s. 112-114.

⁴⁷ M. Wrzosek, *Niegdyśsze wojny przyszłości*, Warszawa 2018, s. 146-150.

⁴⁸ M. Terlikowski, A.M. Dyrer, *Białoruski wektor rosyjskiego zagrożenia dla NATO*, Polski Instytut Spraw Międzynarodowych, <https://www.pism.pl/publikacje/bialoruski-wektor-rosyjskiego-zagrozenia-dla-nato> (19.04.2024).

⁴⁹ A. Dawidczyk, *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*, Warszawa 2001, s. 76-82.

konfliktów, liczne ćwiczenia ze scenariuszami ataków, w tym na państwa NATO, stałą rozbudowę potencjału militarnego na zachodniej granicy Rosji, po liczne działania hybrydowe z wykorzystaniem środków wywiadowczych i cybernetycznych, dezinformacji, propagandy czy nacisku ekonomicznego. Chiny i ich aktywność międzynarodowa będą w ocenie autora w kolejnych latach coraz poważniejszym i kompleksowym wyzwaniem i zagrożeniem⁵⁰. Zaniepokojenie powinien budzić stały przyrost wydatków obronnych Pekinu, militaryzacja polityki Chin w Azji Południowo-Wschodniej, rosnąca obecność polityczno-wojskowa na Bliskim Wschodzie i w Afryce Północnej oraz stały rozwój technologiczny, realizowany poprzez inwestycje m.in. w firmy Pirelli, IBM czy Volvo.

PODSUMOWANIE

W minionych latach w środowisku międzynarodowego bezpieczeństwa istniało wiele problemów, lecz panowała względna stabilność. Obecnie, obok klasycznych zagrożeń, takich jak terroryzm czy cyberprzestępczość, pojawiły się inne, takie jak wojna hybrydowa.

Odnosząc się do mechanizmów tzw. wojen buntowniczych, należy podkreślić, że w działaniach hybrydowych mamy do czynienia ze złożonym środowiskiem ich przygotowania. Charakterystyczne dla tego typu zagrożeń jest dobre rozpoznanie wywiadowcze, które skoncentrowane jest jednocześnie na kierunku politycznym (inwigilacja środowisk politycznych, rozpoznanie nastrojów społecznych), gospodarczym oraz wojskowym. Opracowanie planów wojny hybrydowej obejmuje zestaw działań w zakresie dywersji ideologicznej (informacyjnej) oraz klasycznej dywersji i sabotażu. Dlatego tak istotne jest rozpoznanie systemów wczesnego ostrzegania przeciwnika oraz reagowania kryzysowego. Ważnym elementem jest także, obok informacji o systemie finansowym i obronnym państwa, zebranie szczegółowych informacji dotyczących infrastruktury krytycznej (systemy teleinformatyczne, system transportu, system zaopatrzenia w energię, pokłady surowców energetycznych i paliw, systemy zaopatrzenia w żywność i wodę, system opieki zdrowotnej)⁵¹.

Prowadzenie wojny buntowniczej, a zarazem działań hybrydowych opiera się na strukturze sieciowej, która odzwierciedlona jest systemem formalnie niepowiązanych ze sobą grup społecznych i organizacji. Wykorzystana jest w niej m.in. strategia oporu niekierowanego (ang. Leaderless Resistance), która nie uwidacznia cech centralnego ośrodka kierowniczego. Poszczególne grupy posiadają dość wysoką autonomię działania. Ponadto w działaniach tj. walkach ulicznych, zamieszkach, obniżaniu zaufania do państwa wykorzystywane są, często nieświadomie, grupy niezadowolone społecznie danego państwa. Efektem takich działań ma być wywołanie chaosu lub wrażenia chaosu i braku sterowania wydarzeniami przez władze państwa. Grupy te pochodzą z różnych środowisk i często występują tuż obok nas, mogą to być

⁵⁰ W. Multan, *Wizja bezpieczeństwa międzynarodowego*, Warszawa 2001, s. 45-52.

⁵¹ L. Sykulski, *op. cit.*, s. 108.

marginalizowani politycy, mniejszości narodowe i etniczne, radykalne ugrupowania polityczno-społeczne, związki zawodowe lub jakiegokolwiek grupy dyskryminowane⁵².

W obszarze zainteresowania osób przygotowujących działania polityczno-zbrojne przy użyciu *modus operandi* koncepcji Messnera istotne jest doprowadzenie do niezadowolenia dużych grup społecznych, skłócenia elit politycznych, kolejno do problemów gospodarczych, prowokowania zamieszek, aż wreszcie otwartych działań zbrojnych prowadzonych przez m.in. przerzucane na stronę przeciwnika specjalnie przygotowane pododdziały sił specjalnych, funkcjonariuszy i żołnierzy tajnych służb. Efektywność prowadzenia działań hybrydowych uzależniona jest w dużej mierze od efektywności walki informacyjnej. Kluczowy cel to pogorszenie reputacji państwa, a optymalny efekt – izolacja polityczna kraju⁵³.

Wykorzystanie koncepcji Messnera zakłada unikanie oficjalnego zaangażowania państwa w formalną wojnę. Grupy biorące udział w działaniach nie mogą posiadać cech i oznak rozpoznawczych. W świetle prawa międzynarodowego członkowie takich grup nie mogą być traktowani jako członkowie sił zbrojnych, co pozwala na odcięcie się państwa inicjującego od wrogich działań na terytorium innego kraju. W takim przypadku konflikt przypomina raczej wojnę domową lub chaos wewnętrzny, a to jest jednym z czynników charakterystycznych koncepcji Messnera. Walki przeniesione są w teren zurbanizowany, brak jest określonej linii frontu. Rebelia może rozpocząć się wewnątrz państwa, z dala od jego granicy.

Podsumowując, można stwierdzić, że współcześnie zagrożenia hybrydowe przybierają różne formy, charakteryzują się m.in. zatarciem stanu wojny i pokoju, angażują rozmaite formacje nieregularne (paramilitarne, milicje, grupy motywowane ideologicznie lub religijnie, najemników, grupy przestępcze), podstawową formą walki są działania nieregularne, asymetryczne, toczone z jawnym pogwałceniem zasad prowadzenia wojny wyrażonych w konwencjach międzynarodowych (dywersja, terror, powstania, bunty, irredenta). Ofiarą takich zagrożeń jest przede wszystkim ludność cywilna. Zmianie ulega postrzeganie przestrzeni jako teatru działań wojennych. W coraz mniejszym stopniu znaczenie mają uwarunkowania geograficzne na korzyść determinantów mentalnych, świadomościowych, związanych z dystrybucją informacji (walka informacyjna). Celem działań wojennych jest rozbicie sił zbrojnych przeciwnika, w przypadku działań hybrydowych mamy do czynienia z chęcią zdestabilizowania państwa w wyniku prowadzonych operacji psychologicznych⁵⁴.

Klasyczna geopolityka przybiera formę geopolityki informacyjnej. Inaczej postrzegane są jej trzy główne czynniki, o których pisano wyżej. Siła rozumiana jako potęga to już nie liczba ludności czy terytorium, ani nawet siła gospodarki. Kluczowe stają się społeczne morale, integralność tożsamościowa, a także zdolność do narzucenia innym swojej wizji porządku politycznego. Czas jest postrzegany nie jako początek i koniec, a jako czas reakcji na ataki hybrydowe, zdolność

⁵² Por. J. Tomasiewicz, *Strategia oporu niekierowanego w wojnie asymetrycznej*, „Przegląd Geopolityczny” 2009, t. 1, s. 161-190.

⁵³ L. Sykulski, *op. cit.*, s. 109.

⁵⁴ B. Balcerowicz, *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Warszawa 2010, s. 190-207.

przeciwdziałania im. Natomiast przestrzeń nie ogranicza się już do terytorium, pojęcie to ewoluowało i rozlało się na sferę mentalną, świadomościową – informacyjną.

Takie spojrzenie na zagrożenia daje odpowiedź na pytanie, czym jest świat hybrydowy. Działania prowadzone przez podmioty państwowe i niepaństwowe w sposób zaplanowany i skoordynowany mają na celu osiągnięcie celów politycznych i strategicznych z możliwością utrzymania dotychczasowych stosunków gospodarczych i dyplomatycznych⁵⁵.

Obecnie świat stoi wobec wielu wyzwań i zagrożeń, w sytuacji zmniejszającej się roli państw i ograniczania nakładów na obronność niezbędna jest rewizja Strategii Bezpieczeństwa NATO. W dalszej działalności Sojusz powinien kierować się następującymi priorytetami:

1. koncentracja na najbliższym sąsiedztwie państw NATO;
2. wykorzystanie doświadczeń współpracy regionalnej;
3. budowanie i umacnianie partnerstwa;
4. zapewnienie synergii między bezpieczeństwem zewnętrznym i wewnętrznym oraz militarnym i niemilitarnym;
5. budowanie zdolności w zakresie odporności na działania hybrydowe⁵⁶.

Ponadto na podstawie analizy zagrożeń hybrydowych można ocenić, że złożone wyzwania, jakimi są zagrożenia hybrydowe, w domenie wiedzy, a szerzej w domenie gospodarczej wymagają dogłębnego zrozumienia ich wielowarstwowej i wielowektorowej natury. W szczególności NATO musi więcej inwestować w badania z zakresu nauk społecznych, aby zrozumieć naturę tego wyzwania i sformułować skuteczne sposoby reagowania. Nie wystarczy rozpoznanie tych wyzwań z czysto technicznej lub wojskowo-strategicznej perspektywy, należy przyjąć szerszy punkt widzenia – w kontekście podejmowania decyzji politycznych. NATO powinno inwestować w podnoszenie świadomości na temat tego, jak wiedza i technologie mogą przemieszczać się przez granice i z jakim skutkiem. Jednocześnie powinno zachęcać państwa członkowskie do przyjęcia podejścia zniuansowanego i dostosowanego do potrzeb oraz do wzmacniania współpracy między podmiotami wojskowymi i cywilnymi, na szczeblu rządowym i poza nim, celem sprostowania wspólnym wyzwaniom⁵⁷.

Aby skutecznie reagować na zagrożenia hybrydowe w domenach cywilnych, a nie tylko w obszarze wiedzy, zainteresowane strony muszą zważyć sprzeczne interesy i zająć się kwestiami politycznymi. NATO musi w przejrzysty sposób uwzględnić nie tylko interesy bezpieczeństwa i gospodarcze, ale także aspekty podstawowe dotyczące wolności, które definiują to, co reprezentuje Sojusz. Takie wnioski dotyczą także polityki mającej na celu przeciwdziałanie dezinformacji.

Koncepcja wojen buntowniczych w odniesieniu do zagrożeń hybrydowych, a wzbogacona o nowe technologie i doświadczenia wielu konfliktów asymetrycznych ostatniego półwiecza, daje obraz i pokazuje kierunek, jaki mogą obrać przyszłe konflikty międzynarodowe. To, na co

⁵⁵ C. Pawlak, J. Keplin, *Ujarzmić hybrydę*, „Przegląd Sił Zbrojnych” 2019, s. 45.

⁵⁶ T. Okraska, *Oblicza współczesnych konfliktów zbrojnych*, Katowice 2014, s. 178-186.

⁵⁷ M. Wrzosek, *Nowe i stare zagrożenia Sojuszu Północnoatlantyckiego*, „Zeszyty Naukowe AON” 2013, nr 2, s. 45-46.

należy zwrócić uwagę w tym kontekście, to niskie koszty tego typu działań w stosunku do wojny tradycyjnej. Ośrodkiem decyzyjnym nie musi być państwo. Strategia oporu niekontrolowanego i złożone możliwości, jakie daje technologia informacyjna, pozwalają na oddziaływanie w skali globalnej przy wykorzystaniu stosunkowo niewielkich środków i nakładów. Niezwykle ważna jest destrukcja moralna wrogiego narodu, w późniejszym etapie celem staje się dopiero wojsko i organizacje paramilitarne. Kolejny etap to dążenie do opanowania lub zniszczenia obiektów o wartości psychologicznej i materialnej. W efekcie takiego działania dochodzi do rozkładu, a w najlepszym przypadku zmiany porządku wewnętrznego.

BIBLIOGRAFIA

- Balcerowicz Bolesław. 2006. Siły zbrojne w państwie i stosunkach międzynarodowych. Warszawa: Scholar.
- Balcerowicz Bolesław. 2010. Siły zbrojne w stanie pokoju, kryzysu, wojny. Warszawa: Scholar.
- Bilal Arsalan. 2021. Wojna hybrydowa – nowe zagrożenia, złożoności i „zaufanie” jako antidotum W <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.
- Borkowski Robert. 2011. Konflikty współczesnego świata. Kraków: Uczelniane Wydawnictwa Naukowo-Dydaktyczne.
- Budzisz Marek. 2021. Wszystko jest wojną. Rosyjska Kultura Strategiczna. Warszawa: Zona Zero.
- Dawidezyk Andrzej. 2001. Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku. Warszawa: Akademia Sztuki Wojennej.
- Dębczak Artur, Pawlak Cezary, Keplin Jarosław. 2015. „Analityczny model oceny hybrydowości współczesnych konfliktów”. Zeszyty Naukowe AON Nr 2 (99): 44-52.
- ENISA. 2023. Threat Landscape for DoS Attacks W <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-dos-attacks>.
- Estonian Information System Authority. 2024. Number of cyber incidents increased by a quarter in a year W <https://www.ria.ee/en/news/information-system-authority-number-cyber-incidents-increased-quarter-year>.
- Friedman Thomas. 2012. The Lexus and the Olive Tree: Understanding Globalization. New York: Picador.
- Hedlund Stefan. 2023. Nordic media take aim at Russian threats W <https://www.gisreportsonline.com/r/russia-nordic-threats/>.
- Kaushal Sidharth. 2023. Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure W <https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure>.
- Kaldor Mary. 2001. New & Old Wars: Organized Violence in a Global Era. Stanford: University Press.
- Kennedy Caroline, Waldman Thomas. 2017. Ways of War in the 21st Century. W Issues in 21st Century World Politics, 94-105. Red Globe Press.
- Kopczewski Marian, Wizimirska-Napora Klaudia. 2022. Świat hybrydowy a bezpieczeństwo międzynarodowe. W Społeczeństwo jako uczestnik bezpieczeństwa. Wybrane zagadnienia, 104-109. Akademia Sztuki Wojennej.

- Kopeć Rafał, Mazur Przemysław. 2017. *Odstraszanie militarne w XXI wieku. Polska – NATO – Rosja*. Kraków: Uniwersytet Pedagogiczny.
- Kraj Kazimierz. 2012. „Wojny asymetryczne czy miatieżwojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku”. *Bezpieczeństwo. Teoria i Praktyka* 3 (VIII): 33-39.
- Kraj Kazimierz. 2012. „Miatieżwojna Jewgienija Messnera”. *e-Terroryzm* 2: 16-17.
- Lanoszka Alexander, Hunzeker Michael. 2019. *Conventional Deterrence and Landpower in Northeastern Europe*. USA: USAWC Press.
- Levi Isaac. 2023. October 2023 – Monthly analysis on Russian fossil fuel exports and sanctions W <https://energyandcleanair.org/october-2023-monthly-analysis-on-russian-fossil-fuel-exports-and-sanctions/>.
- Makaraityte Indre. 2023. Secret Kremlin document reveals Russia’s plans for Baltic states – LRT investigation W <https://www.lrt.lt/en/news-in-english/19/1973471/secret-kremlin-document-reveals-russia-s-plans-for-baltic-states-lrt-investigation>.
- Miniats Magdalena. 2019. *War of Nerves: Russia’s Use of Cyber Warfare in Estonia, Georgia and Ukraine*. Bard Digital Commons.
- Multan Wojciech. 2001. *Wizja bezpieczeństwa międzynarodowego*. Warszawa: Elipsa.
- Okraska Tomasz. 2014. *Oblicza współczesnych konfliktów zbrojnych*. Katowice: Instytut Nauk Politycznych i Dziennikarstwa Uniwersytetu Śląskiego.
- Olech Aleksander, Rogozińska Agnieszka. 2021. *Zagraniczne obiekty wojskowe jako system wzmacniania międzynarodowego potencjału militarnego Federacji Rosyjskiej*. Warszawa: Akademia Sztuki Wojennej.
- Orzelska-Stączek Agnieszka, 2013. *Bezpieczeństwo Europy Środkowo-Wschodniej w perspektywie ładu globalnego*. W *System euroatlantycki w wielobiegunowym ładzie międzynarodowym*, 12-43. Elipsa.
- Panek Bogdan. 2020. *Bezpieczeństwo Europy w II i III dekadzie XXI wieku. Zagrożenia i wyzwania*. Warszawa: Difin.
- Pawlak Cezary, Keplin Jarosław. 2019. „Ujarzmić hybrydę”. *Przegląd Sił Zbrojnych* 2: 54-59.
- Pokora Wojciech. 2018. *Wojna hybrydowa nie jest patentem Putina* W <https://kuriergalicyjski.com/wojna-hybrydowa-nie-jest-patentem-putina/>.
- Policikiewicz Zdzisław. 2012. „Właściwości przyszłych wojen oraz ich implikacje społeczne”. *Zeszyty Naukowe WSOWL Nr 1 (163)*: 94-111.
- Praks Henrik. 2024. *Russia’s hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, Hybrid CoE Working Paper 32.
- Rogozińska Agnieszka. 2017. „Doświadczenia wojny hybrydowej na Ukrainie w kontekście bezpieczeństwa państw bałtyckich”. *Horyzonty Bezpieczeństwa* 9(4): 85-97.
- Romerstein Herbert. 2001. „Disinformation as a KGB Weapon in the Cold War”. *Journal of Intelligence History* Nr 1: 54-67.
- Rumer Eugene. 2019. *The Primakov (Not Gerasimov) Doctrine in Action*. Washington: Carnegie Endowment for International Peace.
- Shirreff Richard. 2016. *2017 Wojna z Rosją. Przeróżający scenariusz wydarzeń w Europie*. Poznań: Rebis.
- Snetselaar David. 2002. *Bezpieczeństwo wiedzy – wnioski dla NATO* W <https://www.nato.int/docu/review/pl/articles/2022/09/30/bezpieczenstwo-wiedzy-wnioski-dla-nato/index.html>.

- Szymański Piotr. 2020. NATO i Unia Europejska wobec zagrożeń hybrydowych, Ośrodek Studiów Wschodnich W <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych>.
- Sykulski Leszek. 2015. „Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera”. *Przegląd Geopolityczny* 11: 103-112.
- Sytasa Andrius. 2023. Latvia says Russia trying to disrupt border with Ukraine passport ruling W <https://www.reuters.com/world/europe/latvia-says-russia-trying-disrupt-border-with-ukraine-passport-ruling-2023-10-13/>.
- Terlikowski Marcin, Dyner Anna Maria. 2024. Białoruski wektor rosyjskiego zagrożenia dla NATO W <https://www.pism.pl/publikacje/bialoruski-wektor-rosyjskiego-zagrozenia-dla-nato>.
- Tilles Daniel. 2024. Polish border guard report shows scale of migrant pressure from Belarus W <https://notesfrompoland.com/2024/01/02/polish-border-guard-report-shows-scale-of-migrant-crisis-from-belarus/>.
- Tomasiewicz Jarosław. 2009. „Strategia oporu niekierowanego w wojnie asymetrycznej”. *Przegląd Geopolityczny Tom 1*: 161-190.
- Towle Philip. 1981. „The strategy of war by proxy”. *The RUSI Journal* 126:21-26.
- Watling Jack. 2024. The Threat from Russia’s Unconventional Warfare beyond Ukraine 2022–24 W <https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf>.
- Wrzosek Marek. 2018. *Niegdyśejsze wojny przyszłości*. Warszawa: Fronda.
- Wrzosek Marek. 2013. „Nowe i stare zagrożenia Sojuszu Północnoatlantyckiego”. *Zeszyty Naukowe AON* 2: 31-46.
- Załęski Krzysztof. 2018. *Siły zbrojne. Teoria i praktyka funkcjonowania*. Warszawa: Difin.