

dr hab. inż. Zbigniew Ciekankowski

Akademia Białka im. Jana Pawła II w Białej Podlaskiej

ORCID: 0000-0002-0549-894X

e-mail: zbigniew@ciekanowski.pl

dr Bartosz Błaszczak

Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu

ORCID: 0009-0002-0457-434

e-mail: bartosz.blaszczak@wskz.pl

dr Irena Malinowska

Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu

ORCID: 0000-0002-9194-3121

e-mail: galindia@wp.pl

SYSTEM ZARZĄDZANIA KRYZYSOWEGO NATO A ZAGROŻENIA HYBRYDOWE

NATO CRISIS MANAGEMENT SYSTEM AND HYBRID THREATS

Streszczenie

Celem niniejszego artykułu jest zbadanie rozwoju zdolności systemu zarządzania kryzysowego NATO w zwalczaniu zagrożeń o charakterze hybrydowym. Problematykę tę należy rozumieć w kontekście zmieniających się realiów bezpieczeństwa, gdzie działania hybrydowe stanowią coraz większe wyzwanie dla Sojuszu. W pierwszej części artykułu opisano system zarządzania kryzysowego NATO, wymieniając podstawowe elementy. Następnie przedstawiono element odstraszania jako istotną determinantę zdolności NATO. W głównej części skupiono się na działaniach mających na celu zwiększania zdolności NATO do zwalczania zagrożeń hybrydowych, w aspekcie zarządzania kryzysowego. Podsumowując stwierdzono, iż rozwój zdolności zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych jest kluczowym elementem adaptacji sojuszu do zmieniających się realiów bezpieczeństwa. W celu przeprowadzenia badań sformułowano problem badawczy: *Jakie działania podejmuje Sojusz Północnoatlantycki w celu zwiększenia zdolności systemu zarządzania kryzysowego do zwalczania nowych zagrożeń o charakterze hybrydowym?* Problem badawczy koncentruje się na efektywności działań podejmowanych przez NATO w zwalczaniu zagrożeń hybrydowych

oraz na identyfikacji obszarów, wymagających dalszych usprawnień. Badanie skupia się na ocenie zarówno działań militarnych, jak i cywilnych, podejmowanych przez NATO w reakcji na zagrożenia hybrydowe. Odpowiednio do postawionego problemu badawczego autorzy sformułowali hipotezę badawczą, która zakłada, że *poprzez skoordynowane działania obejmujące zarówno aspekty militarno-obronne, jak i cywilne, NATO jest w stanie skuteczniej przeciwdziałać zagrożeniom hybrydowym. Jednakże istnieje również prawdopodobieństwo, że istnieją obszary, w których zdolności NATO do zwalczania zagrożeń hybrydowych mogą być ograniczone lub wymagają dalszego rozwoju.* W ramach badania przeprowadzono szczegółową analizę dokumentów oficjalnych NATO, takich jak raporty, strategie, wytyczne i dokumenty polityczne, aby zrozumieć podejście sojuszu do zwalczania zagrożeń hybrydowych oraz ocenić postępy w rozwoju zdolności kryzysowych, a także przeprowadzono analizę w oparciu o artykuły naukowe z ostatnich lat. Dokonano również analizy przypadków działań hybrydowych, które miały miejsce w przeszłości i w których NATO było zaangażowane lub mogło zastosować swoje zdolności kryzysowe. Studia przypadków dostarczyły wglądu w skuteczność działań NATO oraz identyfikację obszarów wymagających usprawnienia. Wykorzystane metody badawcze pozwoliły na uzyskanie kompleksowego i dogłębnego zrozumienia problematyki oraz efektywnego oceniania zdolności systemu zarządzania kryzysowego NATO w zwalczaniu zagrożeń hybrydowych.

Słowa kluczowe: analiza, bezpieczeństwo, efektywność, reagowanie, zdolność

Summary

The purpose of this article is to examine the development of the capabilities of the NATO crisis management system in countering hybrid threats. This issue should be understood in the context of the changing security reality, where hybrid activities are an increasing challenge for the Alliance. The first part of the article describes NATO's crisis management system, listing the basic elements. The deterrence element was then presented as an important determinant of NATO's capabilities. The main part focused on activities aimed at increasing NATO's ability to combat hybrid threats in the aspect of crisis management. In conclusion, it was concluded that the development of NATO's crisis management capabilities in the context of hybrid threats is a key element of the alliance's adaptation to the changing security reality. The research problem was formulated: What actions is the North Atlantic Alliance taking to increase the ability of the crisis management system to combat new hybrid threats? The research problem focuses on the effectiveness of NATO's actions in countering hybrid threats and on the identification of areas for further improvement. The survey focuses on assessing both military and civilian actions taken by NATO in response to hybrid threats. In accordance with the research problem posed, the author formulated a research hypothesis which assumes that through coordinated actions covering both military-defence and civilian aspects, NATO is able to counter hybrid threats more effectively. However, there is

also the likelihood that there are areas where NATO's capabilities to counter hybrid threats may be limited or require further development. The study conducted a detailed analysis of official NATO documents, such as reports, strategies, guidelines and policy documents, to understand the Alliance's approach to countering hybrid threats and to assess progress in the development of crisis capabilities, and to draw on scientific articles from recent years. It also analysed cases of hybrid activities that have taken place in the past and in which NATO has been involved or could have deployed its crisis capabilities. The case studies provided insight into the effectiveness of NATO's operations and the identification of areas for improvement. The research methods used allowed for a comprehensive and in-depth understanding of the issues and effective assessment of the capabilities of the NATO crisis management system in combating hybrid threats.

Keywords: analysis, security, efficiency, response, capability

Wstęp

W obliczu dynamicznie zmieniającego się środowiska bezpieczeństwa, NATO stoi przed nowymi wyzwaniami związanymi z zagrożeniami hybrydowymi, które łączą tradycyjne działania militarno-polityczne z nieliniowymi, asymetrycznymi formami agresji. Te zagrożenia, charakteryzujące się użyciem różnorodnych środków – od cyberataków, przez kampanie dezinformacyjne, po wspieranie ruchów separatystycznych i wykorzystanie niepaństwowych aktorów – stanowią poważne wyzwanie dla stabilności i bezpieczeństwa państw członkowskich NATO. Zagrożenia hybrydowe są trudne do zidentyfikowania i przeciwdziałania, ponieważ często nie przekraczają progu tradycyjnego konfliktu militarno-politycznego, a jednocześnie mogą skutecznie destabilizować i wpływać na społeczeństwa oraz systemy polityczne.

W odpowiedzi na te złożone wyzwania, NATO nieustannie rozwija swoje zdolności zarządzania kryzysowego, aby skutecznie przeciwdziałać i neutralizować zagrożenia hybrydowe. Organizacja ta inwestuje w innowacyjne technologie, rozwija nowe strategie i procedury, a także zacieśnia współpracę między państwami członkowskimi oraz z innymi międzynarodowymi partnerami. Celem tych działań jest nie tylko zwiększenie zdolności do szybkiej i skutecznej reakcji na incydenty, ale także wzmocnienie odporności społeczeństw na różnorodne formy agresji hybrydowej.

Rozwój systemu zarządzania kryzysowego NATO, w kontekście zagrożeń hybrydowych, obejmuje szereg inicjatyw i projektów, które mają na celu wzmocnienie zdolności sojuszu do identyfikacji, analizy i reagowania na tego typu zagrożenia. Wprowadzane są nowe technologie, takie jak zaawansowane systemy monitoringu cyberprzestrzeni oraz rozwijane są mechanizmy wymiany

informacji i współpracy wywiadowczej między państwami członkowskimi. Ponadto, NATO kładzie duży nacisk na edukację i szkolenie personelu, aby zapewnić, że posiada on odpowiednie umiejętności i wiedzę niezbędną do efektywnego działania w środowisku zagrożeń hybrydowych.

W niniejszym artykule podjęta została szczegółowa analiza rozwoju zdolności zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych. Omówione zostaną główne elementy strategii NATO, nowe technologie i procedury, a także przykłady operacji, które ilustrują praktyczne zastosowanie tych zdolności. Analiza ta ma na celu ukazanie, w jaki sposób NATO adaptuje się do współczesnych wyzwań bezpieczeństwa i jakie kroki podejmuje, aby zapewnić skuteczną ochronę swoich członków przed zagrożeniami hybrydowymi, które stają się coraz bardziej powszechne i złożone.

System zarządzania kryzysowego NATO

Zgodnie ze strategią przyjętą w Madrycie w 2022 roku, jednym z priorytetowych zadań NATO pozostaje zapobieganie i reagowanie na kryzysy bezpieczeństwa w sąsiedztwie. Doświadczenia zdobyte w ciągu blisko trzech dekad prowadzenia misji poza obszarem traktatowym, szczególnie w Afganistanie, wpłynęły na zmianę podejścia Sojuszu. NATO planuje teraz w większym stopniu angażować się w działania prewencyjne zamiast bezpośrednich interwencji. Wzrastać będzie znaczenie budowania zdolności i odporności partnerów NATO, w tym cywilnego zarządzania kryzysowego¹.

System zarządzania kryzysowego NATO (NATO Crisis Management System, NCMS) to złożony i wszechstronny mechanizm, który umożliwia Sojuszowi szybkie i efektywne reagowanie na różnorodne sytuacje kryzysowe. Jego struktura jest wielopoziomowa i obejmuje szereg organów decyzyjnych, operacyjnych oraz doradczych, które współpracują, aby zapewnić bezpieczeństwo państw członkowskich NATO. Obejmuje również planowanie cywilne (Civil Emergency Planning, CEP), współpracę cywilno-wojskową, a także zarządzanie skutkami (Consequence Management). Dzięki temu można reagować na różnorodne zagrożenia i przewyżczać różnego typu sytuacje kryzysowe. Proces zarządzania kryzysowego w ujęciu NATO-wskim obejmuje sześć faz:

- oznaki sytuacji kryzysowej i ostrzeżenie (Indications and Warning),
- ocena sytuacji (Assessment),
- dobór opcji reagowania (Response Options Development),
- planowanie (Planning),
- wykonanie (Execution),
- stadium przejściowe (Transition)².

¹ F. Bryjka, *Przyszłość reagowania kryzysowego w nowej strategii NATO*, „Biuletyn PISM”, nr 118 (2537), 21 lipca 2022 r., s. 1.

² Współpraca w ramach NATO, RCB, <https://archiwum.rcb.gov.pl/wspolpraca-w-ramach-nato/> [dostęp: 31.05.2024]

Granice pomiędzy tymi fazami są jednak traktowane jako płynne. Na szczycie struktury NCMS znajduje się Rada Północnoatlantycka (North Atlantic Council, NAC), która jest głównym organem decyzyjnym NATO. Rada podejmuje kluczowe decyzje polityczne i operacyjne, związane z zarządzaniem kryzysowym. W jej pracach wspomaga ją Komitet Wojskowy NATO (NATO Military Committee), który dostarcza fachowego doradztwa w sprawach wojskowych. Komitet ten składa się z szefów obrony wszystkich państw członkowskich³.

Komitet Planowania Obrony (Defence Planning Committee, DPC) odgrywa ważną rolę w planowaniu obronnym i współpracuje z NAC, w kwestiach związanych z zarządzaniem kryzysowym. Operacyjne centrum zarządzania kryzysowego stanowi NATO Crisis Management Centre (NCMC). To właśnie tutaj monitorowane są potencjalne kryzysy oraz koordynowana jest odpowiedź NATO. Centrum zbiera informacje, analizuje sytuację i przekazuje dane do odpowiednich organów.

Ważnym elementem NCMS jest również Stała Grupa Robocza Zarządzania Kryzysowego (Standing Crisis Management Group, SCMG), która składa się z ekspertów z różnych dziedzin. Grupa ta wspiera NAC i NCMC, przygotowując rekomendacje oraz plany działania w sytuacjach kryzysowych.

Operacyjne prowadzenie działań wojskowych leży w gestii Dowództwa Sojuszniczego Operacji (Allied Command Operations, ACO), które kieruje operacjami z Naczelnego Dowództwa Sojuszniczych Sił w Europie (SHAPE). Innym kluczowym elementem jest mechanizm szybkiej reakcji, który umożliwia natychmiastowe działania w odpowiedzi na kryzysy. W ramach tego mechanizmu działa m.in. Siły Szybkiego Reagowania NATO (NATO Response Force, NRF). Siły Odpowiedzi NATO (NATO Response Force, NRF) to wielonarodowa siła szybkiego reagowania, utworzona przez NATO w celu szybkiego reagowania na różnorodne zagrożenia bezpieczeństwa. NRF jest wszechstronna i zdolna do realizacji szerokiego spektrum misji, od operacji bojowych po działania humanitarne⁴.

Jednak konieczne było posiadanie kolejnych brygad powietrznodesantowych w celu przeciwstawienia się agresji. Na wyższym poziomie dowodzenia problem stawał się bardziej skomplikowany z wielu przyczyn, głównie o charakterze politycznym⁵.

System zarządzania kryzysowego NATO opiera się również na szeregu procedur i mechanizmów. Jednym z nich jest System Ostrzegania i Reakcji

³ NATO – Topic: North Atlantic Council (NAC), https://www.nato.int/cps/en/natohq/topics_49763.htm [dostęp: 31.05.2024]

⁴ NATO – Temat: Siły Odpowiedzi NATO, https://www.nato.int/cps/en/natolive/topics_49755.htm [dostęp: 31.05.2024]

⁵ M. Banasik, *Zarządzanie kryzysowe NATO mechanizmem zapewniania bezpieczeństwa i ochrony ludności*, „Przedsiębiorczość i Zarządzanie”, Issue 5.3, 2017, s. 348.

(Warning and Response System), który zapewnia wczesne ostrzeżenie przed potencjalnymi kryzysami poprzez monitorowanie i ocenę sytuacji⁶. Regularne ćwiczenia i szkolenia są również integralną częścią systemu, mając na celu przygotowanie sił NATO do różnorodnych scenariuszy kryzysowych oraz wzmocnienie gotowości operacyjnej i koordynacji między państwami członkowskimi.

System zarządzania kryzysowego NATO jest kluczowym elementem zapewniającym skoordynowaną i skuteczną reakcję na zagrożenia dla państw członkowskich Sojuszu, wzmacniając tym samym bezpieczeństwo międzynarodowe.

Zarządzanie kryzysowe jest jednym z kluczowych zadań NATO, które wykorzystuje odpowiednią kombinację narzędzi politycznych i wojskowych w celu zarządzania kryzysami, w coraz bardziej złożonym środowisku bezpieczeństwa. NATO jest jedną z niewielu organizacji międzynarodowych, dysponujących doświadczeniem i narzędziami do prowadzenia operacji zapobiegania kryzysom oraz zarządzania kryzysowego. Solidne zdolności NATO w zakresie zarządzania kryzysowego pozwalają na skuteczne radzenie sobie z szerokim wachlarzem kryzysów, które mogą stanowić zagrożenie dla bezpieczeństwa terytorium i ludności Sojuszu. Kryzysy te mogą mieć charakter polityczny, wojskowy lub humanitarny, a także mogą wynikać z klęsk żywiołowych lub zakłóceń technologicznych. NATO zapewnia ramy, w których państwa członkowskie mogą wspólnie pracować i szkolić się w celu planowania oraz prowadzenia wielonarodowych operacji zarządzania kryzysowego, często w krótkim czasie. Może również szkolić i w stosownych przypadkach, współpracować z innymi podmiotami na potrzeby połączonych operacji i misji zarządzania kryzysowego.

Wojna hybrydowa oraz zagrożenia, zmusiły NATO do wprowadzenia gruntownych zmian, które umożliwiłyby Sojuszowi adaptację do nowych uwarunkowań i skuteczną odpowiedź na zagrożenia ze strony Federacji Rosyjskiej. Na szczycie w Newport w 2014 roku zdecydowano o konieczności prowadzenia skutecznego odstraszenia oraz szybkiej koncentracji wojsk na wybranych kierunkach strategicznych⁷.

Członkowie Sojuszu podejmują decyzje o zaangażowaniu się w operacje zarządzania kryzysowego na zasadzie indywidualnych przypadków i w drodze konsensusu. NATO uznaje, że siły zbrojne nie są w stanie samodzielnie rozwiązać kryzysu czy konfliktu. Wnioski wyciągnięte z poprzednich operacji jasno pokazują, że skuteczne zarządzanie kryzysowe wymaga wszechstronnego podejścia politycznego, cywilnego i wojskowego⁸.

⁶ R. Gottemoeller, K. Hedgecock, J. Magula, P. Poast, *Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept*, "Defence Studies", 22(3), 2022, s. 516–524.

⁷ M. Banasik, *Zarządzanie kryzysowe...*, op. cit., s. 348.

⁸ NATO – Topic: Crisis management, https://www.nato.int/cps/en/natohq/topics_49192.htm? [dostęp: 31.05.2024]

Odstraszanie jako istotny element zdolności NATO

W środowisku bezpieczeństwa, charakteryzującym się strategiczną konkurencją, wszechobecną niestabilnością i powtarzającymi się wstrząsami, sojusznicy w dalszym ciągu muszą stawić czoła zagrożeniom hybrydowym, cybernetycznym i innym asymetrycznym zagrożeniom.⁹

Dzięki siłom natychmiastowego reagowania i rozmieszczeniu elementów dowodzenia w sześciu państwach granicznych Sojuszu, możliwe jest szybkie udzielenie wsparcia wschodniej flance. Siły te powinny być jednak wzmocnione „tarczą”, czyli zdolnością do odstraszania i długoterminowym zaangażowaniem sojuszników w budowę regionalnego bezpieczeństwa¹⁰. Sojusz posiada zdolność do odparcia agresji i posiada narzędzia do oddziaływania, tak aby przeciwnik poniósł wszelkie jej konsekwencje¹¹.

Zdolności NATO są różnorodne i obejmują zarówno aspekty wojskowe, jak i polityczne, co umożliwia mu skuteczne reagowanie na różnorodne zagrożenia w sferze wojskowej. NATO dysponuje znacznymi siłami zbrojnymi, obejmującymi jednostki lądowe, powietrzne i morskie, które są dostarczane przez państwa członkowskie. Cyberobrona jest kluczowym obszarem działalności NATO. W odpowiedzi na rosnące zagrożenia w cyberprzestrzeni, sojusz rozwija zaawansowane zdolności obronne, aby chronić swoje sieci i systemy¹². Centrum Doskonalenia Cyberobrony NATO (CCDCOE) odgrywa centralną rolę w tej dziedzinie, prowadząc badania, szkolenia i rozwijając strategię obronne¹³. W aspekcie politycznym, NATO opiera swoje decyzje na zasadzie konsensusu, co oznacza, że wszystkie 31 państw członkowskich muszą zgodzić się na podjęcie działań. Ta zasada zapewnia, że decyzje są wspólne i mają szerokie poparcie, co wzmacnia jedność i koordynację w sojuszu. NATO rozwija również liczne partnerstwa z krajami na całym świecie, w tym z państwami Partnerstwa dla Pokoju, aby promować międzynarodową stabilność i bezpieczeństwo.

NATO angażuje się również w różnorodne operacje i misje na całym świecie. Przykładem może być rola NATO w stabilizacji Bałkanów, gdzie prowadziło operacje takie jak IFOR i SFOR w Bośni i Hercegowinie oraz KFOR w Kosowie. Innym przykładem jest misja Resolute Support w Afganistanie, której celem było szkolenie, doradztwo i wsparcie afgańskich sił bezpieczeństwa. NATO prowadzi również operacje antypirackie u wybrzeży Somalii w ramach misji Ocean Shield, mającej na celu ochronę szlaków morskich i zwalczanie piractwa.

⁹ The Secretary General's Annual Report 2023, s. 39.

¹⁰ W. Lorenz, *Szpica NATO potrzebuje tarczy na wschodniej flance*, „Biuletyn PISM”, nr 15 (1252), 2015, s. 1.

¹¹ J. Stocker, *Deterrence in the 21st century*, 2017, <https://www.japcc.org/deterrence-in-the-21st-century/> [dostęp: 01.06.2024]

¹² M. Kulczycki, *Rozwój zdolności NATO wobec zagrożeń cybernetycznych*, „Rocznik Bezpieczeństwa Międzynarodowego”, vol. 14, nr 2, 2020, s. 154.

¹³ L. Brent, *Rola NATO w cyberprzestrzeni*, „NATO Review”, 2019, <https://www.nato.int/docu/review/pl/articles/2019/02/12/rola-nato-w-cyberprzestrzeni/index.html>

Zdolności NATO są więc szerokie i zróżnicowane, obejmując zarówno twardą siłę wojskową, jak i miękkie narzędzia dyplomatyczne. Organizacja nieustannie adaptuje się do nowych wyzwań, takich jak cyberzagrożenia, jednocześnie kontynuując swoje tradycyjne role w zapewnianiu bezpieczeństwa i stabilności na arenie międzynarodowej. Odstraszanie powraca dziś do gry. Choć było postrzegane przez wielu jako jedynie relikw zimnej wojny, rosyjsko-ukraiński kryzys na Ukrainie przyspieszył jego odrodzenie¹⁴. Odstraszanie jest jednym z kluczowych elementów strategii NATO, mającym na celu zapobieganie agresji i zapewnienie bezpieczeństwa państw członkowskich. Opiera się na przekonaniu potencjalnych przeciwników, że koszty podjęcia działań zbrojnych przeciwko NATO przewyższają potencjalne korzyści. Ta strategia obejmuje zarówno zdolności konwencjonalne, jak i nuklearne, oraz szeroki wachlarz działań politycznych i wojskowych. Państwa Sojuszu Północnoatlantyckiego podjęły szereg działań, mających na celu „stworzenie” czynników odstraszania w stosunku do różnego rodzaju zagrożeń¹⁵. W celu zminimalizowania ryzyka rosyjskiej agresji i wzmocnienia politycznej spójności NATO, konieczne będą znaczne zmiany w podejściu do obrony i odstraszania w dłuższej perspektywie¹⁶.

Odstraszanie NATO opiera się na zintegrowanym podejściu, które łączy zdolności konwencjonalne i nuklearne z innowacyjnymi strategiami w obszarach takich jak cyberobrona i wojna hybrydowa. Wzmocnienie wschodniej flanki, budowanie partnerstw oraz zachowanie jedności politycznej są kluczowymi elementami tej strategii. NATO nieustannie adaptuje swoje podejście do zmieniających się zagrożeń, aby zapewnić bezpieczeństwo swoim członkom i utrzymać stabilność na arenie międzynarodowej.

Zdolność NATO do zwalczania zagrożeń hybrydowych w aspekcie zarządzania kryzysowego

NATO jako sojusz obronny, stoi przed wyzwaniem dostosowania swoich strategii, doktryn i narzędzi do skutecznego zwalczania zagrożeń hybrydowych. Kluczowym elementem tej transformacji jest zrozumienie natury zagrożeń hybrydowych oraz rozwój zdolności, które pozwolą na ich identyfikację, przeciwdziałanie oraz minimalizowanie ich skutków. Wymaga to ścisłej współpracy między członkami sojuszu, a także z partnerami międzynarodowymi, sektorem prywatnym i społeczeństwem obywatelskim. Ataki hybrydowe to strategia, która łączy tradycyjne metody militarne z narzędziami niemilitarnymi, w tym cyberatakami, dezinformacją, propagandą oraz działaniami ekonomicznymi

¹⁴ M. Rühle, *Odstraszanie. Co może sprawić a czego nie?* „Przegląd NATO”, 2015, <https://www.nato.int/docu/review/pl/articles/2022/12/30/odstraszanie-co-moze-sprawic-a-czego-nie/index.html> [dostęp: 01.06.2024]

¹⁵ Z. Śliwa, S. Wojciechowski, *Odstraszanie militarne oraz odporność strategiczna państw w rejonie północno-wschodniej flanki NATO*, „Roczniki Nauk Społecznych”, nr 2/2021, s. 76.

¹⁶ W. Lorenz, *Wysunięta obrona - nowe podejście do polityki obrony i odstraszania NATO*, „PISM Policy Paper”, nr 2(210), 2022, s. 5.

i politycznymi. Głównym celem tych działań jest destabilizacja państwa i jego struktur, podważenie zaufania publicznego do instytucji demokratycznych oraz osłabienie przeciwnika na różnych poziomach – lokalnym, regionalnym, państwowym czy instytucjonalnym¹⁷. Działania hybrydowe są wykorzystywane do zacierania granic między wojną a pokojem i próbują zasiać wątpliwości w społeczeństwie¹⁸. Poniżej w tabeli 1 przedstawiono potencjalne zdolności NATO do zwalczania zagrożeń hybrydowych.

Tabela 1. Zdolności NATO do zwalczania zagrożeń hybrydowych.

Zdolność	Opis
Obrona Cybernetyczna	Ochrona sieci NATO, poprawa odporności na cyberataki i wzmocnienie zdolności obrony cybernetycznej.
Wymiana wywiadowcza	Wymiana informacji wywiadowczych między państwami członkowskimi w celu zwiększenia świadomości sytuacyjnej i wczesnego ostrzeżenia o zagrożeniach hybrydowych.
Komunikacja Strategiczna	Zarządzanie informacjami i przeciwdziałanie dezinformacji poprzez skoordynowane strategie komunikacyjne.
Siły Szybkiego Reagowania	Wysyłanie sił szybkiego reagowania w celu szybkiego i skutecznego reagowania na zagrożenia hybrydowe.
Kontrterroryzm	Zapobieganie i reagowanie na działania terrorystyczne jako część szerszej strategii zwalczania zagrożeń hybrydowych.
Innowacje w Obronie	Wdrażanie innowacji w technologii obronnej, aby być krok przed nowymi taktykami zagrożeń hybrydowych.
Ramowe Struktury Prawne i Polityczne	Opracowywanie ram prawnych i politycznych, aby sprostać złożonościom wojny hybrydowej.
Współpraca międzynarodowa	Współpraca z organizacjami międzynarodowymi i państwami niebędącymi członkami NATO w celu wzmocnienia zbiorowego bezpieczeństwa.

Źródło: opracowanie własne.

NATO wykorzystuje te zdolności w sposób zintegrowany, aby przeciwdziałać różnym formom zagrożeń hybrydowych i chronić swoich członków przed ich skutkami. Jak wynika z powyższej tabeli jednym z elementów jest zdolność do szybkiego reagowania poprzez skuteczne funkcjonowanie systemu zarządzania kryzysowego.

Zarządzanie kryzysowe NATO odgrywa kluczową rolę w przeciwdziałaniu zagrożeniom hybrydowym. NATO, poprzez swoje struktury i procedury za-

¹⁷ Zagrożenia hybrydowe – współczesne formy wywierania nacisku politycznego, Polska Platforma Bezpieczeństwa Wewnętrznego, <https://ppbw.pl/zagrozenia-hybrydowe-wspolczesne-formy-wywierania-nacisku-politycznego/> [dostęp: 01.06.2024]

¹⁸ M. Chudoba, *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej*, „Studia Bezpieczeństwa Narodowego”, Zeszyt 29, 2023, s. 126.

zarządzania kryzysowego, może skutecznie reagować na różnorodne wyzwania związane z zagrożeniami hybrydowymi. Poniżej w tabeli 2 przedstawiono elementy zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych.

Tabela 2. Elementy zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych.

Aspekt	Opis
System wczesnego ostrzegania i monitorowania	Wykorzystanie zaawansowanych systemów wywiadowczych i nadzoru do wczesnego wykrywania potencjalnych zagrożeń hybrydowych.
Koordinacja międzysojusznicza	Ścisła współpraca między państwami członkowskimi NATO, koordynacja działań i wymiana informacji.
Zintegrowane planowanie i ćwiczenia	Regularne ćwiczenia symulujące scenariusze hybrydowe, zintegrowane planowanie obejmujące aspekty militarne i cywilne.
Szybkie Siły Reagowania	Dysponowanie Siłami Odpowiedzi zdolnymi do szybkiego rozmieszczenia w przypadku kryzysu.
Wzmocnienie cyberobrony	Zwiększanie zdolności w zakresie cyberobrony, współpraca z sektorem prywatnym i partnerami międzynarodowymi.
Strategiczna komunikacja	Prowadzenie skoordynowanych kampanii informacyjnych, przeciwdziałanie dezinformacji i propagandzie.
Wsparcie dla państw członkowskich	Wsparcie techniczne i doradcze dla państw członkowskich, szkolenia, wsparcie w zakresie infrastruktury krytycznej.

Źródło: opracowanie własne.

Rozwiązania polityczne i strategiczne w zakresie zwalczania wojny hybrydowej często obejmują skomplikowany zestaw działań, które uwzględniają nie tylko aspekty militarno-bezpieczeństwa, ale także kwestie informacyjne, kognitywne i społeczne¹⁹. Pomimo że wiele z tych rozwiązań koncentruje się na wykrywaniu, powstrzymywaniu, przeciwdziałaniu i reagowaniu na zagrożenia hybrydowe, istotną kwestią jest także budowanie zaufania społecznego i prawdziwej informacji jako kontrastu dla dezinformacji i manipulacji²⁰.

Działania hybrydowe to nie tylko działania militarne, ale także szeroko zakrojone kampanie informacyjne, propagandowe i wpływu społecznego. W tej dziedzinie budowanie zaufania jest kluczowe. Bez rzetelnych informacji i zaufania społecznego, działania mające na celu przeciwdziałanie zagrożeniom

¹⁹ L. Elak, P. Ochyra, S. Żurawski, *Działania militarne i niemilitarne w zwalczaniu zagrożeń hybrydowych*, [w:] *Odporność społeczeństwa, państwa na zagrożenia hybrydowe*, red. L. Elak, T. Zieliński, Z. Ciekanowski, S. Żurawski, Wydawnictwo im. prof. Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie, Warszawa 2023, s. 278.

²⁰ A. Bilal, *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie” jako antidotum*, „NATO Review”, 2021, <https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html> [dostęp: 01.06.2024]

hybrydowym mogą być nieskuteczne lub wręcz przyczynić się do eskalacji konfliktu.

W kontekście zarządzania kryzysowego, NATO działa na wielu płaszczyznach. Opracowuje strategie, procedury i mechanizmy reagowania na różnorodne sytuacje kryzysowe, włączając w to zagrożenia hybrydowe. Istnieje współpraca i wymiana informacji pomiędzy państwami członkowskimi oraz partnerami, co umożliwia szybką reakcję na kryzysy i podejmowanie wspólnych działań. Ponadto NATO prowadzi działania na rzecz zwiększania odporności swoich członków na zagrożenia hybrydowe poprzez szkolenia, wymianę najlepszych praktyk oraz rozwój zdolności obronnych, w tym cyberobrony i obrony informacyjnej.

Podsumowanie

Proces rozwijania zdolności systemu zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych jest krytycznym elementem adaptacji sojuszu do nowych realiów bezpieczeństwa. Poprzez podejmowane działania, NATO skutecznie ulepsza swoje zdolności do reagowania na złożone i zmienne wyzwania, jakie niosą za sobą działania hybrydowe. W ostatnich latach NATO dokonało znacznego postępu w rozwijaniu zdolności zarządzania kryzysowego wobec zagrożeń hybrydowych. Wprowadzenie podejścia wielowymiarowego, obejmującego aspekty militarno-obronne, cywilne oraz inne, było kluczowe dla skutecznego przeciwdziałania temu rodzajowi zagrożeń. Integracja działań informacyjnych, cybernetycznych, gospodarczych i politycznych umożliwiła bardziej kompleksowe podejście do zwalczania hybrydowych zagrożeń.

Efektywna obrona przed zagrożeniami hybrydowymi wymaga ścisłej współpracy między państwami członkowskimi NATO i innymi podmiotami, włączając w to organizacje międzynarodowe, sektor prywatny i społeczeństwo obywatelskie. Ze względu na zmieniającą się naturę zagrożeń hybrydowych, niezbędny jest ciągły rozwój i dostosowanie zdolności NATO do nowych wyzwań. Proces ten powinien być oparty na analizie trendów oraz monitorowaniu ewolucji technologicznej i taktycznej. Kluczowym elementem skutecznego zarządzania kryzysowego wobec zagrożeń hybrydowych jest odpowiednie przygotowanie personelu oraz szkolenia w zakresie identyfikacji, analizy i reagowania na tego rodzaju działania.

Konieczne jest przeprowadzenie szczegółowej analizy skuteczności działań podejmowanych przez NATO w celu zwalczania zagrożeń hybrydowych, aby zidentyfikować obszary wymagające dalszych usprawnień. Ze względu na dynamiczną naturę zagrożeń hybrydowych, istotne jest prowadzenie ciągłych analiz ich ewolucji, w tym identyfikacja nowych technik i narzędzi wykorzystywanych

przez potencjalnych przeciwników. NATO powinno kontynuować budowanie partnerstw z innymi organizacjami międzynarodowymi oraz podmiotami spoza sektora obronnego w celu zwiększenia zdolności do reagowania na zagrożenia hybrydowe, tym samym postawiona hipoteza badawcza została potwierdzona.

Rozwój zdolności zarządzania kryzysowego NATO w kontekście zagrożeń hybrydowych jest kluczowym elementem adaptacji sojuszu do zmieniających się realiów bezpieczeństwa. Dalsze analizy i usprawnienia są niezbędne dla skutecznego przeciwdziałania tym wyzwaniom w przyszłości.

Bibliografia

1. Banasik M., *Zarządzanie kryzysowe NATO mechanizmem zapewniania bezpieczeństwa i ochrony ludności*, „Przedsiębiorczość i Zarządzanie”, Issue 5.3, 2017.
2. Bilal A., *Wojna hybrydowa – nowe zagrożenia, złożoność i „zaufanie” jako antidotum*, „NATO Review”, 2021, <https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html>
3. Brent L., *Rola NATO w cyberprzestrzeni*, „Nato Review”, 2019, <https://www.nato.int/docu/review/pl/articles/2019/02/12/rola-nato-w-cyberprzestrzeni/index.html>
4. Bryjka F., *Przyszłość reagowania kryzysowego w nowej strategii NATO*, „Biuletyn PISM”, nr 118 (2537), 21 lipca 2022 r.
5. Chudoba M., *Zagrożenia hybrydowe – wnioski dla Sił Zbrojnych Rzeczypospolitej Polskiej*, „Studia Bezpieczeństwa Narodowego”, Zeszyt 29, 2023.
6. Z. Ciekanski, *Wsparcie informacyjne systemu zarządzania kryzysowego*, wyd. MANS, Warszawa 2023.
7. Elak L., Ochyra P., Żurawski S., *Działania militarne i niemilitarne w zwalczaniu zagrożeń hybrydowych*, [w:] *Odporność społeczeństwa, państwa na zagrożenia hybrydowe*, red. L. Elak, T. Zieliński, Z. Ciekanski, S. Żurawski, Wydawnictwo im. prof. Leszka J. Krzyżanowskiego Menedżerskiej Akademii Nauk Stosowanych w Warszawie, Warszawa 2023.
8. Gottemoeller R., Hedgecock K., Magula J., Poast P., *Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept*, „Defence Studies”, 22(3), 2022.
9. Kulczycki M., *Rozwój zdolności NATO wobec zagrożeń cybernetycznych*, „Rocznik Bezpieczeństwa Międzynarodowego”, vol. 14, nr 2, 2020.
10. Lorenz W., *Szpica NATO potrzebuje tarczy na wschodniej flance*, „Biuletyn PISM”, nr 15 (1252), 2015.
11. Lorenz W., *Wysunięta obrona – nowe podejście do polityki obrony i odstraszania NATO*, „PISM Policy Paper”, nr 2(210), 2022.
12. Rühle M., *Odstraszanie. Co może sprawić a czego nie?* „Przegląd NATO”, 2015, <https://www.nato.int/docu/review/pl/articles/2022/12/30/odstraszanie-co-moze-sprawic-a-czego-nie/index.html>
13. Stocker J., *Deterrence in the 21st century*, 2017, <https://www.japcc.org/deterrence-in-the-21st-century>
14. Śliwa Z., Wojciechowski S., *Odstraszanie militarne oraz odporność strategiczna państw w rejonie północno-wschodniej flanki NATO*, „Roczniki Nauk Społecznych”, nr 2/2021.
15. The Secretary General's Annual Report 2023.

Netografia

1. NATO – Topic: North Atlantic Council (NAC), https://www.nato.int/cps/en/natohq/topics_49763.htm
2. NATO – Temat: Siły Odpowiedzi NATO, https://www.nato.int/cps/en/natolive/topics_49755.htm
3. NATO – Topic: Crisis management, https://www.nato.int/cps/en/natohq/topics_49192.htm
4. Współpraca w ramach NATO, RCB, <https://archiwum.rcb.gov.pl/wspolpraca-w-ramach-nato/>
5. Zagrożenia hybrydowe – współczesne formy wywierania nacisku politycznego, Polska Platforma Bezpieczeństwa Wewnętrznego, <https://ppbw.pl/zagrozenia-hybrydowe-wspolczesne-formy-wywierania-nacisku-politycznego/>