**dr Sławomir Żurawski**
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0001-9527-3391

**dr Zbigniew Skwarek**
Akademia Sztuki Wojennej
ORCID: 0000-0002-9083-4695

**dr Marcin Oskierko**
Państwowa Akademia Nauk Stosowanych w Chełmie
ORCID: 0000-0003-3450-6037

**mgr Łukasz Stelmaszczyk**

Studia Społeczne
ISSN 2081-0008
e-ISNN 2449-9714
str. 33–43

# Bezpieczeństwo Polski w obliczu zagrożeń hybrydowych

## *Poland's security in the face of hybrid threat*

**Streszczenie**

Celem niniejszego artykułu jest identyfikacja i charakterystyka wybranych zagrożeń hybrydowych przez Polskę. W artykule przedstawiono istotę zagrożeń hybrydowych. Kolejno opisano współpracę w zwalczaniu zagrożeń hybrydowych. Następnie opisano bezpieczeństwo Polski w obliczu zagrożeń hybrydowych ze strony Federacji Rosyjskiej. W podsumowaniu wskazano, iż konieczne jest utrzymanie i rozwijanie współpracy z partnerami międzynarodowymi, w tym Unią Europejską, NATO i innymi państwami, aby skutecznie reagować na zmieniające się zagrożenia i zapewnić bezpieczeństwo i stabilność regionu. Mając na uwadze powyższe, sformułowano problem badawczy: Czy państwo polskie jest przygotowane na zwalczanie zagrożeń hybrydowych? W celu odpowiedzi na pytanie problemowe posłużyła krytyczna analiza literatury, analiza aktów prawnych i dokumentów, w tym raportu Najwyższej Izby Kontroli dotyczącym przygotowania państwa na zagrożenia związane z działaniami hybrydowym, a także rzetelnych źródeł internetowych.

**Słowa kluczowe:** bezpieczeństwo, państwo, zagrożenia hybrydowe, współpraca, NATO, Unia Europejska.

**Abstract**

The aim of this article is to identify and characterize selected hybrid threats by Poland. The article presents the essence of hybrid threats. Cooperation in countering hybrid threats was subsequently described. Next, the security of Polish in the face of hybrid threats from the Russian Federation is described. The summary indicates that it is necessary to maintain and develop cooperation with international partners, including the European Union, NATO and other countries, in order to effectively respond to changing threats and ensure the security and stability of the region. With the above in mind, a research problem was formulated: Is the Polish state prepared to combat hybrid threats? In order to answer the problematic question, a critical analysis of the literature, legal acts and documents, including the report of the Supreme Audit Office on the state's preparedness for the threats related to hybrid activities, as well as reliable online sources were used.

**Key words:** security, state, hybrid threats, cooperation, NATO, European Union.

## Wstęp

Bezpieczeństwo Polski w obliczu zagrożeń hybrydowych staje się coraz bardziej istotnym zagadnieniem w kontekście zmieniającego się otoczenia międzynarodowego oraz rozwoju nowych technologii. Współczesne wyzwania bezpieczeństwa nie ograniczają się już jedynie do tradycyjnych zagrożeń militarystycznych, ale obejmują również obszary informacyjne, cybernetyczne, ekonomiczne i polityczne. Zagrożenia hybrydowe stanowią kompleksowe i złożone działania podejmowane przez państwa, organizacje międzynarodowe lub inne podmioty, które wykorzystują różnorodne narzędzia i techniki w celu osiągnięcia swoich celów. Mogą to być działania dezinformacyjne, ataki cybernetyczne, manipulacja polityczna, destabilizacja ekonomiczna czy też agresja militarystyczna, prowadzone w sposób zdecentralizowany i trudny do zidentyfikowania. W obliczu tych zagrożeń Polska staje przed koniecznością wzmocnienia swojej odporności oraz zdolności do skutecznego przeciwdziałania. Działania te wymagają współpracy różnych sektorów społeczeństwa, w tym instytucji rządowych, służb specjalnych, sektora prywatnego, społeczeństwa obywatelskiego oraz partnerów międzynarodowych. Niniejszy artykuł ma na celu przybliżenie analizy zagrożeń hybrydowych dla Polski oraz przedstawienie kierunków działań mających na celu wzmocnienie jej bezpieczeństwa w tym kontekście. Poprzez zrozumienie natury i sposobów działania tych zagrożeń, Polska może skuteczniej zarządzać ryzykiem oraz budować odporność na wszelkie próby destabilizacji czy manipulacji ze strony wrogich aktorów.

## 1. Istota zagrożeń hybrydowych

Wraz z dynamicznym postępem technologicznym, wzrasta poziom i rodzaj zagrożeń, z jakimi państwa i społeczeństwa mają do czynienia. Wojna w XXI wieku nie opiera się nie tylko na wykorzystaniu konwencjonalnych metod. Agresorzy korzystają z działań hybrydowych, łącząc metody militarne i pozamilitarne, co stało się już charakterystyczne dla aktualnego sposobu prowadzenia wojny. Granice między działaniami poniżej progu wojny i wojennymi mocno się zatarły[1]. Przykładów zagrożeń hybrydowych nie trzeba daleko szukać. W ostatnich latach obserwujemy między innymi rosyjską inwazję na Ukrainę, opierającą się na działaniach militarnych, poprzedzonych i wspieranych przez akcje dezinformacyjne i propagandowe[2]. Możliwości prowadzenia działań hybrydowych są praktycznie nieograniczone. Może to być m.in. przestrzeń polityczna, dyplomatyczna, dezinformacyjno-propagandowa, gospodarcza, kulturalna, społeczna oraz humanitarna[3].

Zagrożenia hybrydowe są różnorodne i ciągle się ewoluują. Mogą być prowadzone w różny sposób. Poniżej przedstawiono wybrane sposoby:

- wielowymiarowy – mogą obejmować kilka działań jednocześnie;
- skryty – utrudniający identyfikację przeciwnika i przypisanie odpowiedzialności za nie sprawcy;
- zaplanowany i skoordynowany – często rozłożone są w dłuższym czasie;
- łączący różne środki – wywierania nacisku i uzależnienia od potencjalnego agresora;
- prowadzone bezpośrednio – prowadzone z wykorzystaniem lokalnych podmiotów, organizacji i osób prywatnych, co utrudnia wykrycie i przeciwdziałanie im;
- przy użyciu środków – przy użyciu środków politycznych, ekonomicznych, prawnych, militarnych i społecznych w tym z wykorzystaniem różnego rodzaju kanałów komunikacji społecznej[4].

W chwili obecnej Unia Europejska definiuje zagrożenia hybrydowe jako koncepcję, która: „ma na celu uchwycenie mieszanki konwencjonalnych i niekonwencjonalnych, wojskowych i niemilitarnych, jawnych i tajnych działań, które mogą być wykorzystane w skoordynowany sposób przez podmioty państwowe lub niepaństwowe do osiągnięcia określonych celów, pozostając poniżej progu oficjalnie wypowie-

1 *Zagrożenia hybrydowe – współczesne formy wywierania nacisku politycznego*, Polska Platforma Bezpieczeństwa Wewnętrznego, https://ppbw.pl/pl/zagrozenia-hybrydowe-formy-nacisku/ [dostęp: 20.03.2024]

2 Ibidem.

3 *Hybrydowe zagrożenie (zapis konferencji prasowej)*, https://www.nik.gov.pl/aktualnosci/dzialania-hybrydowe-zagrozenia.html [dostęp: 20.03.2024].

4 *Przygotowanie Państwa na zagrożenia związane z działaniami hybrydowymi*, Informacje o wynikach kontroli, NIK, https://www.nik.gov.pl/kontrole/P/22/029/ [dostęp: 21.03.2024].

dzianej wojny"[5]. Natomiast Sojusz Północnoatlantycki przedstawia je następująco: „zagrożenia hybrydowe łączą środki wojskowe i pozamilitarne, tajne i jawne, w tym dezinformację, ataki cybernetyczne, presję ekonomiczną, rozmieszczanie nieregularnych grup zbrojnych i użycie sił regularnych. Metody hybrydowe są wykorzystywane do zacierania granic między wojną a pokojem i próbują zasiać wątpliwości w umysłach docelowych populacji. Ich celem jest destabilizacja i osłabienie społeczeństw"[6].

Podsumowując, pojęcie zagrożenia hybrydowe używane jest do opisywania szerokiej gamy agresywnych działań o różnych cechach i wykorzystujące różne metody i narzędzia. Z tego względu, należy stwierdzić, że jest to termin niejednoznaczny i może być różnie postrzegany. Priorytetem powinno być zatem dążenie do wyeliminowania takiej rozbieżności oraz do precyzyjnego zdefiniowania tego pojęcia[7].

## 2. Współpraca w zwalczaniu zagrożeń hybrydowych

W ciągu ostatnich pięciu lat, w świetle znanych i pojawiających się wyzwań stojących przed obiema organizacjami, wieloletnie partnerstwo UE–NATO poczyniło bezprecedensowe postępy, wykazując i wzmacniając solidność więzi transatlantyckich. W ciągu ostatniego roku obie organizacje w dalszym ciągu konsolidowały swoje wzajemnie wzmacniające się partnerstwo strategiczne z korzyścią dla wszystkich sojuszników NATO i państw członkowskich UE, mając na celu utrzymanie i promowanie wspólnych wartości i interesów regionu euroatlantyckiego[8].

Od 2016 r. UE ustanowiła szeroki wachlarz środków mających na celu stworzenie całościowej reakcji obejmującej odpowiednie instrumenty i zaangażowane podmioty w celu przeciwdziałania zagrożeniom hybrydowym w coraz większej liczbie obszarów polityk i konsekwentnie dostosowuje je, aby reagować na stale zmieniające się działania związane z zagrożeniami hybrydowymi[9]. Polityka UE przeciwdziałająca zagrożeniom hybrydowym opiera się na czterech kierunkach działania, które przedstawiono poniżej.

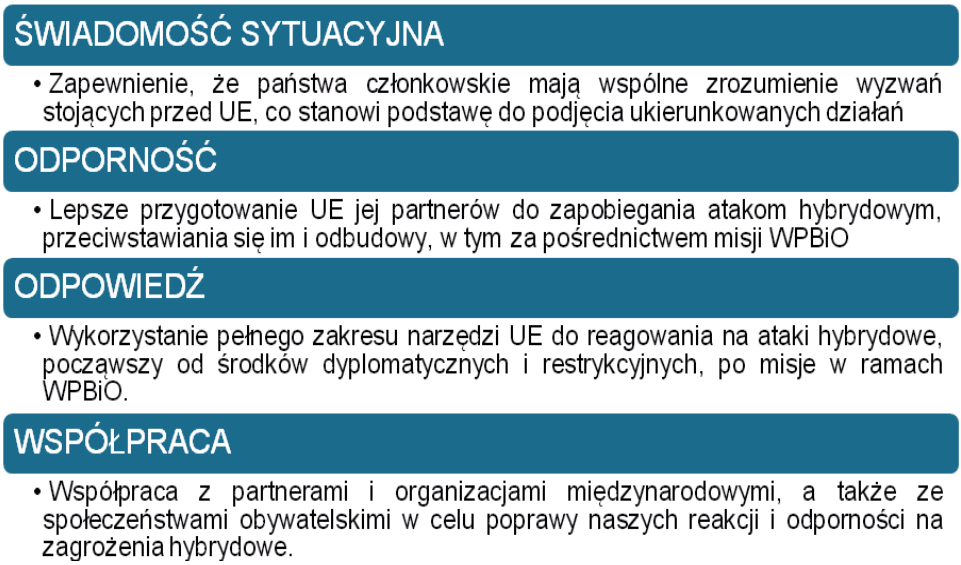
5 *Komisja Europejska*, https://ec.europa.eu/commission/presscorner/home/en [dostęp: 21.03.2024].

6 *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text [dostęp: 21.03.2024].

7 M. Chudoba, Hybrid threats – conclusions for the Polish Armed Forces, „Studia Bezpieczeństwa Narodowego" 29/2023, s. 126.

8 Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 3 June 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf [dostęp: 21.023.2024].

9 *Oint staff working document*, *Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, Brussels, 23.6.2021, SWD (2021) 729 final, https://data.consilium.europa.eu/doc/document/ST-13344-2023-INIT/en/pdf [dostęp: 20.03.2024].




**Rysunek 1. Kierunki działania Polityka UE przeciwdziałania zagrożeniom hybrydowym**

**Źródło:** *Countering hybrid threats*, March 2024, https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en?s=331.

Zagrożenia hybrydowe obejmują szeroki zakres działań podejmowanych przez państwa lub inne podmioty, które łączą tradycyjne metody agresji z nowoczesnymi narzędziami informacyjnymi, cybernetycznymi, ekonomicznymi, czy też wpływem politycznym. Dlatego UE powołała Horyzontalną Grupę Roboczą ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym, która jest instytucją mającą na celu koordynowanie działań oraz opracowywanie strategii dotyczących wzmocnienia odporności społeczeństwa, oraz przeciwdziałania zagrożeniom hybrydowym[10]. Zadania grupy to:

- przeciwdziałanie zagrożeniom hybrydowym,
- zwiększanie odporności państw i społeczeństw na takie zagrożenia,
- poprawa komunikacji strategicznej i przeciwdziałanie dezinformacji.

Grupa robocza zapewnia przekrojowy obraz zagadnień związanych z zagrożeniami hybrydowymi, tak by wspierać spójność i współpracę w UE i między jej państwami członkowskimi. Analizuje warianty i wskazuje narzędzia mogące wzmacniać gotowość i odporność UE i jej państw członkowskich na zagrożenia hybrydowe. Grupa robocza ułatwia koordynację działań Rady w dziedzinie zwalczania zagrożeń hybrydowych, a także w razie potrzeby współpracuje z innymi organami przygotowaw-

10 F. Bryjka, *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych*, w: *Strategic file*, red. S. Dębski, P. Sasnal, W. Lorenz, PISM 9/(117)/2022, https://www.pism.pl/publikacje/rozwoj-unijnych-zdolnosci-do-zwalczania-zagrozen-hybrydowych#_ftn2 [dostęp: 21.03.2024].

czymi. W stosownych przypadkach grupa współdziała też z innymi instytucjami, służbami i agencjami UE[11].

Wymienione obszary współpracy, mają znaczenie w kontekście przeciwdziałania zagrożeniom hybrydowym. Obrany kierunek wydaję się właściwym na drodze do ściślejszej koordynacji dotychczas równoległych wysiłków obu organizacji w tym zakresie[12].

Współpraca między Unią Europejską (UE) a Organizacją Traktatu Północnoatlantyckiego (NATO) w zwalczaniu zagrożeń hybrydowych stanowi kluczowy element skutecznego reagowania na nowe wyzwania bezpieczeństwa. Zarówno UE, jak i NATO rozumieją, że zagrożenia hybrydowe wymagają zintegrowanego podejścia, które obejmuje środki polityczne, wojskowe, cywilne i inne.

Wspólne zrozumienie zagrożeń: Zarówno UE, jak i NATO regularnie prowadzą analizy i oceny zagrożeń hybrydowych, dzieląc się informacjami oraz wspólnie identyfikując kluczowe obszary ryzyka. Ta wspólna diagnoza pozwala na skuteczniejsze planowanie działań prewencyjnych oraz reakcyjnych. Istnieją mechanizmy wymiany informacji między UE a NATO, które umożliwiają szybkie reagowanie na ewentualne zagrożenia hybrydowe. Te mechanizmy obejmują wspólne ćwiczenia, seminaria, spotkania ekspertów oraz regularne raportowanie. Zarówno UE, jak i NATO podejmują działania mające na celu koordynację działań państw członkowskich w zakresie zwalczania zagrożeń hybrydowych. Mogą to być inicjatywy dotyczące zwiększenia świadomości społecznej, wzmocnienia cyberbezpieczeństwa, poprawy zdolności obronnych czy też działań dyplomatycznych.

Organizacje te regularnie organizują wspólne ćwiczenia i szkolenia, które pozwalają na doskonalenie współpracy między nimi oraz podnoszenie zdolności państw członkowskich do skutecznego przeciwdziałania zagrożeniom hybrydowym. Istnieją również struktury instytucjonalne, które umożliwiają regularny dialog i współpracę między UE a NATO, takie jak Wspólna Deklaracja o Współpracy między NATO a UE z 2016 roku czy też Centrum Unii Europejskiej ds. Analiz Strategicznych (EUSC) i Centrum NATO ds. Doskonalenia Analizy Strategicznej (NCIA).

Współpraca między UE a NATO w zwalczaniu zagrożeń hybrydowych jest istotna nie tylko dla bezpieczeństwa państw członkowskich tych organizacji, ale również dla bezpieczeństwa całego obszaru transatlantyckiego i europejskiego. Dzięki wspólnemu podejściu i współdziałaniu państwa te mogą skuteczniej bronić się przed nowymi i złożonymi wyzwaniami bezpieczeństwa, jakimi są zagrożenia hybrydowe.

11 *Horyzontalna Grupa Robocza ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym*, https://www.consilium.europa.eu/pl/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/ [dostęp: 21.023.2024].

12 A. Ignaciuk, *NATO i UE wobec zagrożeń hybrydowych – nowe otwarcie we wzajemnej współpracy?* „Bezpieczeństwo Narodowe" I–IV/2016. s. 98.

## 3. Bezpieczeństwo Polski w obliczu zagrożeń hybrydowych ze strony Federacji Rosyjskiej

Po zakończeniu zimnej wojny ustanowiony w Europie ład bezpieczeństwa opierał się na odrzuceniu stref wpływów oraz uznaniu prawa wszystkich państw do samodzielnego decydowania o kierunkach polityki zagranicznej, w tym o przynależności do sojuszy (NATO) i organizacji integracyjnych (UE). Natomiast Rosja nigdy nie przestała uznawać NATO i Unii Europejskiej za potencjalne zagrożenie, a ich rozszerzenie na wschód w dużym stopniu krzyżowało rewizjonistyczne plany Rosji. Połączenie działań militarnych i niemilitarnych prowadzonych przez reżim W. Putina w skoordynowany sposób przeciwko państwom członkowskim UE oraz Paktu Północnoatlantyckiego (NATO) jest konfliktem trudnym do ujęcia. Zagrożenia hybrydowe stosowane przez Rosję to przeprowadzane ataki cybernetyczne na infrastrukturę krytyczną i jej systemy informacyjne. To również zakłócenia usług krytycznych związane z dostawami energii czy działania ukierunkowane na podważanie zaufania społecznego do instytucji rządowych oraz pogłębiania podziałów społecznych.

M. Menkiszak zidentyfikował następujące cele działań hybrydowych wymierzonych w Polskę, do których należą:

1. Uniemożliwienie użycia sojuszniczych i polskich sił zbrojnych oraz infrastruktury (dróg, linii kolejowych, lotnisk, portów, miejsc postojowych) w działaniach udzielenia pomocy Estonii, Litwie i Łotwie.
2. Zmuszenie Polski do wycofania się z działań sprzecznych z interesami Rosji.
3. Wymuszenie na Polsce umożliwienia organizacji komunikacji lądowej Rosji z Obwodem Kaliningradzkim lub przerwania połączenia lądowego Polski z Litwą.
4. Potencjalnie – zmuszenie do wycofania sił amerykańskich i innych sił NATO z terytorium Polski[13].

Zdaniem A. Dyner do najważniejszych obszarów rosyjskiej aktywności należą wojna informacyjna, cyberataki oraz instrumentalizacja migracji. Szczególną rolę w rosyjskich działaniach dezinformacyjnych odgrywają media społecznościowe. Rozpowszechnianie rosyjskiej dezinformacji odbywa się za sprawą fałszywych kont i grup. Aktywność związaną z rosyjską dezinformacją zwiększają firmy zatrudniające pracowników do rozsiewania w sieci konkretnego rodzaju informacji. Rosyjskie działania skoncentrowane są na kwestiach społecznie i politycznie wrażliwych. Obecnie tematami są rosnąca inflacja oraz bezpieczeństwo energetyczne. W związku z rosnącą inflacją uwypuklany jest fakt udzielania Ukrainie pomocy wojskowej przez państwa UE i NATO oraz w związku z udzielaną pomocą zwiększanie wydatków na obronę przez część członków Sojuszu. W przypadku bezpieczeństwa energetycznego

13 M. Piekarski, *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych*, „Terroryzm - studia, analizy, prewencja" 2022/2/(1), s. 79.

propaganda rosyjska przekonuje, że przez lata Rosja była gwarantem niskich cen energii, a za ich obecny wzrost odpowiedzialne są państwa Unii Europejskie, które wycofały się z dotychczasowej współpracy[14].

W swoich działaniach dezinformacyjnych Rosja próbuje wykorzystywać również obecność uchodźców z Ukrainy w Polsce i na zachodzie Europy, wskazując, że rządy państw przyjmujących skupiają się na pomocy Ukraińcom kosztem własnych obywateli i ich zabezpieczenia zdrowotnego i edukacyjnego. Celem Rosji jest zmniejszanie poczucia bezpieczeństwa mieszkańców państw zachodnich (np. co do dostaw paliw i energii), podważanie ich zaufania do władz krajowych, UE oraz NATO, a także zwiększanie polaryzacji społecznej – np. w sprawach związanych z ochroną zdrowia[15].

Oprócz prowadzonych przez Rosję działań dezinformacyjnych dokonywane stale dokonywane są ataki sabotażowe i w cyberprzestrzeni. Wymierzone są one w funkcjonowanie infrastruktury krytycznej (elektrownie, sieci przesyłowe, koleje) państw NATO i UE. Opracowany przez Microsoft raport stwierdził w okresie od lutego do maja 2022 r. przeprowadzenie przez Rosję masowych cyberataków. Ataki przeprowadzone zostały w 42 państwach (poza Ukrainą), a ich głównym celem w 49% były agencje rządowe, w 19 % instytucje zarządzające infrastrukturą krytyczną. Najczęściej atakowana była Polska (8% przypadków) oraz państwa bałtyckie (w sumie 14%)[16].

Rosja, dokonując 24 lutego 2022 r. pełnoskalowej agresji na Ukrainę, dążyła do jej całkowitego podporządkowania[17]. Rosyjska agresja nie stanowiła tylko ataku na Ukrainę, ale na cały porządek międzynarodowy, którego podstawą jest prawo i uzgodnione normy oraz stanowiła zagrożenie dla interesów państw broniących międzynarodowego systemu opartego na sile prawa, a nie prawie siły. Tworząc strategiczne i militarne zagrożenie zarówno dla państw Europy środkowo -wschodniej oraz całego NATO i UE[18].

Rosyjska agresja przeciwko Ukrainie naruszyła wynikający z Karty Narodów Zjednoczonych zakaz użycia siły oraz stanowiła „pogwałcenie suwerenności, niezależności politycznej i integralności terytorialnej Ukrainy". W związku z powyższym Sejm RP uznał Federację Rosyjską za państwo wspierające terroryzm i stosujące środki terroru". Zdaniem polskiego parlamentu Rosja regularnie naruszała prawa człowieka, prawo międzynarodowe oraz Kartę Narodów Zjednoczonych oraz szereg innych zo-

14 A.M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE*, Polski Instytut Spraw Międzynarodowych, „Biuletyn PISM" 183/(2602)/2022, s. 1.
15 Ibidem, s. 1.
16 Ibidem, s. 1-2.
17 W. Lorenz, *Bezpieczeństwo europejskie – przeciw Rosji, a nie z Rosją,* w: *Bez powrotu? Transformacja ładu międzynarodowego po inwazji Rosji na Ukrainę,* red. M. Terlikowski, Raport PISM, Polski Instytut Spraw Międzynarodowych, Warszawa 2023, s. 7.
18 Ibidem, s. 8.

bowiązań, dokonując aneksji terytoriów innych państw, napaści zbrojnych, zbrodni wojennych i ludobójstw. Podejmowała wrogie działania gospodarcze, w szczególności w sferze energetyki"[19] oraz bezpośrednio odpowiedzialna jest za zestrzelenie w lipcu 2014 r. samolotu malezyjskich linii lotniczych (lot MH17), w którym zginęło 298 osób (pasażerów i członków załogi).

Przeprowadzane przez Rosyjskie wojsko na terytorium Ukrainy ataki przyczyniły się do śmierci tysięcy ludzi, w tym dzieci. Rosyjska Grupa Wagnera oraz czeczeńskie oddziały bojowe podległe Ramzanowi Kadyrowi dokonywały zbiorowych egzekucji oraz dopuszczały się uprowadzeń, przemocy seksualnej i tortur, zaś rosyjskie wojsko przeprowadzało ataki wymierzone w infrastrukturę cywilną oraz akty terroru odrywania dzieci od rodzin celem poddania ich rusyfikacji, masowych deportacji ludności, przymusowego poboru obywateli Ukrainy do rosyjskich sił zbrojnych oraz rabunku mienia. Ponadto Federacja Rosyjska powszechnie łamała konwencję genewską o traktowaniu jeńców wojennych oraz dopuszczała się aktu piractwa międzynarodowego, dokonując blokad ukraińskich portów, a także paraliżując komunikację na morskich szlakach, uniemożliwiając Ukrainie eksport płodów rolnych do państw Afryki i Azji[20].

W rezolucji Parlament Europejski stwierdził, że Rosja od lat inicjowała akty terrorystyczne oraz wspierała i finansowała reżimy terrorystyczne dostarczając broń reżimowi al-Asada i atakując cywilów w Syrii przeprowadzając celowe ataki na pokojowe miasta, infrastrukturę cywilną, targi, placówki medyczne oraz szkoły. Ponadto Federacja Rosyjska powszechnie stosowała terror wobec ludności cywilnej w Sudanie, Libii, Republice Środkowoafrykańskiej i Mali, korzystając z usług prywatnych najemników grupy Wagnera[21].

Zgodnie z rezolucją Federacja Rosyjska nieustannie dopuszcza się systemowych aktów terroryzmu: politycznie zabójstwa i próby zabójstw, zatruć opozycjonistów, dziennikarzy, działaczy i przywódców zagranicznych. Ofiarami reżimu Putina są przeciwnicy w Rosji i za granicą, a ofiarami takich działań byli m.in. Wiktor Juszczenko, Aleksander Litwinienko, Aleksiej Nawalny Borys Niemcow, Anna Politkowska, Siergiej Protazanow, Siergiej i Julia Skripal[22]. Polska jako państwo członkowskie UE oraz Paktu Północnoatlantyckiego, mocno zaangażowana jest w pomoc Ukra-

19 *Uchwała Sejmu ws. agresji Federacji Rosyjskiej na Ukrainę. „Atak na cały porządek międzynarodowy",* Druk nr 2048 Przedstawiony przez Prezydium Sejmu projekt oświadczenia Sejmu Rzeczypospolitej Polskiej w sprawie agresji Federacji Rosyjskiej na Ukrainę, Sejm Rzeczypospolitej Polskiej, Warszawa 2022.

20 Ibidem.

21 *Resolution on recognising the Russian Federation as a state sponsor of terrorism,* 2022/2896(RSP), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/2896(RSP), [dostęp: 21.03.2024].

22 Ibidem.

inie, udostępniając tranzyt amunicji i sprzętu wojskowego przez terytorium państwa oraz pomoc humanitarną udzielaną uchodźcom z Ukrainy na terytorium Polski, stając się przy tym jednym z wrogich państw Rosji.

## Podsumowanie

W obliczu zagrożeń hybrydowych, bezpieczeństwo Polski staje przed nowymi wyzwaniami, które wymagają skoordynowanego i zintegrowanego podejścia. Analiza tych zagrożeń pokazuje, że są one złożone i dynamiczne, obejmując różnorodne obszary, takie jak cyberprzestrzeń, informacja, polityka oraz gospodarka. Wdrażanie działań mających na celu wzmocnienie odporności Polski na zagrożenia hybrydowe wymaga zaangażowania wielu sektorów społeczeństwa, w tym rządu, służb specjalnych, sektora prywatnego oraz społeczeństwa obywatelskiego. Konieczne jest również budowanie partnerstw zarówno na poziomie krajowym, jak i międzynarodowym, aby efektywnie przeciwdziałać tym zagrożeniom. Podsumowując, Polska musi kontynuować prace nad doskonaleniem swoich zdolności obronnych, w tym w obszarze cyberbezpieczeństwa, zarządzania kryzysowego oraz świadomości społecznej. Jednocześnie konieczne jest utrzymanie i rozwijanie współpracy z partnerami międzynarodowymi, w tym Unią Europejską, NATO i innymi państwami, aby skutecznie reagować na zmieniające się zagrożenia i zapewnić bezpieczeństwo i stabilność regionu.

## Bibliografia

### Literatura


1. Chudoba M., *Hybrid threats – conclusions for the Polish Armed Forces*„Studia Bezpieczęństwa Narodowego", 29/2023.
2. Dyner A.M., *Działania hybrydowe Rosji przeciw państwom NATO i UE*, Polski Instytut Spraw Międzynarodowych, „Biuletyn PISM" 83/(2602)/2022.
3. Ignaciuk A., *NATO i UE wobec zagrożeń hybrydowych – nowe otwarcie we wzajemnej współpracy?* „Bezpieczeństwo Narodowe" I-IV/2016.
4. Lorenz W., *Bezpieczeństwo europejskie – przeciw Rosji, a nie z Rosją*, w: *Bez powrotu? Transformacja ładu międzynarodowego po inwazji Rosji na Ukrainę,* red. M. Terlikowski, Raport PISM, Polski Instytut Spraw Międzynarodowych, Warszawa 2023.
5. Piekarski M., *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych*, „Terroryzm - studia, analizy, prewencja" 2/(1)/2022.
6. Uchwała Sejmu ws. agresji Federacji Rosyjskiej na Ukrainę. „Atak na cały porządek międzynarodowy", Druk nr 2048 Przedstawiony przez Prezydium Sejmu projekt oświadczenia Sejmu Rzeczypospolitej Polskiej w sprawie agresji Federacji Rosyjskiej na Ukrainę, Sejm Rzeczypospolitej Polskiej, Warszawa 2022.


### Netografia


1. *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm#:~:text.

2. *Horyzontalna Grupa Robocza ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym*, https://www.consilium.europa.eu/pl/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/.
3. https://ec.europa.eu/commission/presscorner/home/en.
4. *Hybrydowe zagrożenie* (zapis konferencji prasowej), https://www.nik.gov.pl/aktualnosci/dzialania- Bryjka F., *Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych,* w: *Strategic file*, red. S. Dębski, P. Sasnal, W. Lorenz, „PISM" 9/(117)/2022, https://www.pism.pl/publikacje/rozwoj-unijnych-zdolnosci-do-zwalczania-zagrozen-hybrydowych#_ftn2_hybrydowe-zagrozenia.html.
5. *Oint staff working document*, *Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, Brussels, 23.6.2021, SWD (2021) 729 final, https://data.consilium.europa.eu/doc/document/ST-13344-2023-INIT/en/pdf.
6. *Przygotowanie Państwa na zagrożenia związane z działaniami hybrydowymi*, Informacje o wynikach kontroli, NIK, https://www.nik.gov.pl/kontrole/P/22/029/.
7. *Resolution on recognising the Russian Federation as a state sponsor of terrorism*, 2022/2896(RSP), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2022/2896(RSP).
8. *Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 3 June 2021*, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf.
9. *Zagrożenia hybrydowe – współczesne formy wywierania nacisku politycznego*, Polska Platforma Bezpieczeństwa Wewnętrznego, https://ppbw.pl/pl/zagrozenia-hybrydowe-formy-nacisku/.