ROCZNIKI NAUK SPOŁECZNYCH
Tom 14(50), numer 4 – 2022
DOI: https://doi.org/10.18290/rns22504.10

TOMASZ NOWAK

# BUDOWA ODPORNOŚCI NA OBECNE I PRZYSZŁE ZAGROŻENIA O CHARAKTERZE HYBRYDOWYM. REKOMENDACJE DLA POLSKI

## BUILDING RESILIENCE TO CURRENT AND FUTURE HYBRID THREATS. RECOMMENDATIONS FOR POLAND

A b s t r a c t. The contents of the article focuses on the problem of building resilience, which is a key element of state security. It is the basis of deterrence and defense, and therefore allows you to effectively counter threats. The aim of the article was to identify the current and future hybrid threats created by Russia and Belarus, as well as to present guidance and recommendations for Poland in the field of strengthening resilience to these threats. In view of the changes in the security architecture in Poland's neighborhood resulting from Russia's neo-imperial policy and Belarus, which is under its influence, the issues raised constitute an added value. In the research process, general methods of scientific cognition were used, which were based mainly on the analysis and criticism of literature, inference and own assessment of facts.

**Keywords:** Poland's security; resilience; threat; hybrid threat; Russian Federation.

## WPROWADZENIE

Współczesne zagrożenia dla bezpieczeństwa państwa w zasadniczy sposób różnią się od zagrożeń dominujących jeszcze pół wieku temu. Eskalacja konfliktów wykracza poza tradycyjne pole walki. Następuje wzrost znaczenia niemilitarnych środków i metod oddziaływania. W sposobach prowadzenia walki zaczynają dominować aspekty informacyjne, gospodarcze i ideologiczne. Do realizacji celów politycznych wykorzystuje się szantaże ekonomiczne, kampanie dezinformacyjne, kryzysy energetyczne. Informacja staje się przekonującym narzędziem walki w cyberprzestrzeni. Społeczeństwa są manipulowane, przez

Mgr TOMASZ NOWAK – Uniwersytet Jana Kochanowskiego w Kielcach, Wydział Prawa i Nauk Społecznych, Instytut Nauk o Bezpieczeństwie; adres do korespondencji: ul. Uniwersytecka 15, 25-406 Kielce; e-mail: tk.nowak@wp.pl; ORCID: https://orcid.org/0000-0003-4144-0937.

co zachodzą trudności w odróżnieniu prawdy od fałszu. Ład oparty na prawie międzynarodowym podlega kolejnym wstrząsom. Nawiązując do tytułu jednego z dzieł wybitnego socjologa Immanuela Wallersteina można stwierdzić, że następuje „koniec świata jaki znamy" (Wallerstein, 2004).

Zachodzące zmiany w globalnym środowisku bezpieczeństwa i niestabilne sąsiedztwo wschodniej flanki NATO implikują potrzebę ponownego przejrzenia i skorygowania obowiązujących do tej pory koncepcji, planów, poglądów. Dotyczy to również sfery pojęciowej. W warunkach globalizacji gwałtowne konflikty przybrały nowy wymiar (Kaldor, 2013, s. 2-8). Oprócz zagrożenia konwencjonalnego, pojawia się zagrożenie w postaci wojny hybrydowej[1]. Rosja przekształciła obszar Europy Wschodniej w „szarą strefę bezpieczeństwa" i czyni starania o wciągnięcie w nią państw położonych w bezpośredniej bliskości, m.in. Polski.

Obecnie głównym źródłem zagrożeń dla bezpieczeństwa Polski jest imperialna polityka Rosji realizowana poprzez walkę polityczno-gospodarczo-ideologiczną z Zachodem. Rosja destabilizuje regionalne i globalne bezpieczeństwo i poszerza swoje strefy wpływów używając siły militarnej. Drugie źródło zagrożeń dla bezpieczeństwa europejskiego, w tym bezpośrednio dla Polski generuje nieprzewidywalność działań Białorusi. W kooperacji z reżimem Alaksandra Łukaszenki Rosja wykorzystuje terytorium Białorusi i intensyfikuje serię destrukcyjnych, nieodpowiedzialnych posunięć. Od naruszeń przestrzeni powietrznej i morskiej państw członkowskich NATO przez wywoływanie kryzysów migracyjnych i uchodźczych aż do szeroko zakrojonych ćwiczeń i manewrów o charakterze ofensywnym i jądrowym.

Podstawowym warunkiem bezpieczeństwa w wymiarze krajowym, unijnym i sojuszniczym jest budowa odporności, rozumiana jako „utrzymywanie i rozwijanie takich zdolności w sferze cywilnej i wojskowej, które znacząco utrudnią nieprzyjazne działania" (Rey, 2022). W ujęciu NATO odporność to „zdolność społeczeństwa do przeciwstawienia się wstrząsom (np. klęska żywiołowa, awaria infrastruktury krytycznej, atak hybrydowy lub zbrojny) i odbudowy,

[1] W naukach o bezpieczeństwie dotychczas nie ma powszechnie uznanej i jednoznacznej definicji wojny hybrydowej. Najczęściej w opracowaniach przywołuje się interpretacje F.G. Hoffmana, J.J. McCuena i W.J. Nemetha, z których można wywnioskować, że wojna hybrydowa to połączenie i stosowanie konwencjonalnych i niekonwencjonalnych metod oraz narzędzi walki. Na potrzeby artykułu przyjęto, że wojna hybrydowa to „wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp.". Zob. *(Mini)Słownik BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa* (2015), https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 20.05.2022].

która łączy w sobie gotowość cywilną i potencjał wojskowy" (*Resilience, Civil Preparedness and Article 3*, 2022). Wzmacnianie odporności należy postrzegać zarówno jako fundamentalne zadanie każdego państwa, jak i obowiązek wynikający z przynależności do struktur i zasad określonych w UE i NATO. Uzyskanie pełnej synergii w działaniach nie jest możliwe bez integracji w trzech domenach. Pierwsza dotyczy sektora publicznego (chodzi o współdziałanie cywilno-wojskowe), druga to partnerstwo publiczno-prywatne (zaangażowanie podmiotów prywatnych w możliwość wsparcia sił zbrojnych), trzecią stanowi społeczeństwo (odporne społeczeństwo to społeczeństwo świadome zagrożeń i posiadające umiejętność właściwej reakcji) (Rey, 2022). Integracja wskazanych domen sprawia, że państwo jest mniej podatne na zagrożenia, zmniejsza swoje słabe strony, stając się trudniejszym celem dla potencjalnego agresora. Warto pamiętać, że odporność kraju na agresję jest istotnym elementem polityki odstraszania i obrony (Śliwa, Wojciechowski, 2021, s. 73-83; Koziej, 2016, s. 84).

Na szczycie NATO w Warszawie w 2016 roku przywódcy państw członkowskich Sojuszu Północnoatlantyckiego zgodzili się na przyjęcie „Baseline Requirements National Resilience". Zgodnie z tą koncepcją wzmacnianie narodowej odporności dokonuje się poprzez dążenie do realizacji siedmiu podstawowych wymogów (*Resilience through Civil Preparedness*, 2019), takich jak: gwarancja ciągłości rządów i najważniejszych usług rządowych, odporność dostaw energii, zdolność do skutecznego radzenia się z niekontrolowanym przemieszczaniem osób, odporność zasobów żywności i wody, zdolność do radzenia sobie z dużą liczbą ofiar, odporność cywilnych systemów łączności i systemów transportu[2]. Charakterystykę podejścia NATO do wskazanych obszarów przedstawiono w tabeli 1.

[2] Ponadto w 2021 roku sojusznicy w ramach NATO 2030 zgodzili się zintensyfikować wysiłki na rzecz: zabezpieczenia i dywersyfikacji łańcuchów dostaw, zapewnienia odporności infrastruktury krytycznej (lądowej, morskiej, kosmicznej, cyberprzestrzeni) i kluczowych gałęzi przemysłu, w tym poprzez ochronę przed szkodliwą działalnością gospodarczą oraz wpływu zagrożeń naturalnych, które nasilają się w wyniku zmian klimatu. Zob. *Strengthened Resilience Commitment* (2021), https://www.nato.int/cps/en/natohq/official_texts_185340.htm [dostęp: 20.05.2022].

Tabela 1. Obszary odporności państwa
zgodnie z „NATO Baseline Requirements National Resilience"

| Obszar odporności | Charakterystyka |
|---|---|
| 1. Assured continuity of government and critical government services | Gwarancja ciągłości rządów oraz najważniejszych usług rządowych (np. zdolność do podejmowania decyzji, ich komunikowania i egzekwowania w sytuacjach kryzysowych). |
| 2. Resilient energy supplies | Dostatecznie zabezpieczone dostawy energii (posiadanie planów awaryjnych oraz odpowiednio zabezpieczonych sieci elektroenergetycznych wewnętrznych i transgranicznych). |
| 3. Ability to deal effectively with uncontrolled movement of people | Zdolność do skutecznego rozwiązywania problemów związanych z niekontrolowanym przemieszczaniem się ludzi (działania na rzecz ochrony granic obszaru traktatowego, w tym rozwiązywanie konfliktów związanych z rozmieszczeniem personelu NATO). |
| 4. Resilient food and water resources | Dostatecznie zabezpieczone zapasy żywności i wody (zapewnienie dostaw i zabezpieczenie ich przed wszelkimi zakłóceniami lub sabotażem). |
| 5. Ability to deal with mass casualties and disruptive health crises | Zdolność do radzenia sobie z dużą liczbą ofiar i destrukcyjnymi kryzysami zdrowotnymi (utrzymanie cywilnych systemów opieki zdrowotnej odpornych na sytuacje kryzysowe i zabezpieczenie wystarczającej ilości środków i sprzętu medycznego). |
| 6. Resilient civil communications systems | Odporne cywilne systemy łączności (zapewnienie funkcjonowania sieci telekomunikacyjnych i sieci cybernetycznych w warunkach kryzysu z utrzymaniem zdolności rezerwowych, niezawodność systemów łączności, w tym sieci 5G). |
| 7. Resilient transport systems | Odporne systemy transportu (zdolność sił NATO do szybkiego przemieszczania się po terytorium państw Sojuszu, w tym utrzymanie możliwości sprawnego poruszania dla służb cywilnych także w sytuacjach kryzysowych). |

Źródło: Opracowanie własne na podstawie: *Resilience, Civil Preparedness and Article 3* (2022), https://www.nato.int/cps/en/natohq/topics_132722.htm [dostęp: 20.05.2022].

Według Jamie Shea (Shea, 2016) przyjęte obszary mają zastosowanie do całego spektrum kryzysów, od ewoluującego zagrożenia o charakterze hybrydowym, po najbardziej wymagające scenariusze, które zostały opracowane przez planistów w ramach procesów planowania obronnego (Roepke, Thankey, 2019).

Budując odporność na zagrożenia hybrydowe, działania Polski powinny charakteryzować się kompleksowym, wielowymiarowym podejściem w wymiarze wewnętrznym i zewnętrznym. Wyciągając wnioski i doświadczenia z obecnych

kryzysów[3] przy wschodniej granicy, należy podejmować nieustannie wysiłki na rzecz zapobiegania zagrożeniom i przygotowania do późniejszego reagowania. Zaniedbanie lub słabość tych elementów ograniczy bądź w niesprzyjających okolicznościach uniemożliwi realizację bezpośrednich działań służących zahamowaniu lub zwalczeniu występujących zagrożeń.

Prowadząc aktywne działania w wymiarze wewnętrznym i zewnętrznym, należy dążyć do identyfikacji zagrożeń i redukcji prawdopodobieństwa ich wystąpienia. Priorytetem jest m.in. monitorowanie, analiza i ocena źródeł i symptomów potencjalnych zagrożeń, przygotowanie instrumentów prawnych, systemów zabezpieczeń, szkolenie podmiotów wchodzących w skład systemu bezpieczeństwa państwa, edukacja dla bezpieczeństwa. W przygotowaniu do działań związanych z reagowaniem fundamentalne znaczenie przypisuje się opracowaniu scenariuszy i procedur działań, w tym planów ochrony ludności i obrony cywilnej, właściwej organizacji systemów monitorowania, ostrzegania i alarmowania, łączności i komunikacji, a także informowaniu ludności o zagrożeniu.

Co istotne, strategia przeciwdziałania atakom hybrydowym musi zostać zbudowana w taki sposób, aby potencjalny agresor był świadomy, że poniesie dotkliwe konsekwencje, że straty będą niewspółmierne do osiągniętych korzyści (*deterrence by punishment*). Podejmując wysiłki na rzecz zapewnienia bezpieczeństwa, dąży się przede wszystkim do ochrony istotnych dla narodu wartości takich, jak przetrwanie, integralność terytorialna, niezależność polityczna, jakość życia, wzrost siły państwa i pozycji międzynarodowej. W tym celu państwo wykorzystuje posiadane zasoby i instrumenty polityczne, ekonomiczne, wojskowe, ideologiczne, kulturowe i społeczne.

Tak identyfikowana sytuacja problemowa prowadzi do sformułowania głównego problemu badawczego, który brzmi: *Jakie działania powinna podjąć Polska w celu wzmacniania odporności na zagrożenia o charakterze hybrydowym?* Aby rozwiązać główny problem badawczy, określono problemy szczegółowe, które przyjęły formę następujących pytań badawczych: 1) *Czym są zagrożenia hybrydowe i jakie jest ich źródło?* 2) *Jakie przedsięwzięcia powinna podjąć Polska w wymiarze polityczno-militarnym?* 3) *W jaki sposób Polska powinna wzmacniać odporność w wymiarze gospodarczo-energetycznym?* 4) *Jakie czynności powinna podjąć Polska w wymiarze informacyjnym?* 5) *Jakie przedsięwzięcia powinna podjąć Polska w wymiarze społecznym?*

[3] Kryzys polityczno-militarny na Ukrainie trwający od 2013 roku, który przekształcił się w 2022 roku w wojnę na pełną skalę i wygenerował największy kryzys uchodźczy w Europie od zakończenia II wojny światowej. Kolejny przykład to kryzys migracyjny wywołany w sposób celowy przez Białoruś, który zaczął się w maju 2021 roku przy granicy z Polską, Litwą i Łotwą.

Celem badań była identyfikacja obecnych i przyszłych zagrożeń hybrydowych kreowanych przez Rosję i Białoruś, a także sformułowanie zaleceń i rekomendacji dla Polski w zakresie wzmacniania odporności na zagrożenia hybrydowe. Biorąc pod uwagę uwarunkowania bezpieczeństwa Polski, istotne wydaje się przedstawienie rekomendacji w domenie politycznej, militarnej, gospodarczej, energetycznej, informacyjnej i społecznej.

## 1. ISTOTA I ŹRÓDŁO ZAGROŻEŃ HYBRYDOWYCH

Przyjmując leksykalne rozumienie można stwierdzić, że zagrożenie to: ktoś lub coś powodujące poczucie niepewności, strachu, obawy, braku spokoju o najważniejsze wartości odnoszące się do bezpieczeństwa (żywotnie ważne, egzystencjalne). Według autorów *Słownika terminów z zakresu bezpieczeństwa narodowego* (2009, s. 162) zagrożenie to „sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia". Współcześnie wyodrębnił się nowy rodzaj zagrożenia, z jednej strony szczególnie widoczny w dyskursie politycznym i coraz częściej powielany w mediach, ale z drugiej niewystarczająco zbadany – zagrożenie hybrydowe. Mimo że zagrożenie hybrydowe jest postrzegane przez część zachodnich ekspertów jako *novum*, to – jak zostało wykazane poniżej – zagrożenie stanowi konglomerat wcześniej znanych i obecnie rozwijanych metod destrukcyjnych.

Podjęcie badań nad działaniami hybrydowymi w konfliktach zbrojnych pojawiło się stosunkowo niedawno w Stanach Zjednoczonych Ameryki. Przykładem są prace m.in. Williama Nemetha (w 2002 roku dokonał analizy sposobu walki Czeczenów w wojnie z Rosją), Franka Hoffmana (w 2007 roku zbadał konflikty XXI wieku z naciskiem na klasyczne wykorzystanie działań hybrydowych w wojnie między Izraelem a Hezbollahem). Dzisiaj można postawić tezę, iż pojęcie „hybrydowość" nie tylko upowszechniło się w związku z wydarzeniami na Ukrainie, ale zostało już *de facto* przypisane do prowadzonej przez Rosję wojny przeciwko Ukrainie. Przegląd wybranych definicji zagrożenia hybrydowego ukazano w tabeli 2. Interpretacje są do siebie zbliżone i jednoznacznie wykazują, że specyfiką tego zagrożenia jest przenikanie różnych metod i środków, połączenie ich, a następnie synergiczne użycie do osiągnięcia określonego celu.

Tabela 2. Przegląd wybranych definicji „zagrożenie hybrydowe"

| Autor | Definicja |
|---|---|
| Frank G. Hoffman | „Każdy przeciwnik stosujący jednocześnie połączoną kombinację broni konwencjonalnej, nieregularnej taktyki, terroryzmu i elementów przestępczych w przestrzeni bitewnej dla osiągnięcia celów politycznych" (Hoffman, 2009). |
| Army Doctrine Publication (ADP) 3-0 Unified Land Operations | „Zróżnicowane i dynamiczne połączenie sił regularnych, sił nieregularnych, elementów przestępczych lub kombinacja tych sił i elementów, ujednoliconych, by osiągnąć wzajemnie korzystne efekty" (*Unified Land Operations*, 2011, s. 4). |
| Brian P. Fleming | „Przeciwnik państwowy lub niepaństwowy, który szybko dostosowuje i łączy różnorodne kombinacje konwencjonalnych, nieregularnych, terrorystycznych i przestępczych zdolności, a także środków niewojskowych, równocześnie jednocząc siły w całym spektrum konfliktu, aby osiągnąć swoje cele" (Fleming, 2011, s. 2-3). |
| NATO | „Połączenie działań militarnych i niemilitarnych, a także ukrytych i jawnych środków, w tym dezinformacji, ataków cybernetycznych, presji gospodarczej, rozmieszczenia nieregularnych grup zbrojnych i wojsk regularnych. Służy do zatarcia granicy między wojną a pokojem i manipulacji określonych populacji. Ma na celu destabilizację i osłabienie społeczeństw (*NATO's response to hybrid threats*, 2022). |
| Komisja Europejska | „Kombinacja represyjnych i wywrotowych działań, konwencjonalnych i niekonwencjonalnych metod (tj. dyplomatycznych, militarnych, ekonomicznych i technologicznych), które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe, by osiągnąć określone cele, przy czym działania te są poniżej progu oficjalnie wypowiedzianej wojny" (JOIN/2016/018 final, s. 2). |
| Jolanta Darczewska | „Jednocześnie zagrożenie zewnętrzne i wewnętrzne, krajowe i ponadnarodowe, militarne i wywiadowcze, na które nie można odpowiedzieć symetrycznie. Operacje hybrydowe są prowadzone przez podmioty państwowe i niepaństwowe w sposób tajny i półjawny, przy wykorzystaniu metod legalnych i nielegalnych" (Darczewska, 2018, s. 40). |
| Olga Wasiuta | „To metody, narzędzia i działania ukierunkowane na podatność przeciwnika w celu wzmocnienia własnych interesów, strategii i celów […] Kombinacja działań łączących często metody konwencjonalne i niekonwencjonalne, które mogą być stosowane w sposób skoordynowany przez podmioty państwowe i niepaństwowe. Pozostają one jednocześnie poniżej progu formalnego wypowiedzenia wojny. Ich celem jest nie tylko spowodowanie bezpośrednich szkód i wykorzystanie słabości, ale również destabilizacja społeczeństw oraz stworzenie niejasności utrudniającej podejmowanie decyzji" (Wasiuta, 2019, s. 728). |

Źródło: Opracowanie własne na podstawie literatury przedmiotu.

Na podstawie przeprowadzonych badań można stwierdzić, że istotą działań o charakterze hybrydowym jest:

- konfrontacja militarna poniżej progu wojny;
- połączenie operacji konwencjonalnych i walk nieregularnych;
- występowanie punktowych aktów terroru;
- użycie destrukcyjnych narzędzi pozamilitarnych na płaszczyźnie: politycznej, ekonomicznej (gospodarczej), społecznej, kulturowej, ideologicznej, humanitarnej;
- wrogie działania w cyberprzestrzeni;
- udział aktorów niepaństwowych (najemnicy, partyzanci).

W *Krajowym Planie Zarządzania Kryzysowego 2017* (s. 43), opracowanym przez Rządowe Centrum Bezpieczeństwa, działania hybrydowe uznano za jedno z głównych zagrożeń, które może zaistnieć na terenie Polski. Biorąc pod uwagę fizyczne środowisko występowania, działania hybrydowe są zjawiskiem wielowymiarowym. Z przeprowadzonych badań wynika, że kombinacje destrukcyjnych metod stosuje się w środowisku lądowym, morskim, powietrznym oraz w cyberprzestrzeni.

Badacze zajmujący się obserwacją współczesnych konfliktów zbrojnych wskazują, że destabilizowanie państwa staje się łatwiejsze i jednocześnie tańsze dzięki metodom nietradycyjnym. Wykorzystuje się zatem instrumenty niemilitarnego oddziaływania w przestrzeni pomiędzy binarnymi granicami wojny i pokoju (Banasik, 2016, s. 193). Zagrożenia pozamilitarne dotyczą czynników, które nie są bezpośrednio związane z doświadczeniem przemocy lub presji militarnej. W zależności od wyznaczonego celu stosuje się pojedyncze środki lub ich kombinacje. Zakładając niemilitarną postać działań hybrydowych, będą to czynności prowadzone przy użyciu m.in. środków politycznych, ekonomicznych, społeczno-kulturowych, ideologicznych. Od momentu upowszechnienia Internetu, państwa i podmioty pozapaństwowe wykorzystują środki szeroko dostępne w cyberprzestrzeni (Warden, 1995, s. 40-55). Coraz częściej rywalizacja międzynarodowa przebiega również w przestrzeni kosmicznej.

Ocenia się, że jeżeli zagrożenia hybrydowe nie zostaną wykryte na czas, może dojść do wojny hybrydowej (Wasiuta, 2019, s. 731). Polska angażując się w konflikt na Ukrainie politycznie, a od 2022 roku również militarnie poprzez m.in. dostawy broni i sprzętu, musi brać pod uwagę prawdopodobieństwo wystąpienia zagrożeń hybrydowych na swoim terytorium niemal w każdej domenie.

Obecne zagrożenia dla bezpieczeństwa Polski o charakterze hybrydowym generowane przez Rosję i Białoruś to:

• demonstracja siły (naruszenie przestrzeni powietrznej i morskiej, manewry i ćwiczenia w pobliżu wschodniej flanki NATO, militaryzacja Obwodu Kaliningradzkiego i obszaru Białorusi, użycie siły militarnej na wschodnich rubieżach NATO i UE);

• nieprzestrzeganie umów i prawa międzynarodowego;

• zmiana granic państwa sąsiedniego (wojna na Ukrainie od 2014 roku);

• infiltracja polskich służb wywiadowczych (aktywność szpiegów);

• ingerencja w system polityczny (dyskredytacja stanowiska Polski i jej sojuszników, lobbing na rzecz rosyjskich podmiotów, próby wpływania na decyzje polityczne rządu i wyniki wyborów);

• wywieranie nacisku gospodarczego (embargo na mięso, ryby, owoce i warzywa, produkty mleczarskie);

• sterowanie społeczne (manipulacja świadomością i psychiką przy użyciu środków masowego przekazu i nowych mediów);

• dezinformacja (rozpowszechnianie zmanipulowanych, nieprawdziwych informacji w celu wywarcia wpływu na polskie społeczeństwo i skłonienia do określonych zachowań korzystnych dla Rosji);

• cyberataki (m.in. polskie instytucje rządowe, banki, sieci telekomunikacyjne, sektor energetyczny);

• masowe migracje ludności (sztuczny kryzys migracyjny wywołany przez Alaksandra Łukaszenkę i kryzys uchodźczy spowodowany przez Władimira Putina wojną na Ukrainie);

• szantaż energetyczny (groźby odcięcia dostaw surowców energetycznych, podwyżki cen surowców, następnie wstrzymanie dostaw).

Według autora do przyszłych zagrożeń dla Polski o charakterze hybrydowym generowanych przez Rosję i Białoruś należeć będą:

• demonstracja siły (rozmieszczenie rosyjskiej taktycznej broni jądrowej na terytorium Białorusi);

• cyberataki na infrastrukturę krytyczną (m.in. system sterowania ruchem kolejowym, system elektroenergetyczny, sieć przesyłową gazu);

• działania dywersyjne na Morzu Bałtyckim (ryzyko uszkodzenia gazociągu Baltic Pipe, terminalu LNG, doprowadzenia do kolizji kontenerowców, zbiornikowców);

• inicjowanie incydentów granicznych (np. realizacja scenariusza ukraińskiego, żądanie umożliwienia przejazdu konwoju humanitarnego z Białorusi „z pomocą" do Obwodu Kaliningradzkiego w związku z „trudną sytuacją ekonomiczną" rosyjskiej eksklawy);

• zamach terrorystyczny (wykorzystanie aktorów pozapaństwowych, np. wyznawcy islamu z obszaru poradzieckiego);

• pogłębienie inflacji (kryzys żywnościowy zapoczątkowany blokowaniem ukraińskich portów morskich na Morzu Czarnym utrudniający eksport zbóż, a także szok cenowy na światowych rynkach gazu i paliw ciekłych wywołany konfrontacyjną polityką energetyczną Rosji);

• paraliż służby zdrowia (w przypadku intensyfikacji rosyjskich działań militarnych na Ukrainie masowa fala osób rannych, poszkodowanych, przewlekle chorych wymagających specjalistycznego leczenia);

• dezinformacja (fake newsy mające zantagonizować stosunki polsko-ukraińskie i wywołać niepokoje społeczne; nieprawdziwe informacje uderzające w rząd, premiera i prezydenta Polski ukierunkowane na osłabienie partii rządzącej i niezadowolenie społeczne, w konsekwencji zmianę niewygodnej dla Kremla władzy).

Należy przyjąć, że powyższy katalog nie jest zamknięty. Co więcej, pozostaje ograniczony jedynie przez wyobraźnię i pomysłowość Rosji i będzie prawdopodobnie kombinacją jednoczesnych lub selektywnych działań o charakterze kinetycznym i niekinetycznym z zastosowaniem elementu pomocy humanitarnej.

## 2. WZMACNIANIE ODPORNOŚCI W WYMIARZE POLITYCZNO-MILITARNYM

Rosja dąży do zmiany ładu międzynarodowego obowiązującego po zimnej wojnie. Ostatnie działania wskazują, że celem długoterminowym Rosji jest zupełne wypchnięcie Stanów Zjednoczonych z Europy, a w perspektywie krótkoterminowej wyparcie ich za Odrę. Wysuwając polityczne żądania Kreml domaga się wycofania natowskich sił oraz uzbrojenia i przywrócenia stanu konfiguracji bezpieczeństwa z 1997 roku. Krótko mówiąc oznacza to, że Stany Zjednoczone mają odpuścić Europę Wschodnią i zostawić takie państwa, jak Litwa, Łotwa, Estonia, Polska, Czechy, Słowacja, Rumunia, Bułgaria rosyjskiej strefie wpływów[4].

Wielowymiarowa eskalacja zagrożeń przez Rosję wzdłuż wschodniej flanki NATO została zogniskowana na destabilizację struktur państw i społeczeństw

[4] Tekst projektu umowy między Federacją Rosyjską a Stanami Zjednoczonymi Ameryki o gwarancjach bezpieczeństwa przekazany przez Moskwę do podpisu stronie amerykańskiej w dniu 15.12.2021 roku. Polskie tłumaczenie: https://www.osw.waw.pl/pl/publikacje/analizy/2021-12-20/rosyjski-szantaz-wobec-zachodu [dostęp: 30.05.2022].

zachodnich, a także na wywołanie podziałów i osłabienie stosunków transatlantyckich. Włączenie Białorusi w imperialne ambicje Moskwy dowodzi, że następuje daleko idąca zmiana uwarunkowań bezpieczeństwa w regionie Europy Środkowej i Wschodniej. Ścisła współpraca wojskowa z Rosją, użycie siły militarnej wobec Ukrainy, liczne prowokacje w postaci aktów terroryzmu, jakim było uprowadzenie samolotu pasażerskiego czy wywołanie kryzysu migracyjnego na granicach UE i NATO, obrazują coraz większą nieprzewidywalność Białorusi w środowisku bezpieczeństwa. Dla Rosji środki militarne są równie ważne jak polityczne, wobec czego nie można wykluczyć użycia przez Moskwę w najbliższej przyszłości sił zbrojnych do prowadzenia wojny z Zachodem.

Teoria i praktyka bezpieczeństwa wskazuje, że zaniechanie działań w kierunku rozwiązania powstających problemów jest swego rodzaju kołem zamachowym w rękach adwersarzy, generując zagrożenia. W nowej sytuacji geopolitycznej wynikającej ze zmiany granic na wschodnich rubieżach NATO i pod groźbą eskalacji kryzysów polityczno-militarnych Polska wraz z sojusznikami musi skoncentrować swoje wysiłki do skutecznego odstraszania i reagowania na działania militarne i pozamilitarne generowane na ścianie wschodniej. W budowaniu odporności kraju na zagrożenia, istotnego znaczenia nabiera zdolność do oporu i przetrwania potencjalnej agresji, którą można osiągnąć poprzez obronne przygotowanie społeczeństwa, zwiększenie niedostępności operacyjnej terytorium, działania nieregularne wspierające różne struktury państwowe (Koziej, 2016, s. 86).

Nawiązując do natowskiego „Baseline Requirements National Resilience", priorytetem pozostaje utrzymanie gwarancji w odniesieniu do ciągłości rządów oraz najważniejszych usług rządowych. Chodzi o zdolność do podejmowania decyzji, ich komunikowania i egzekwowania w przypadku operacji hybrydowych. Perspektywa skutecznego rozwiązywania problemów związanych z niekontrolowanym przemieszczaniem się ludzi stanowi dla Polski kluczowe wyzwanie w najbliższej dekadzie. Ponadto implikacje wojny na Ukrainie wskazują na potrzebę tworzenia odpornych systemów transportu ukierunkowanych na szybkie przemieszczanie sił NATO po terytorium państw Sojuszu, w tym utrzymanie możliwości sprawnego poruszania dla służb cywilnych zarówno w czasie kryzysu, jak i wojny.

W wymiarze polityczno-militarnym należy:

• Dążyć do konsolidacji wspólnoty transatlantyckiej wokół wspólnego zagrożenia (reorientacja świadomości sytuacyjnej w kontekście oceny ryzyk generowanych przez Rosję i Białoruś).

• Podnosić na arenie międzynarodowej kwestie reformy ONZ (*casus* Rosji w Radzie Bezpieczeństwa).

• Zacieśnić współpracę w ramach współpracy regionalnej, tj. Trójmorza, Bukaresztańskiej Dziewiątki, Grupy Wyszehradzkiej, Trójkąta Weimarskiego.

• Zmienić charakter stacjonowania wojsk Stanów Zjednoczonych Ameryki z rotacyjnego na stały (permanentny) i dostosować istniejące w Polsce bazy do stałej obecności.

• Aktywnie działać na rzecz rozmieszczenia na wschodniej flance NATO sił, które będą zdolne do zatrzymania ataku Rosji już na samym jego początku. Powinny stacjonować wielonarodowe grupy bojowe o wielkości minimum brygady wraz ze sprzętem.

• Zabiegać o ujednolicenie standardów i usunięcie barier w ramach programu *Action Plan on Military Mobility* służącemu poprawie mobilności wojskowej sił natowskich na obszarze UE.

• Rozwijać zdolności operacyjne sił zbrojnych do zwalczania zagrożeń hybrydowych.

• Nalegać na rozbudowę zachodniej sieci rurociągów paliwowych (CEPS) zaopatrujących wojska Sojuszu w paliwo, wzorem operacji PLUTO z okresu II wojny światowej.

• Zwiększyć poziom ochrony obiektów kategorii I oraz kategorii II.

• Przyspieszyć realizację krajowych programów zbrojeniowych (m.in. system obrony przeciwlotniczej i przeciwrakietowej krótkiego i średniego zasięgu).

• Wzmocnić zdolności do prowadzenia działań militarnych w cyberprzestrzeni, a także rozszerzyć współpracę wywiadowczą i kontrwywiadowczą w ramach UE i NATO.

• Wzmocnić zabezpieczenie organów państwowych i infrastruktury krytycznej państwa przed aktywnością wywiadowczą obcych służb.

• Działać na rzecz zacieśnienia współpracy przemysłów obronnych Polski i Ukrainy, Polski z państwami skandynawskimi.

• Niezwłocznie rozbudować infrastrukturę strzelnic sportowych i pneumatycznych, utworzyć strzelnice wirtualne, a także przeprowadzić szkolenia strzeleckie dla uczniów szkół i wszystkich zainteresowanych dorosłych.

• Przeprowadzić kampanie społeczne ukierunkowane na szerokie upowszechnienie strzelectwa wśród młodzieży i dorosłych.

## 3. WZMACNIANIE ODPORNOŚCI W WYMIARZE GOSPODARCZO-ENERGETYCZNYM

Nie ulega wątpliwości, że potencjał ekonomiczny państwa jest głównym determinantem jego potęgi czy prestiżu na arenie międzynarodowej. Niejednokrotnie przez siłę ekonomiczną rozpatruje się siłę militarną państwa. Pozycja państwa w otoczeniu międzynarodowym zależy również od prowadzonej polityki gospodarczej. Państwo dążąc do zapewnienia sobie bezpieczeństwa ekonomicznego wybiera i realizuje określoną strategię. Mogą to być działania jednostronne (unilateralne) lub wielostronne (multilateralne).

Co istotne, bezpieczeństwo ekonomiczne w sposób bezpośredni wpływa na pokój międzynarodowy. Zakłada się, że im wyższy poziom rozwoju gospodarczego osiągnie dane państwo, tym korzystniejsze warunki stworzy dla ukształtowania się społeczeństwa obywatelskiego i upowszechnienia demokracji liberalnej. Zgodnie z liberalną teorią stosunków międzynarodowych demokracje liberalne nie toczą ze sobą wojen. Potencjalna wojna jest nieopłacalna z punktu widzenia interesów narodowych (Czaputowicz, 2007, s. 111). Rosja wybrała inną drogę, prowadzi konfrontację z Zachodem na wszystkich możliwych płaszczyznach. W wymiarze ekonomicznym Moskwa odpowiada kontrposunięciami, wprowadzając m.in. sankcje wizowe czy embargo na dostawy żywności i towarów, zaś czynnik energetyczny traktuje jako instrument wojny hybrydowej.

Polityka sankcji UE wobec Rosji, która miała zmusić Władimira Putina do zaprzestania działań destabilizacyjnych dwa wschodnie obwody Ukrainy i zagarnięty Krym, nie przyniosła oczekiwanych rezultatów. Pozostając w solidarności z Ukrainą od 2014 roku, państwa UE i Stany Zjednoczone nakładają sankcje ekonomiczne na Rosję. Wybiórczość ówczesnych restrykcji, charakteryzująca się chociażby pominięciem kluczowego rosyjskiego sektora – przemysłu zbrojeniowego, wystawia negatywną ocenę europejskim decydentom w świetle aktualnie trwającej wojny na Ukrainie. Polityka uległości i krótkowzroczność zachodnich elit zachęciła Rosję do kolejnej zbrojnej napaści, tym razem na pełną skalę. Warto przypomnieć, że Bruksela w 2015 roku znosiła sankcje gospodarcze na Białoruś utrzymywane od 2006 roku, licząc na „odwilż" w stosunkach dwustronnych.

Prognozy analityków i badaczy mówiące o rosnącym zapotrzebowaniu na energię elektryczną stały się faktem. Wśród czynników, które warunkują bezpieczeństwo energetyczne danego państwa, można wskazać takie, jak: poziom samowystarczalności energetycznej, kondycja systemu zaopatrzenia, forma własności

przedsiębiorstw sektora energetycznego, stopień dywersyfikacji źródeł i kierunków energii, możliwość finansowania nowych technologii, ilość zmagazynowanych rezerw, stabilność sytuacji wewnętrznej i międzynarodowej (Soroka, 2015, s. 27-28). Zgodnie z „Baseline Requirements National Resilience" główną przesłanką wzmacniania przez Polskę odporności narodowej w analizowanym obszarze będzie dostateczne zabezpieczenie dostaw i źródeł energii.

Rosja dzięki zdecydowanej dominacji na Starym Kontynencie pod względem produkcji oraz eksportu (przesyłu) gazu ziemnego, ropy naftowej i węgla kamiennego posiada szerokie możliwości wywierania nacisków wobec krajów „bliskiej zagranicy" i wielu państw UE uzależnionych od rosyjskich węglowodorów w stopniu wysokim. Doświadczenia ostatniej dekady wskazują, że Rosja z powodzeniem stosuje: szantaż (projekt gazociągu Nord Stream 2, punktowe groźby odcięcia dostaw surowców), demonstrację siły (podwyżki cen paliw, ograniczenie i wstrzymanie dostaw gazu ziemnego), terroryzm (eksplozje rurociągów), roszczenia (zakaz reeksportu nadwyżek sprowadzonego gazu), embargo (eksport ropy naftowej i produktów naftowych), cyberataki na system elektroenergetyczny. W świetle prowadzonych operacji hybrydowych wymierzonych w sektor energetyczny, państwa muszą dążyć do minimalizacji ryzyka przerwania dostaw i utrzymania ceny na pożądanym poziomie.

W wymiarze gospodarczo-energetycznym należy:

• Wzmacniać stabilność finansów publicznych budując odporność na możliwe międzynarodowe kryzysy finansowe.

• Zabiegać o wykluczenie (bądź co najmniej bezterminowe zawieszenie) Rosji z organizacji międzynarodowych (G20, WTO, FAO, UNESCO).

• Zabiegać o wprowadzenie sankcji pośrednich w celu przeciwdziałania omijaniu obowiązujących sankcji gospodarczych (mogą być nakładane na podmioty państw trzecich w przypadku współpracy z podmiotami już objętymi).

• Pogłębić współpracę gospodarczą z partnerami strategicznymi (Niemcy, Wielka Brytania, Francja, Włochy, Stany Zjednoczone).

• Zabiegać na forum UE o przyspieszenie odejścia od importu surowców energetycznych z Rosji, a także o ograniczenie eksportu usług i nowoczesnych technologii do Rosji i Białorusi.

• Dążyć do rozbudowy połączeń energetycznych między państwami członkowskimi w oparciu o środki europejskie na rozwój infrastruktury.

• Zabiegać o wdrożenie mechanizmu wspólnych zakupów surowców energetycznych dla państw członkowskich UE.

• Zaktualizować plany awaryjne oraz dostatecznie zabezpieczyć wewnętrzne i transgraniczne sieci elektroenergetyczne.

• Sfinalizować drugą nitkę Rurociągu Pomorskiego łączącego Gdańsk z Płockiem, co przełoży się na zabezpieczenie transportu ropy naftowej na odcinku północnym.

• Rozbudować polskie bazy magazynowe gazu zimnego, ropy naftowej i paliw ciekłych.

• Przyspieszyć budowę terminalu pływającego LNG wraz całą infrastrukturą w Zatoce Gdańskiej, a także podnieść rolę odnawialnych źródeł energii w krajowej produkcji energii.

## 4. WZMACNIANIE ODPORNOŚCI W WYMIARZE INFORMACYJNYM

Współcześnie informacja jest wykorzystywana jako broń, narzędzie walki, narzędzie ataku. Z perspektywy kreowanych zagrożeń może przybrać różną postać. Analiza kampanii dezinformacyjnych dowodzi, że najczęściej informacja jest przekazywana za pośrednictwem dowolnego medium, zwykle Internetu, i wówczas ze względu na zasięg stanowi najskuteczniejsze oręże. W nieco mniejszym stopniu wrogie kampanie realizowane są za pośrednictwem telewizji, radio i prasy, wszystko w zależności od grupy docelowej. Agresor kierując się określonym celem, dąży do wywołania społecznych emocji, kształtowania niepokojów społecznych, zmiany postaw odbiorców lub ukrycia prawdziwej informacji poprzez jej zniekształcenie (Zalewski, 2016, s. 201-219). Inną groźną postać stanowi wykorzystanie informacji jako narzędzia ataku przy użyciu programu komputerowego. Celem będzie wywołanie określonych skutków w systemie informatycznym danego podmiotu, np. strategicznych sektorów związanych z infrastrukturą krytyczną państwa. W działaniach Rosji zauważa się współwystępowanie działalności propagandowej z atakami na infrastrukturę krytyczną (Wrzosek, 2016, s. 42-59).

Raporty Agencji Bezpieczeństwa Wewnętrznego RP potwierdzą wysokie zainteresowanie aktywnością rosyjskich i białoruskich służb specjalnych (https://infolupki.pgi.gov.pl/sites/default/files/czytelnia_pliki/1/raport_2015_int.pdf).

Działania destruktorów uwarunkowane wydarzeniami na ścianie wschodniej dotyczą m.in. dyskredytacji stanowiska Polski i jej natowskich sojuszników, kształtowania prorosyjskich i antyukraińskich opinii za pośrednictwem internetowych portali, serwisów społecznościowych, blogów przez podstawione osoby działające na zlecenie i stosujące mechanizm tzw. *поле́зный идиот*. Kołem zamachowym są zarówno cybernajemnicy, jak i obywatele rosyjscy

wykorzystujący rozległe kontakty wśród polskiej klasy politycznej i w strukturach unijnych. Kreml w tym celu wykorzystuje specjalnie stworzone „farmy trolli". Wśród innych metod działania strony rosyjskiej kontrwywiad wskazuje m.in. lobbing na rzecz rosyjskich podmiotów, w tym próby zdobycia informacji w zakresie pozyskiwania towarów podwójnego zastosowania, a także rozpoznania polskiego sektora energetycznego (np. wizji jego rozwoju).

Wobec Polski i państw wspólnoty euroatlantyckiej podczas informacyjnych operacji hybrydowych Rosja wykorzystuje na niespotykaną wcześniej skalę następujące narzędzia: dezinformację, manipulację, fake newsy, zakłócanie informacyjne, cyberataki, cyberszpiegostwo. Kluczową rolę odgrywają takie grupy, jak: APT28 (Fancy Bear) – związana z GRU, APT29 (Cozy Bear, The Dukes) – złączona z FSB i służbą wywiadu zagranicznego SWR, Turla (Snake/ Uroburos) – funkcjonująca w strukturach FSB. W prowadzonej wojnie informacyjnej celem ataków są podmioty rządowe, agencje wywiadowcze, sektor zbrojeniowy, transportowy, medialny, energetyczny, farmaceutyczny. Rosja również finansuje, rozwija i wykorzystuje elity do zakłócenia procesów politycznych w Europie. Dużym zainteresowaniem cieszy się rekrutacja agentów w Parlamencie Europejskim, głównie w celu poprawy wizerunku Rosji przez liderów partii i społeczność międzynarodową, zwłaszcza po agresji na Ukrainę (Nowak, 2020, s. 67-84).

Według *EU Hybrid Fusion Cell* dezinformacja Rosji jest największym zagrożeniem dla Unii Europejskiej: „Pod względem koordynacji, poziomów ukierunkowania i strategicznych implikacji dezinformacja stanowi część szerszego zagrożenia hybrydowego, które wykorzystuje szereg narzędzi, nacisków i podmiotów pozapaństwowych" (*Action Plan against Disinformation*, 2018, s. 4). Szczególnie niebezpieczeństwo wynika z podsycania antagonizmów uwarunkowanych doświadczeniami historycznymi, dążenia do podziałów oraz torpedowania współpracy i procesu decyzyjnego poprzez ingerencję w wybory prezydenckie czy parlamentarne. Dlatego tak istotnym zadaniem jest budowanie wśród obywateli świadomości posługiwania się informacją.

Innym obszarem wymienionym również przez NATO w „Baseline Requirements National Resilience" jest zdolność państwa do tworzenia i utrzymywania odpornych na zagrożenia hybrydowe cywilnych systemów łączności. Niezawodność komunikacji, ciągłość i sprawność jej przywracania m.in. z perspektywy administracji rządowej odgrywa szczególną rolę. Działania Polski powinny zmierzać do zapewnienia funkcjonowania sieci telekomunikacyjnych i sieci cybernetycznych w warunkach kryzysu z utrzymaniem zdolności i źródeł rezerwowych.

W wymiarze informacyjnym należy:

• Zobowiązać największe podmioty, jak np. Google, Facebook, Twitter do wzięcia odpowiedzialności za publikowane treści, często będących kołem zamachowym kampanii dezinformacyjnych prowadzonych przez Rosję.

• Wprowadzić zakaz nadawania na terytorium UE wszystkich rosyjskich i białoruskich programów telewizyjnych i radiowych.

• Zabiegać o stworzenie przez UE rosyjskojęzycznego kanału informacyjnego dla obywateli Rosji i obszaru poradzieckiego, który mógłby nadawać w Internecie.

• Powołać resortowy zespół weryfikowania i zwalczania fake newsów.

• Podnieść kompetencje (wiedzę, umiejętności, postawy) i świadomość wśród pracowników administracji publicznej i całego społeczeństwa w zakresie zagrożeń hybrydowych generowanych w cyberprzestrzeni oraz w przestrzeni informacyjnej.

• Uwrażliwić polskie media na posługiwanie się zweryfikowanym materiałem źródłowym, w tym rozważyć prawne uregulowanie odpowiedzialności autorów fałszywych wiadomości.

• Usprawnić proces strategicznej komunikacji celem zabezpieczenia żywotnych interesów, osiągania celów i promowania spójności koalicji euroatlantyckiej.

• Podnieść poziom odporności i zapewnić ciągłość działania sieci telekomunikacyjnych i systemów teleinformatycznych państwa w warunkach kryzysu, w tym odporność na możliwość użycia przez przeciwnika broni generującej impuls elektromagnetyczny (EMP).

• Dokonać dogłębnej oceny wszystkich zagrożeń dla systemów łączności, w tym sieci 5G.

• Przeprowadzić ogólnopolskie kampanie społeczne na temat dezinformacji za pomocą m.in. mediów tradycyjnych i mediów społecznościowych, citylightów, billboardów.

• Włączyć organizacje pozarządowe w prowadzenie pogadanek, prelekcji odnoszących się do problematyki dezinformacji.

## 5. WZMACNIANIE ODPORNOŚCI W WYMIARZE SPOŁECZNYM

Istotną rolę w budowaniu odporności na zagrożenia odgrywa świadomość społeczna, którą można określić jako pewien zbiór wyobrażeń, opinii, poglądów, pojęć wspólnych dla jakiejś społeczności. W szerszym kontekście oznacza

całokształt charakterystycznych dla danego społeczeństwa treści i formy życia duchowego. Źródłem świadomości jednostkowej i społecznej będzie zatem wiedza, prawo, kultura, tradycja, wiara, doświadczenie. Odnosząc się do wiedzy współcześnie, każdy człowiek powinien mieć podstawową wiedzę o potencjalnych zagrożeniach w miejscu, w którym funkcjonuje, i posiadać zdolność do sterowania własnym życiem (Grocki, 2012, s. 139-143). Ukraiński kryzys uchodźczy trzeba postrzegać jako *lessons learned* dla Polski.

Nie bez znaczenia pozostaje umiejętność adaptacji do nowych warunków przeobrażającego się świata, a ściślej mówiąc – do zmiany architektury bezpieczeństwa na naszych oczach. W kształtowaniu świadomości głównym celem powinno być zdobywanie wiedzy, która pozwoli przygotować i rozwinąć cechy oraz umiejętności ukierunkowane na radzenie sobie z wieloma zagrożeniami (wewnętrznymi i zewnętrznymi, losowymi i celowymi). Świadomość kształtowana przez wiedzę w dziedzinie bezpieczeństwa odbywa się poprzez działalność edukacyjną (rozumianą jako edukacja dla bezpieczeństwa), której adresatami są jednostki, grupy społeczne, państwa, społeczność międzynarodowa.

Umiejętność antycypowania niebezpieczeństwa stanowi jedną z najważniejszych kompetencji człowieka. Odporne społeczeństwo to społeczeństwo świadome zagrożeń i posiadające umiejętność właściwej reakcji, opartej na świadomości narodowej, historycznej i patriotyczno-obronnej. Znając i rozumiejąc słabości narodowe, mamy szansę uniknąć błędów popełnionych w historii, prowadzących do zguby narodowej. Ukształtowanie stanu świadomości, który zapewni zdolność do obrony wartości cenionych, przetrwania i rozwoju, jest procesem złożonym. Edukacja jako proces rozwoju możliwości intelektualnych człowieka służy zdobywaniu wiedzy. Obejmuje wychowanie i kształcenie (Pieczywok, 2012, s. 64-73).

Edukacja dla bezpieczeństwa (Stępień, 2011, s. 579-590) odnosi się do wymiaru instytucjonalnego. Właśnie w ramach instytucji społecznych dokonuje się transfer wiedzy. Jego treść stanowią te wartości, informacje, których pogłębienie i upowszechnienie jest ważne dla zapewnienia bezpieczeństwa w wymiarze jednostkowym, grupowym czy narodowym. Edukacja dla bezpieczeństwa jest procesem ciągłym, w ramach którego m.in. zachodzi: przekaz wiedzy o zagrożeniach; kształtowanie bezpiecznych zachowań i postaw; motywowanie do podejmowania działań na rzecz zapewnienia bezpieczeństwa; uświadamianie skali i rodzaju potrzeb w sytuacjach zagrożeń; rozwijanie poczucia odpowiedzialności za podejmowane działania; kształtowanie odpowiednich nawyków w sytuacjach trudnych (Pieczywok, 2012, s. 67).

Nieodłącznym elementem wzmacniania odporności w wymiarze społecznym pozostaje organizacja i utrzymywanie sprawnego, zintegrowanego systemu ochrony ludności dostosowanego do aktualnych zagrożeń i wyzwań, w tym o charakterze hybrydowym. Realizacja szkoleń, ćwiczeń i próbnych ewakuacji jest prostą metodą na podniesienie świadomości obywateli w zakresie samoochrony i kształtowania prawidłowych postaw, co następnie przekłada się na poczucie i postrzeganie bezpieczeństwa przez społeczeństwo. Posiłkując się „NATO Baseline Requirements National Resilience" należy podkreślić w tym miejscu celowość zabezpieczenia zapasów żywności i wody pitnej w kontekście zagrożeń hybrydowych, a także zdolność do radzenia sobie z dużą liczbą ofiar i destrukcyjnymi kryzysami zdrowotnymi. Inwazja zbrojna Rosji na Ukrainę rozpoczęta w lutym 2022 roku dobitnie pokazuje, że zaniedbania w tym zakresie mogą mieć tragiczne skutki dla ludności cywilnej.

W wymiarze społecznym należy:

• Dążyć do podniesienia kwalifikacji kadry pracowników struktur administracyjnych, którym powierzono zadania z zakresu obrony cywilnej i zarządzania kryzysowego.

• Aktualizować na bieżąco plany zarządzania kryzysowego, w szczególności dotyczy to procedur, posiadanego sprzętu i katalogu potencjalnych i realnych zagrożeń.

• Zmodernizować system ostrzegania i alarmowania ludności o zagrożeniach o możliwość nadawania komunikatów głosowych.

• Włączyć do ochrony ludności organizacje pozarządowe i stowarzyszenia, które działają w systemie ratowniczym.

• Zabezpieczyć zapasy żywności i wody pitnej przed możliwymi zakłóceniami lub akcjami sabotażu.

• Utworzyć bazy magazynowe od gmin do ministerstw, wyposażone w sprzęt i środki techniczne do prowadzenia akcji ratowniczych i akcji pomocy humanitarnej.

• Utrzymywać cywilne systemy opieki zdrowotnej w gotowości, przygotować zastępcze miejsca szpitalne, zabezpieczyć wystarczające ilości środków medycznych.

• Wdrożyć w trybie pozaszkolnym zajęcia edukacyjne dla dzieci i młodzieży poświęcone m.in. radzeniu sobie w warunkach kryzysu i wojny.

• Niezwłocznie dostosować istniejące budowle ochronne do stanu używalności poprzez ich modernizację.

• Dokonać ewidencji miejsc, które w razie potrzeby można zaadaptować do celów ochronnych dla ludności, i zwiększyć liczbę doraźnych ukryć na terenach publicznych.

## WNIOSKI

Odnosząc się do postawionego problemu badawczego należy stwierdzić, że Polska w celu wzmacniania odporności na zagrożenia o charakterze hybrydowym, które są nieustannie implikowane przez Rosję i Białoruś, powinna podjąć szereg działań wyprzedzających w kluczowych wymiarach bezpieczeństwa, zgodnych z wytycznymi „NATO Baseline Requirements National Resilience". Warto mieć na uwadze, że utrzymywanie i rozwijanie zdolności w sferze cywilnej i wojskowej, które znacząco utrudnią nieprzyjazne działania, jest podstawowym warunkiem bezpieczeństwa, pierwszą linią odstraszania i obrony państwa. Podnoszenie odporności musi obejmować działania o zasięgu krajowym, unijnym i sojuszniczym.

Proponuje się w wymiarze polityczno-militarnym rozbudowę własnych zdolności obronnych, wzmocnienie potencjału relacji sojuszniczych w ramach UE i NATO, partnerstwa strategicznego ze Stanami Zjednoczonymi i aktywną politykę regionalną. Priorytetem będzie zdolność do rozpoznawania i oceny zagrożeń w ramach narodowego i transatlantyckiego systemu bezpieczeństwa, co przełoży się na zdolność do odpowiedzi na zagrożenia hybrydowe.

Celowe jest również wzmacnianie odporności na możliwe międzynarodowe kryzysy finansowe i energetyczne poprzez utrzymanie stabilności finansów publicznych i zabezpieczenie dostaw energii, zapasów żywności i wody. Za konieczne należy uznać zwalczanie rosyjskiej dezinformacji, budowanie wśród obywateli świadomości posługiwania się informacją, a także zapewnienie funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej. Duży nacisk należy położyć na przygotowanie społeczeństwa do radzenia sobie w warunkach kryzysu i wojny, w tym reformę systemu ochrony ludności.

Sformułowane zalecenia i rekomendacje dla Polski dotyczące wzmacniania odporności na zagrożenia hybrydowe nie są wyczerpujące, gdyż podejmowana problematyka dotyczy rzeczywistości nie tylko zastanej, ale przede wszystkim – przyszłości. Stanowią wstęp do pogłębionej debaty nad stanem bezpieczeństwa państwa, a także kondycji współczesnego świata i agend odpowiedzialnych za utrzymanie równowagi systemu bezpieczeństwa międzynarodowego.

Na podstawie przeprowadzonych badań ustalono, że zagrożenia hybrydowe polegają na wielowymiarowym, jednoczesnym oddziaływaniu przez agresora w sferze militarnej z zastosowaniem klasycznych i nieregularnych działań zbrojnych i w sferze pozamilitarnej z użyciem pozostających w dyspozycji środków, tak aby osiągnąć zamierzone efekty. Wielomodelowa forma prowadzenia walki jest stosowana pojedynczo lub symultanicznie w różnym czasie, w różnym wymiarze, z różnym natężeniem.

## BIBLIOGRAFIA

*Action Plan against Disinformation* (2018), Bruksela 5.12.2018, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf [dostęp: 12.06.2022].

Banasik M. (2016), *Współczesne wojny w szarej strefie zagrożeniem dla bezpieczeństwa. Wyzwania i dylematy reagowania*, Przedsiębiorczość i Zarządzanie, XVII, z. 5, część 3, s. 183-197.

Czaputowicz J. (2007), *Teorie stosunków międzynarodowych. Krytyka i systematyzacja*, Warszawa: PWN.

Darczewska J. (2018), *Środki aktywne jako rosyjska agresja hybrydowa w retrospekcji. Wybrane problemy*, Przegląd Bezpieczeństwa Wewnętrznego, nr 18, s. 40-67.

Fleming B.P. (2011), *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, Kansas: School of Advanced Military Studies.

Grocki R. (2012), *Zarządzanie kryzysowe. Dobre praktyki*, Warszawa: Difin.

Hoffman F.G. (2009), *Hybrid vs. compound War. The Janus choice: Defining today's multifaceted conflict*, http://armedforcesjournal.com/hybrid-vs-compound-war/ [dostęp: 28.05.2022].

Kaldor M. (2013), *In Defence of New Wars*, Stability. International Journal of Security & Development, 2, nr 1, s. 1-16.

Koziej S. (2016), *Strategiczna odporność kraju i rola w niej podmiotów niepaństwowych*, Krytyka Prawa, 8, nr 1, s. 82-92.

*Krajowy Plan Zarządzania Kryzysowego 2017. Część A* (2017), Warszawa: Rządowe Centrum Bezpieczeństwa.

*(Mini)Słownik BBN. Propozycje nowych terminów z dziedziny bezpieczeństwa* (2015), https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp: 20.05.2022].

*NATO's response to hybrid threats* (2022), https://www.nato.int/cps/en/natohq/topics_156338.htm [dostęp: 28.05.2022].

Nowak T. (2020), *Działania hybrydowe w cyberprzestrzeni prowadzone przez Rosję jako zagrożenie dla bezpieczeństwa euroatlantyckiego*, [w:] M. Banasik, A. Rogozińska (red.), *Zagrożenia Federacji Rosyjskiej i bezpieczeństwo międzynarodowe*, Warszawa: Difin, s. 67-84.

Pieczywok A. (2012), *Edukacja dla bezpieczeństwa wobec zagrożeń i wyzwań współczesności*, Warszawa: Akademia Obrony Narodowej.

*Resilience, Civil Preparedness and Article 3* (2022), https://www.nato.int/cps/en/natohq/topics_132722.htm [dostęp: 20.05.2022].

*Resilience through Civil Preparedness. A CCOE Info Sheet* (2019), Civil-Military Cooperation, Centre of Excellence, https://www.cimic-coe.org/resources/fact-sheets/resilience-through-civil-preparedness.pdf [dostęp: 20.05.2022].

Rey R. (2022), *Społeczeństwo odporne na zagrożenia*, https://www.gov.pl/web/rcb/spoleczenstwo-odporne-na-zagrozenia [dostęp: 24.05.2022].

Roepke W.D., Thankey H. (2019), *Odporność – pierwsza linia obrony*, https://www.nato.int/docu/review/pl/articles/2019/02/27/odpornosc-pierwsza-linia-obrony/index.html [dostęp: 24.05.2022].

Shea J. (2016), *Resilience: a core element of collective defence*, https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html [dostęp: 24.05.2022].

*Słownik terminów z zakresu bezpieczeństwa narodowego* (2009), Warszawa: Akademia Obrony Narodowej.

Soroka P. (2015), *Bezpieczeństwo energetyczne. Między teorią a praktyką*, Warszawa: Dom Wydawniczy ELIPSA.

Stępień R. (2011), *Edukacja dla bezpieczeństwa*, [w:] R. Jakubczak, J. Marczak (red.), *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie*, Warszawa: Bellona, s. 579-590.

*Strengthened Resilience Commitment* (2021), https://www.nato.int/cps/en/natohq/official_texts_185340.htm [dostęp: 20.05.2022].

Śliwa Z., Wojciechowski S. (2021), *Odstraszanie militarne oraz odporność strategiczna państw w rejonie północno-wschodniej flanki NATO*, Roczniki Nauk Społecznych, 13(49), nr 2, s. 71-86.

*Unified Land Operations* (2011), Army Doctrine Publication (ADP) 3-0, Washington: Headquarters Department of the Army.

Wallerstein I. (2004), *Koniec świata jaki znamy*, Warszawa: Wydawnictwo Naukowe Scholar.

Warden J.A. (1995), *The Enemy as a System*, Airpower Journal, nr 9, s. 40-55.

Wasiuta O. (2019), *Zagrożenia hybrydowe*, [w:] O. Wasiuta, R. Klepka, R. Kopeć (red.), *Vademecum Bezpieczeństwa*, Kraków: Wydawnictwo LIBRON.

Wrzosek M. (2016), *Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka*, Kwartalnik Bellona, nr 4(687), s. 42-59.

*Wspólny komunikat do Parlamentu Europejskiego i Rady. Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym odpowiedź Unii Europejskiej* (2016), JOIN/2016/018 final, Bruksela 6.4.2016.

Zalewski J. (2016), *Intoksykacja psychologiczno-informacyjna głównym elementem wojny informacyjnej prowadzonej przez Federację Rosyjską*, Studia Bezpieczeństwa Narodowego, 6, nr 9, s. 201-220.

## BUDOWA ODPORNOŚCI NA OBECNE I PRZYSZŁE ZAGROŻENIA O CHARAKTERZE HYBRYDOWYM.
### REKOMENDACJE DLA POLSKI

Streszczenie

Treści artykułu koncentrują się wokół problemu budowy odporności, która jest istotnym elementem bezpieczeństwa państwa. Stanowi fundament odstraszania i obrony, przez co pozwala na skuteczne przeciwstawienie się zagrożeniom. Celem artykułu była identyfikacja obecnych i przyszłych zagrożeń hybrydowych kreowanych przez Rosję i Białoruś, a także przedstawienie zaleceń i rekomendacji dla Polski w zakresie wzmacniania odporności na te zagrożenia. W świetle zmiany architektury bezpieczeństwa w sąsiedztwie Polski wynikającej z neoimperialnej polityki Rosji i będącej pod jej wpływem Białorusi, podjęta problematyka stanowi wartość dodaną. W procesie badawczym zastosowano ogólne metody poznania naukowego, które opierały się głównie na analizie i krytyce literatury, wnioskowaniu i własnej ocenie faktów.

**Słowa kluczowe:** bezpieczeństwo Polski; odporność; zagrożenie; zagrożenie hybrydowe; Rosja.