Wyższa Szkoła Policji
w Szczytnie

mgr Tomasz Paweł Kijewski

Rozprawa doktorska

Przeciwdziałanie zagrożeniom hybrydowym

Promotor:
prof. dr hab. Waldemar Zubrzycki

Promotor pomocniczy:
dr Marcin Lipka

Szczytno 2023

Spis treści

Wstęp

Odnotowywany w ostatnich latach wzrost ilościowy i jakościowy ataków hybrydowych na świecie, w tym w Europie, wymaga wypracowania skutecznych strategii przeciwdziałania temu zagrożeniu w różnych obszarach i na różnych poziomach decyzyjnych. Problem ten dotyczy zarówno zagrożeń zewnętrznych dla organizmów państwowych (w tym Polski i innych krajów Sojuszu Północnoatlantyckiego – NATO), jak i innych sfer – np. bezpieczeństwa wewnętrznego w kontekście aktywności przestępczości zorganizowanej czy wykorzystania elementów przestępczych w działaniach hybrydowych na społeczno-politycznej scenie w państwie (z wykorzystaniem np. walki informacyjnej i cybernetycznej, w tym – dezinformacji, aktywności bojówek, najemników, inicjowania zagrażających bezpieczeństwu publicznemu sztucznych ruchów społecznych, strajków, demonstracji). Przykładem działań w tej kategorii jest m.in. wykorzystanie migracji, jako broni, co można było zaobserwować w czasie kryzysu na granicy polsko-białoruskiej w 2021 r.

Zagrożenia hybrydowe, co akcentuje rumuńska badaczka Florina Cristiana Matei, należy rozpatrywać w szerszym ujęciu kształtowania się środowiska bezpieczeństwa międzynarodowego po zakończeniu zimnej wojny, ataków terrorystycznych 9/11 i kolejnych fal rozszerzania NATO/UE. Ważnymi czynnikami były w tym kontekście także procesy adaptacji wielu armii do obrony przed zagrożeniami asymetrycznymi i hybrydowymi oraz transformacja sił zbrojnych polegająca na odejściu od powszechnej służby wojskowej i tworzeniu zawodowych sił zbrojnych[1]. Wiele z tych uwarunkowań miało wpływ na sytuację bezpieczeństwa Polski oraz szeregu innych krajów regionu.

Zagrożenia hybrydowe należy postrzegać jako działania wykorzysujące niestandardowe środki wywierania wpływu, które nie mieszczą się w ramach tradycyjnych kategorii. Działania te eksploatują progi wykrywalności oraz atrybucji, jak również granicę między wojną i pokojem, sprawami wewnętrznymi i zagranicznymi, militarnymi i cywilnymi, sektorem państwowym i sferą prywatnej działalności gospodarczej. Ataki hybrydowe mają na celu ingerencję w proces decyzyjny obiektu obranego za cel, co może

[1] F.C. Matei, *NATO, democratic control, and military effectiveness: Romania*, [w:] T. C. Bruneau, F.C. Matei (red.), *The Routledge Handbook Of Civil–Military Relation, Routledge* 2013, s. 319-320.

oznaczać także zakłócenie tego procesu. Zagrożenia hybrydowe to po prostu inna nazwa obszarów ryzyka generowanych przez niekonwencjonalne, nietypowe działania wojenne – wojnę niewypowiedzianą i prowadzoną niejawnymi metodami. Efektem tego jest zaszkodzenie atakowanemu podmiotowi lub osłabienie go. Do głównych czynników stojących za zagrożeniami hybrydowymi można zaliczyć przemieszczanie się globalnego układu sił z Zachodu na Wschód; rywalizację systemową i słabości systemów autorytarnych; rozwój technologiczny oraz niski koszt użycia instrumentów hybrydowego działania[2].

Wbrew pojawiającej się czasem opinii, hybrydowe działania wojenne nie stanowią nowej formy walki, ponieważ znane są w historii konfliktów zbrojnych (wiele takich cech miała np. działalność polskiego ruchu oporu podczas Drugiej Wojny Światowej czy wojna w Wietnamie). Hybrydowe metody prowadzenia wojny, takie jak propaganda, oszustwo, sabotaż i inne taktyki pozamilitarne są od dawna stosowane do destabilizacji przeciwników. Na sposób postrzegania zagrożeń hybrydowych wpływ miały także niektóre współczesne konflikty zbrojne, w tym wojna Izraela z Hezbollahem, która przez część analityków została nazwana hybrydową[3]. Pewną nowością jest natomiast zmieniający się charakter zagrożeń hybrydowych. Kiedyś wiodącym przejawem taktyki hybrydowej był konflikt zbrojny, natomiast obecnie są to bardziej działania pozamilitarne. Zmianą w atakach obserwowanych w ostatnich latach jest ich charakter, szybkość, skala i intensywność, ułatwione dzięki szybkim zmianom technologicznym i globalnym wzajemnym połączeniom.

Hybrydowy to – zgodnie z definicją słownika języka polskiego – „będący wynikiem pomieszania dwóch gatunków, ras, rodzajów”[4]. Definicja ta wskazuje, jak zauważa M. Kwiecińska, że coś, co ma charakter hybrydowy powstało z dwóch innych całkowicie odmiennych form w celu utworzenia nowej (w zamierzeniu – doskonalszej, lepszej i skuteczniejszej, bo łączącej cechy tworzących ją dwóch komponentów). Pojęcie powszechnie używane było tradycyjnie w biologii, językoznawstwie, ale także coraz

[2] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO – Polityki i instrumenty UE oraz NATO,* seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

[3] F. Hoffman, *Conflict in the 21st Century: The Rise of the Hybrid Wars,* https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 29 IV 2022], za: M. Piekarski *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych,* „Terroryzm – studia, analizy, prewencja” 2022, s. 74.

[4] M. Kwiecińska, *Nowy wymiar konfliktów zbrojnych: konflikt hybrydowy a konflikt pełzający*, Doctrina Studia Społeczno-Polityczne 13/2016, Akademia Sztuki Wojennej, Wydział Zarządzania i Dowodzenia, http://www.doctrina.uph.edu.pl/stara/doctrina_2016/6_Kwiecinska.pdf [dostęp: 4.11.2020].

powszechniej w innych dziedzinach i obszarach (np. technice – napędy hybrydowe). Hybryda, kierując się analogią do świata zwierząt, oznacza więc mieszańca łączącego cechy różnych osobników. Niektóre amerykańskie organizacje sfery bezpieczeństwa i obrony preferują termin *pełne spektrum operacji* (*full spectrum operations*), gdyż oddaje to pełny charakter różnorodnych działań (od klasycznych po nieregularne).

W sytuacji utrzymywania się względnej równowagi sił na arenie międzynarodowej i braku otwartego konfliktu zbrojnego pomiędzy mocarstwami (*rozproszona zimna wojna*), ataki hybrydowe stanowią coraz istotniejszy oręż, który ma charakter zastępczy – ale nie mniej groźny – względem konwencjonalnych środków charakterystycznych dla konfliktów zbrojnych i tradycyjnego pola bitwy. Co więcej, zdarza się, że samo tylko zastosowanie działań hybrydowych wystarcza, aby zdecydować o pomyślnym dla danego kraju rozstrzygnięciu danego sporu międzynarodowego (np. o dane terytorium).

Przykładem zagrożeń hybrydowych (ang. *Hybrid Threats, HT*) było zajęcie Krymu przez Rosję po zastosowaniu – w opinii wielu ekspertów – właśnie taktyki hybrydowej w 2014 r., a także ingerencja w wybory prezydenckie w USA w 2016 r. oraz w proces wyborczy i referenda we Francji, w Czechach, Czarnogórze[5]. Zagrożeniem są tu m.in. sztucznie wykreowane przez państwo A ośrodki generujące fałszywe informacje (dezinformację) ukierunkowaną na kraj B, zwłaszcza w internetowych środkach masowego przekazu i mediach społecznościowych (tzw. fermy / fabryki trolli). W takich konfliktach przeciwnikiem państwa może być także podmiot pozapaństwowy.

Elementy zagrożeń hybrydowych można odnaleźć analizując także działania wojenne w Syrii między siłami prezydenta Baszara al-Asada, a zbrojną opozycją, które rozgrywały się od 2011 r. przy udziale państw trzecich. Rosja, jak wykazały wyniki badań, toczyła tam wojnę hybrydową, która byłą realizowana przez łączenie zdolności wojskowych,

[5] Konflikt migracyjny na granicy polsko-białoruskiej w 2021 r., jak wynika z dostępnych informacji, należy oceniać w kategoriach działań hybrydowych. Aparat państwowy oraz instytucje bezpieczeństwa Białorusi były aktywnie zaangażowane w przerzut tysięcy osób z regionu Bliskiego Wschodu, którzy następnie byli celowo kierowani na granicę z Polską (oraz z Litwą). W rezultacie następowała eskalacja sporu granicznego w ważnym strategicznie regionie (wschodnia flanka NATO i granica zewnętrzna UE). Temu procederowi towarzyszyła inspirowana przez władze w Mińsku agresywna kampania dezinformacyjna, która przedstawiała Polskę i Litwę, jako kraje łamiące prawo międzynarodowe, dyskryminujące „uchodźców".

dyplomatycznych i medialnych. Taktyka ta miała za zadanie osiągnąć założone cele przy użyciu ograniczonego zaangażowania zbrojnego Federacji Rosyjskiej[6].

Pandemia COVID-19 także jest wykorzystywana przez niektóre kraje do aktywności hybrydowej, w tym do szerzenia dezinformacji ukierunkowanej na osłabienie, dezorientację i destabilizację obiektu wybranego za cel. Pandemia COVID-19, która objęła praktycznie wszystkie państwa na świecie, służy przykładem wykorzystania przez niektóre państwa, organizacje czy grupy interesu realnych wydarzeń do zastosowania i wzmocnienia skutków działania stosowanej przez te podmioty taktyki hybrydowej. Wysoki stopień zainteresowania szerokich mas społecznych tematyką pandemii oraz ich względnie ograniczona wiedza o mechanizmach dezinformacji czynią organizm państwowy wrażliwym na tego typu zagrożenie. Wiąże się z tym trudność w zakresie wypracowania koniecznych metod przeciwdziałania temu potencjalnie destrukcyjnemu w skutkach zagrożeniu.

Pewne związki z tematyką zagrożeń hybrydowych można też dostrzec w innych wrogich działaniach mających charakter hybrydowy (np. osłabianiu waluty jednego państwa poprzez sztuczne, nierynkowe działania lub wprowadzanie walut alternatywnych lub kryptowalut, niszczeniu wizerunku danego kraju poprzez oskarżanie go o fikcyjne czyny).

NATO opracowało strategię dotyczącą swojej roli w przeciwdziałaniu wojnie hybrydowej i jest gotowe do obrony Sojuszu i wszystkich sojuszników przed jakimkolwiek zagrożeniem, czy to konwencjonalnym, czy hybrydowym[7]. Sojusz Północnoatlantycki definiuje wojnę hybrydową, jako użycie taktyki w celu wykrycia i wykorzystania słabości (przeciwnika) za pomocą środków pozamilitarnych (np. politycznego, informacyjnego czy ekonomicznego zastraszania i manipulacji) popartych groźbą użycia konwencjonalnych i niekonwencjonalnych środków militarnych. Definicja ta powstała w odpowiedzi na powodujące zagrożenie bezpieczeństwa państw członkowskich Sojuszu Północnoatlantyckiego, które przyniósł rosyjsko-ukraiński konflikt i ekspansja Państwa Islamskiego (Daesh, ISIS)[8].

[6] A. Heistein, V. Michlin-Shapir, *Russia's Hybrid-Warfare Victory in Syria* https://nationalinterest.org/feature/russias-hybrid-warfare-victory-syria-16273 [dostęp: 24.01.2021].

[7] *NATO's response to hybrid threats*, strona internetowa NATO, https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=uk [dostęp: 3.02.2021].

[8] M. Kwiecińska, op. cit.

Zagrożenia hybrydowe, zgodnie z definicją NATO, łączą w sobie środki militarne i cywilne oraz jawne i ukryte (*overt and covert*). Zaliczyć można do nich dezinformację, cyberataki, presję gospodarczą, użycie nieregularnych grup zbrojnych (tzw. zielone ludziki) oraz tradycyjnie pojmowanych sił zbrojnych[9]. Warto odnotować, że wiele z tych zjawisk, w tym zagrożenia cybernetyczne, nie jest czymś nowym w konfrontacji międzynarodowej, ani krajowej (walki o władzę). Z wrażliwości systemów komputerowych na ataki cybernetyczne zdawano sobie sprawę od wprowadzania tego typu sprzętu na potrzeby sil zbrojnych. W 1975 r. amerykański resort obrony powołali tzw. Brygady Tygrysa, które, testując zabezpieczenia, włamały się i opanowały wszystkie używane wówczas systemy komputerowe[10].

Jednym z najpoważniejszych zagrożeń hybrydowych jest obecnie dezinformacja. Polska, wraz z innymi krajami sojuszniczymi, wprowadziła rozwiązania mające przeciwdziałać dezinformacji. Szczególnie aktywne w zakresie przeciwdziałania dezinformacji było – powstałe w Rydze w 2014 r. – natowskie Centrum Doskonałości ds. Komunikacji Strategicznej (NATO StratCom COE), wśród którego założycieli znalazła się Polska[11].

Aktywna na tym polu jest też Unia Europejska. 29 października 2019 r. Komisja Europejska (KE) zaprezentowała pierwsze sprawozdania z realizacji *Kodeksu* postępowania w zakresie zwalczania dezinformacji. KE dostrzegła poczynione przez sygnatariuszy postępy, zwracając jednocześnie uwagę, że wciąż jest wiele do zrobienia w kwestii przeciwdziałania zagrożeniom[12]. Jednocześnie, UE prowadziła działania w zakresie podniesienia poziomu wiedzy i przygotowania przedstawicieli państw członkowskich w zakresie przeciwdziałania dezinformacji w postaci specjalnych briefingów.

Parlament Europejski opublikował 10 października 2019 r. rezolucję w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych. Wskazano w niej, że ingerencja wyborcza w jednym państwie

[9] B. Beaulieu, D. Salvo, *NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence,* German Marshall Fund of the United States Jul. 9, 2018 https://www.jstor.org/stable/resrep18856 [dostęp: 23.10.2020].

[10] N. Polmar, T. B. Allen, *Ksiega szpiegow. Encyklopedia*, Warszawa 1997, s. 568-569.

[11] R. Babraj, *Dezinformacja w dobie cyfrowej rewolucji*, 19 maja 2020 https://cyberpolicy.nask.pl/dezinformacja-w-dobie-cyfrowej-rewolucji/ [dostęp: 20.11.2020].

[12] Tamże.

członkowskim wpływa na całą UE. Dlatego niezbędne jest przygotowanie strategii oraz ram prawnych dla zwalczania zagrożeń hybrydowych. Parlament zaapelował też o większe finansowanie krajowe i europejskie na komunikację strategiczną[13]. Z kolei w maju 2019 r. Krajowa Rada Radiofonii i Telewizji przeprowadziła monitoring reklam politycznych umieszczanych na Google, Twitterze i Facebooku przed wyborami do Parlamentu Europejskiego. Działanie to odbywało się w ramach grupy zadaniowej funkcjonującej w ERGA (*European Regulators Group for Audiovisual Media Services*)[14].

W 2019 r. w Ministerstwie Spraw Zagranicznych utworzono komórkę odpowiedzialną za identyfikację, przeciwdziałanie i reagowanie na kampanie dezinformacyjne. W Ministerstwie Spraw Zagranicznych uruchomiony został również system RAS (*Rapid Alert System*)[15], który ma na celu wymianę informacji na temat działań dezinformacyjnych między krajami członkowskimi UE i NATO[16].

Aktywny na polu przeciwdziałania dezinformacji był również NASK PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy). W 2019 r. rozbudowano stronę www.BezpieczneWybory.pl, przeprowadzono warsztaty dla komitetów wyborczych oraz badanie opinii o dezinformacji w sieci. Ważnym wkładem był także raport *Dezinformacja w dobie rewolucji cyfrowej,* opracowany przy współpracy z najważniejszymi ośrodkami przeciwdziałającymi dezinformacji w kraju[17].

W obszarze zagrożeń hybrydowych następują zmiany. Rośnie skuteczność wykorzystania zagrożeń hybrydowych w podważaniu zaufania publicznego do instytucji demokratycznych, kwestionowaniu podstawowych wartości społeczeństw, zdobywaniu wpływów i władzy geopolitycznej oraz wpływaniu na zdolność podejmowania decyzji. Chociaż zagrożenia hybrydowe te od dawna dominują w krajobrazie bezpieczeństwa w Europie, są cały czas ulepszane i zasilane nowymi narzędziami, koncepcjami, innowacjami i technologiami, które w bezprecedensowy sposób wykorzystują luki w określonych obszarach tak bezpieczeństwa międzynarodowego, jak i wewnętrznego państwa.

---

[13] Tamże.

[14] Tamże.

[15] *Factsheet: Rapid Alert System*, UE marzec 2019 https://eeas.europa.eu/headquarters/headquarters-homepage_en/59644/Factsheet:%20Rapid%20Alert%20System [dostęp: 9.03.2022].

[16] A. Wygodny, *Strategia Bezpieczeństwa Narodowego z perspektywy cyberprzestrzeni,* Fundacja Instytut Bezpieczeństwa i Strategii, 10.06.2022 https://fibis.pl/strategia-bezpieczenstwa-narodowego-z-perspektywy-cyberprzestrzeni/ [dostęp:9.03.2022].

[17] R. Babraj, *Dezinformacja w dobie cyfrowej rewolucji…*

Unia Europejska dostrzega pewne związki między zagrożeniami hybrydowymi i międzynarodową przestępczością zorganizowaną. Transnarodowa przestępczość zorganizowana, jak wykazały wyniki badań, ma budżet dwukrotnie większy niż wszystkie budżety wojskowe razem wzięte. Istotna jest ocena jaki zakres wpływów i władzy mogą pozyskać (kupić) podmioty niepaństwowe (i kto ma na nie ewentualnie wpływ, przez kogo mogą być zadaniowane i do jakich celów).

Co istotne, w kontekście określania skutecznych strategii przeciwdziałania atakom hybrydowym, podmioty je stosujące mogą często osiągnąć pożądane cele bez pełnej eskalacji, operując niejako „poza radarem". Niewątpliwie są to ważne czynniki utrudniające ich wykrycie i usprawnianie skutecznych metod przeciwdziałania nowym wymiarom omawianych zagrożeń. Duża zmienność w czasie zagrożeń hybrydowych – wynikająca z innowacyjnych taktyk przeciwnika – stanowi także wyzwanie dla odpowiedzialnych za bezpieczeństwo instytucji i służb, z uwagi na, ich sposoby funkcjonowania i ograniczenia (wynikające m.in. z uregulowań prawnych, koniecznych procedur, biurokracji, rozmycia priorytetów). Konieczność stałego dostosowania środków odpowiedzi do nowych zagrożeń jest dostrzegana zarówno w Polsce, jak i w innych krajach. „Generałowie najczęściej walczą przygotowując się do poprzedniej wojny", jak przypomniał gen. Rajmund Andrzejczak Szef Sztabu Generalnego WP, odnosząc się do problemu nieadekwatnego do potrzeb poziomu przewidywania zagrożeń ze strony dowódców. Wskazał przy tym na niezbędne wyważenie modernizacji środków obrony przed nowymi zagrożeniami, ale równocześnie utrzymanie zdolności tradycyjnego pola walki (strategia obronna i siły konwencjonalne)[18]. Doskonalenie środków ochrony przed zagrożeniami hybrydowymi powinno zatem być postrzegane, jako niezbędne uzupełnienie w kontekście wzmacniania całkowitych zdolności obronnych państwa.

Identyfikacja sposobów usprawnienia przeciwdziałania zagrożeniom hybrydowym dotyczy szeregu zakresów problemowych. Precyzując, wskazane zostały wytypowane działania usprawniające dotyczące m.in. obszarów: strategicznego (wzmocnienie zdolności odstraszania), politycznego (pozyskiwanie sojuszników) i edukacyjnego.

[18] R. Andrzejczak, J. Bartosiak. *Wyzwania wschodniej flanki NATO*, debata w ramach programu Układ Sił z dnia 10.12.2020, https://www.youtube.com/watch?v=uJe5Z9INqX8 [dostęp: 11.12.2020].

W niniejszej pracy odpowiedziano na pytanie (główny problem badawczy) – w jaki sposób usprawnić sposoby przeciwdziałania aktualnym oraz potencjalnym zagrożeniom hybrydowym? Na potrzeby rozprawy, badaniom zostało poddane całe spektrum zagrożeń ze strony czynników hybrydowych. Badania prowadzono z perspektywy doskonalenia sposobów przeciwdziałania zagrożeniom hybrydowym w Polsce. Analiza przypadków zagranicznych miała na celu dostarczenie wzorców i mechanizmów wzmocnienia systemu reagowania na zagrożenia hybrydowe współczesnych państw, zwłaszcza w krajach małych i średnich, jak Polska.

Niniejsza rozprawa składa się z rozdziału pierwszego, w którym zaprezentowano założenia badawcze rozprawy, w tym – cel i problemy badawcze, hipotezy wstępne, przedmiot badań, ograniczenia oraz metody, techniki i narzędzia badawcze.

W rozdziale drugim dokonano charakterystyki zagrożeń hybrydowych przez zdefiniowanie pojęć, omówienie specyfiki konfliktu hybrydowego z użyciem przykładów zagrożeń hybrydowych i ich znaczenia dla bezpieczeństwa państwa. Z uwagi na duże znaczenie kwestii analizy przypadków działań hybrydowych w czasie konfliktów, w dalszych podrozdziałach zaprezentowano dwa studia przypadku w tej domenie. Pierwszym z nich było zaprezentowanie elementów zagrożeń hybrydowych w czasie wojny w Syrii od 2011 r. (między siłami prezydenta Baszara al-Asada, a zbrojną opozycją). W drugim studium przypadku przedstawiono rolę działań hybrydowych w czasie konfliktu na Ukrainie (Krym, Donbas – od 2014 r.).

W rozdziale trzecim przedstawiono rozwiązania w zakresie przeciwdziałania zagrożeniom hybrydowym w Polsce i na świecie. Mając na uwadze poszukiwanie sposobów usprawnienia krajowych rozwiązań prawnych i instytucjonalnych w zakresie przeciwdziałania zagrożeniom hybrydowym, przeanalizowano podejście do przeciwdziałania zagrożeniom hybrydowym dwóch organizacji międzynarodowych: UE i NATO, a także wybranych krajów pozaeuropejskich: Izraela, Australii i Nowej Zelandii.

W rozdziale czwartym ujęto wyniki badań dotyczące potrzeby usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym. Wskazano na znaczenie dynamiki występowania zagrożeń hybrydowych, które cechuje duża zmienność i nieprzewidywalność. Odnotowano także wpływ nowych i prognozowanych zagrożeń hybrydowych na bezpieczeństwo współczesnego państwa.

Możliwości poprawy sposobów przeciwdziałania zagrożeniom hybrydowym są tematem rozdziału piątego. Wypracowano rekomendacje odnośnie strategicznego podejścia do kwestii przeciwdziałania zagrożeniom hybrydowym (wzmocnienie konwencjonalnych i niekonwencjonalnych zdolności odstraszania), a także wskazano na sposoby usprawnienia mechanizmów prawnych i praktycznych systemów reagowania na zagrożenia hybrydowe (m.in. – wzmocnienie zdolności obronnych instytucji i służb odpowiedzialnych za bezpieczeństwo wewnętrzne). Podkreślono także rolę innych instrumentów, których wdrożenie podniesie zdolności przeciwdziałania zagrożeniom hybrydowym (kampanie społeczne uświadamiające o zagrożeniach, przeciwdziałanie dezinformacji w mediach społecznościowych, intensyfikacja współpracy międzynarodowej w zakresie wykrywania i zwalczania zagrożeń hybrydowych).

1. Założenia badawcze

Procesy badań naukowych, jak zauważył Jerzy Apanowicz, były zastępca szefa sztabu Marynarki Wojennej do spraw naukowo-badawczych, stosuje się „w każdej dziedzinie, dyscyplinie i specjalności naukowej. Wiedza oraz działalność ludzka zawarta w systemie nauki jest złożona i wielostronnie uwarunkowana, dlatego też jedynie świadomie i celowo zastosowane procedury badawcze są w stanie zapewnić podstawowe funkcje badań naukowych”[19].

Zadaniem i wynikiem badań naukowych, w ocenie J. Apanowicza, powinien być zawsze „nowy i wymierny wytwór. Wytworem tym może być wyjaśnienie (rozwiązanie) problemu społeczno-gospodarczego, wychowawczego, technicznego, prawnego (…) lub stwierdzenia i ustalenia nieznanych wartości i związków między przedmiotami, organizacjami, strukturami, procesami i innymi komponentami (parametrami) badanych zjawisk”[20].

Twórcze badania naukowe, jak dowodzi J. Apanowicz, powinny cechować się „nowością myśli, ich unikalnością, oryginalnością, niepowtarzalnością i wymierną wartością, a w tym przede wszystkim rozwiązywać lub umożliwiać poznanie faktów, zjawisk i procesów (…) dotychczas nieznanych lub mało znanych, dotychczas w pełni niewyjaśnionych”[21]. Zadaniem badań naukowych jest więc, w ocenie J. Apanowicza, „teoretyczne i empiryczne wyjaśnianie lub odzwierciedlanie realnej rzeczywistości w określonych obszarach wiedzy ludzkiej i naukowej działalności człowieka”[22].

Badania naukowe, jak wskazuje Tomasz Majewski, zaczyna się od sformułowania problemów, które wyniknęły z sytuacji problemowej. To właśnie problem badawczy w znacznym stopniu określa zakres prac badawczych. Dotyczy to wszystkich etapów tego procesu w tym m.in. zakresu i organizacji prac oraz wyboru metod[23].

[19] J. Apanowicz, *Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne*, Difin 2005, s. 38-39.

[20] Tamże, s. 38-39.

[21] Tamże.

[22] Tamże.

[23] T. Majewski, *Miejsce celów, problemów i hipotez w procesie badań naukowych*, AON 2003, s. 44-45.

1.1. Cel i problemy badawcze

Podstawowym celem pracy badawczej jest wielostronne i wnikliwe poznanie określonej kategorii zjawisk. Badania, których wyniki zostały przedstawione w formie niniejszej dysertacji, miały na celu zidentyfikowanie charakteru zagrożeń hybrydowych, pokazanie aktualnych metod przeciwdziałania im zarówno w Polsce, jak i na forum międzynarodowym oraz wskazanie możliwości doskonalenia sposobów przeciwdziałania zagrożeniom hybrydowym. Badania uwarunkowań zagranicznych związanych ze współpracą międzynarodową dotyczącą przeciwdziałania zagrożeniom hybrydowym – w ramach NATO, UE i innych struktur – były prowadzone w kontekście wypracowania usprawnień systemu przeciwdziałania zagrożeniom hybrydowym w Polsce.

Główny problem badawczy sformułowany został w postaci pytania, w jaki *sposób usprawnić sposoby przeciwdziałania aktualnym oraz potencjalnym zagrożeniom hybrydowym?* Udzieleniu odpowiedzi na tak skonstruowany główny problem badawczy, posłużyło rozwiązanie problemów szczegółowych, ujętych w postaci pytań:

1. Jaka jest specyfika konfliktu hybrydowego?
2. Jakie są aktualne oraz prognozowane zagrożenia związane z użyciem środków hybrydowych?
3. Jakie są aktualne sposoby przeciwdziałania zagrożeniom hybrydowym?
4. Jakie czynniki decydują o potrzebie usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym?
5. Jakie rozwiązania, w jakich obszarach i w jakim zakresie należy wprowadzić, aby zwiększyć skuteczność przeciwdziałania zagrożeniom hybrydowym?

1.2. Wstępne hipotezy

Wartościową charakterystykę istoty hipotez przedstawił Jacek Andrzej Piwowarski, reprezentujący Wyższą Szkołę Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, który stwierdził, iż są to „pewne domysły, stwierdzenia, które odpowiadają na nasze pytania, nawiązujące do kwestii dlaczego oraz w jakim sensie takie, a nie zupełnie inne fakty czy też zdarzenia zachodzą. Opierając się na wcześniej przyjętych założeniach,

hipotezy pozwalają nam wyjaśnić zjawiska, procesy i fakty w zakresie nakreślonych przez badającego zagadnień. Punktem wyjścia do rozpoczęcia badań najczęściej są przypuszczenia i domysły, że pośród różnych elementów zachodzą poszczególne związki (…)[24]."

Analizując literaturę przedmiotu, wyniki badań prowadzonych w zakresie nauk pokrewnych, jak również wiedzę i doświadczenie zawodowe autora, sformułowano główną i cząstkowe hipotezy badawcze.

W odpowiedzi na główny problem badawczy przyjęto, że usprawnienie sposobów przeciwdziałania aktualnym oraz potencjalnym zagrożeniom hybrydowym wymaga wielokierunkowych oddziaływań, w tym wprowadzania, doskonalenia i aktualizowania koncepcji strategicznych (w tym zwłaszcza doktryny odstraszania) i mechanizmów ich praktycznego wdrażania, ćwiczeń, współpracy międzynarodowej, a także wykrywania luk w systemie bezpieczeństwa państwa oraz ich neutralizacji.

Zagrożenia hybrydowe łączą w sobie różne rodzaje zagrożeń (konwencjonalne, nieregularne, cybernetyczne i inne). Generujący dane zagrożenie hybrydowe podmiot (kraj, grupa przestępcza) łącząc tradycyjne operacje siłowe / zbrojne z ukrytymi, realizowanymi w sposób niejawny wysiłkami wywrotowymi, agresor zamierza często uniknąć przypisania mu odpowiedzialności lub odpowiedzi (zemsty).

Aktualne zagrożenia związanie z użyciem środków hybrydowych dotyczą szeregu istotnych dla funkcjonowania państwa obszarów i można do nich zaliczyć: dezinformację, cyberataki, presję gospodarczą, groźbę użycia lub użycie nieregularnych grup zbrojnych (tzw. zielone ludziki) oraz tradycyjnie pojmowanych sił zbrojnych, aktywność międzynarodowej przestępczości zorganizowanej i terroryzmu, inspirowanie lub przygotowanie szkodzących danemu krajowi incydentów, innej działalności przestępczej), wykorzystanie mniejszości narodowych do działań antypaństwowych.

Sposoby przeciwdziałania zagrożeniom hybrydowym są zależne od taktyki stosowanej przez przeciwnika i muszą być na tyle elastyczne, aby zapewnić skuteczną odpowiedź / obronę. Możliwości przeciwdziałania dezinformacji polegają na zwiększeniu świadomości społecznej oraz wzmacnianiu prawdziwego, korzystnego dla danego państwa przekazu informacyjnego w mass mediach oraz głównie w mediach społecznościowych.

[24] J. A. Piwowarski, *Metodologiczne i badawcze założenia pracy dyplomowej z dyscypliny nauk o bezpieczeństwie – przykład*, „Security, Economy & Law" 4/2019 (XXV), s. 26 –39, DOI: 10.24356/SEL/25/2, http://security-economy-law.pl/wp-content/uploads/2020/05/SEL-25_26-39.pdf [dostęp: 10.11.2022], s. 28

Może to przybierać postać kampanii informacyjnych. Inne metody opierają się na zdolnościach przeciwdziałania atakom ze strony mniejszości narodowych, grup terrorystycznych lub innych inspirowanych zewnętrznie aktorów.

Do czynników, które decydują o potrzebie usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym można zaliczyć ich specyfikę, wyjątkową naturę, a co za tym idzie, trudność w ich wykrywaniu oraz niwelowaniu / neutralizacji ze strony właściwych służb i instytucji państwowych, które są przygotowane w głównej mierze do zwalczania tradycyjnych zagrożeń. Nowe i prognozowane zagrożenia hybrydowe wymagają od instytucji i służb odpowiedzialnych za bezpieczeństwo narodowe wzmożonych wysiłków oraz skutecznych i często nieszablonowych działań.

Głównym, najbardziej skutecznym sposobem usprawnienia przeciwdziałania zagrożeniom hybrydowym jest wzmocnienie zdolności odstraszania państwa w zakresie ofensywnych i defensywnych zdolności militarnych i cywilnych oraz odpowiednie przygotowanie społeczeństwa. Ponadto, w związku z dynamicznie zmieniającymi się narzędziami używanymi do walki hybrydowej, zagrożenia tego rodzaju wymagają zarówno udoskonalonego monitorowania przez służby państwowe, jak i tzw. działań *miękkich* polegających np. na zwiększaniu świadomości społecznej i odporności na ataki (*resilience*). Istotne jest dostosowywanie mechanizmów prawnych oraz adaptacja praktycznych systemów reagowania na coraz bardziej złożone i częste zagrożenia tego rodzaju. Usprawnienia dotyczyć powinna współpraca międzynarodowa. Celowe byłoby zwiększenie koordynacji wspólnej odpowiedzi na tego rodzaju zagrożenia ze strony organizacji międzynarodowych lub sojuszy z udziałem Polski.. Zwiększona może być ponadto intensywność i skuteczność przeciwdziałania dezinformacji oraz zwalczanie jej społecznych skutków.

1.3. Przedmiot badań

Przedmiot badań naukowych, jak wyjaśnił J. A. Piwowarski, mogą stanowić „informacje, procesy, obiekty, osoby i grupy ludzkie, zjawiska, struktury, motywacje, osobowość, wiedza, postawy i doświadczenia konkretnych ludzi czy grup społecznych, a zatem elementy i działania podlegające wyjaśnieniu i opracowaniu w toku procesu badań. Określając przedmiot badań, należy wskazać dodatkowo wszelkie zjawiska i procesy, którym

ów przedmiot podlega i które są istotne w kontekście formułowanych przez naukowca pytań badawczych. W dziedzinie nauk społecznych i tym samym w ich dyscyplinie, jaką są nauki o bezpieczeństwie, przedmiotem badań jest szeroko rozumiana rzeczywistość społeczna. Składają się na nią twory materialne / obiekty – jak nazwa wskazuje podmioty, przedmioty, instytucje, struktury, rzeczy, które są namacalne; oraz twory idealne / zjawiska – stosunki, procesy, relacje, związki, zależności, które mają charakter niematerialny[25].”

W badaniach, których wyniki prezentuje niniejsza rozprawa, ich przedmiotem objęto zagrożenia hybrydowe oraz sposoby przeciwdziałania tym zjawiskom. Pod tym kątem obiektami badań były:

- literatura tematyczna,
- unormowania prawne,
- incydenty, konflikty i wojny z zastosowaniem technik hybrydowych,
- informacje medialne,
- opinie ekspertów,
- inne (raporty).

1.4. Ograniczenia badawcze

Podstawowym ograniczeniem w procesie badań było założenie, że wykorzystane zostaną jedynie źródła jawne. Omawiane kwestie należały do bieżących obszarów aktywności instytucji i służb odpowiedzialnych za bezpieczeństwo w Polsce, krajach NATO i innych. Ograniczenie dostępu wyłącznie do materiałów jawnych miało szczególne znaczenie w przypadku badanego tematu z uwagi na wrażliwość tej problematyki, a co za tym idzie – niepubliczny charakter wielu kluczowych informacji o współczesnych działaniach hybrydowych.

Badania objęły mechanizmy przeciwdziałania zagrożeniom hybrydowym w Polsce, w NATO oraz UE. Przykłady rozwiązań przeciwdziałania zagrożeniom hybrydowym dotyczyły także krajów pozaeuropejskich: Izraela, Australii i Nowej Zelandii, ponieważ państwa te dostarczały modelów korzystnych z punktu widzenia poprawy sposobów przeciwdziałania zagrożeniom hybrydowym w Polsce. Wybór tych państw był podyktowany

[25] Tamże.

faktem, że nie należały one do NATO i UE, co uzupełniło proces badawczy o cenne wnioski dotyczące rozwiązań przeciwdziałania zagrożeniom hybrydowym.

Kolejne istotne ograniczenie stanowił także brak możliwości dotarcia do uczestników obu stron działań hybrydowych (atakującego i broniącego się). Objęcie badaniami przedstawicieli całej tej zbiorowości mogłoby dostarczyć bezpośrednich informacji na temat badanego zjawiska.

Ważne były też ograniczenia czasowe. Przedział czasu w ograniczeniach badawczych objął lata 2011-2014. Data początkowa była związana z rozpoczęciem się wojny domowej w Syrii, w czasie której różne strony tego konfliktu stosowały środki hybrydowe. Przedział czasowy obejmuje przy tym aneksję Krymu w 2014 r.

Ponadto, ograniczeniem była też, wzrastająca w ostatnich latach, ale wciąż stosunkowo niewielka liczba publikacji na temat zagrożeń hybrydowych, co stanowiło także jedną z głównych przyczyn niskiego poziomu wiedzy na temat sposobów przeciwdziałania tym zjawiskom.

1.5. Metody, techniki i narzędzia badawcze

Od każdej pracy naukowej wymagane jest wykazanie się charakterem badawczym. Termin metoda pochodzi od greckiego słowa *meta hodos*, co oznacza drogę do celu (*methodos* – sposób badania, sposób poszukiwania prawdy). Oznacza ono „zespół teoretycznie uzasadnionych zabiegów koncepcyjnych i instrumentalnych obejmujących całość postępowania badacza, zmierzających do rozważenia określonego problemu naukowego określony jako powtarzalny sposób rozwiązania problemu[26].”

W świetle przyjętego celu badań dla rozwiązania sformułowanych problemów badawczych zastosowane zostały wymienione w dalszej części metody teoretyczne, jakościowe. Wykorzystano metody badawcze z listy najczęściej stosowanych w ocenie J. Apanowicza (m.in. analiza, synteza, porównanie, uogólnianie i wnioskowanie)[27].

[26] *Instrukcja pisania prac dyplomowych,* Instytut Prawa, Administracji i Ekonomii Uniwersytetu Pedagogicznego w Krakowie, 2017, https://ipaie.up.krakow.pl/wp-content/uploads/2017/11/Vademecum_Seminarzysty.pdf [dostęp: 10.11.2022].

[27] J. Apanowicz, op. cit., s. 54-58.

Metody teoretyczne:

a) analiza oraz synteza danych zastanych dotyczących badanego zjawiska, na które składają się komunikaty tekstowe w postaci publikacji zwartych, artykułów naukowych oraz stron internetowych, jak również komunikaty ustne rozpowszechniane poprzez radio i telewizję;

b) porównanie otrzymanych wyników, uogólnianie i wnioskowanie na podstawie kwerendy oraz badań praktycznych.

Metody jakościowe:

a) studium przypadku (konflikty w Syrii i na Ukrainie). Zostało przeprowadzone studium przypadku, jako metoda badawcza zawierająca szeroki opis przedmiotowych konfliktów oraz ich pogłębioną ocenę. To jakościowe badanie, poprzez wykorzystanie szeregu technik gromadzenia oraz analizy danych, pozwoliło poznać naturę i mechanizmy zagrożeń hybrydowych. Metoda studium przypadku w tym ujęciu skoncentrowała się na analizie konkretnych, wyodrębnionych zdarzeń i procesów. Wśród technik stosowanych w studium przypadku znalazł się szeroki wachlarz narzędzi gromadzenia oraz analizy danych (analiza dokumentów i publikacji zwartych, źródła prasowe, internetowe, dostępne bazy danych);

b) sondaż diagnostyczny wśród przedstawicieli środowisk naukowych w Polsce przy użyciu techniki wywiadu eksperckiego, którego celem była ocena zaproponowanych możliwości usprawnienia przeciwdziałania zagrożeniom hybrydowym. Badaniu zostali poddani polscy naukowcy i praktycy zajmujący się kwestiami bezpieczeństwa narodowego, w tym przeciwdziałania zagrożeniom hybrydowym.

Badania jakościowe przeprowadzane zostały przy użyciu narzędzia w postaci kwestionariusza wywiadu, które zawarto w podrozdziale 5.3 – Ekspercka ocena zaproponowanych rozwiązań w zakresie poprawy sposobów przeciwdziałania zagrożeniom hybrydowym. Badanie sondażowe zostało zrealizowane w postaci eksperckiej oceny zaproponowanych sposobów poprawy sposobów przeciwdziałania zagrożeniom hybrydowym.

Odpowiedzi na pytania zawarte w kwestionariuszu udzieliło czterech naukowców praktyków: prof. Ryszard Jakubczak, dr Jarosław Cymerski, dr Krzysztof Malesa oraz dr Damian Szlachter. Poniżej charakterystyka zawodowa ekspertów, z której wynikają ich kompetencje w zakresie przeciwdziałania zagrożeniom hybrydowym.

Prof. dr hab. inż. Ryszard Jakubczak posiada znaczący dorobek naukowy z zakresu działań hybrydowych/wojny hybrydowej. Był przewodniczącym Komitetu Organizacyjnego Konferencji pt. *Sytuacje kryzysowe spowodowane działaniami o charakterze hybrydowym* zorganizowanej przez Rządowe Centrum Bezpieczeństwa oraz Wyższą Szkołę Policji w Szczytnie w dniu 14 stycznia 2022 r. Przedstawił na zaprezentowanej wcześniej konferencji referat pt. *Działania hybrydowe a wojna hybrydowa*. R. Jakubczak jest także autorem rozdziału pt. *System obrony terytorialnej a współczesne zagrożenia działaniami hybrydowymi* w monografii autorstwa R. Jakubczaka i Roberta M. Martowskiego pt. P*owszechna obrona terytorialna w cyberobronie i agresji hybrydowej*, Warszawa 2017 (podrozdziały: *Historyczny i współczesny kontekst hybrydowość, Hybrydowość w sztuce wojennej*). Monografia pod redakcją nadinsp. dr hab. Iwony Klonowskiej, i R. Jakubczaka pt. Wpływ działań hybrydowych na sytuacje kryzysowe, Szczytno 2023. R. Jakubczak jest także Rozdziału w powyżej monografii o tytule *Działania hybrydowe a wojna hybrydowa.* R. Jakubczak jest profesorem nauk wojskowych od 2004 r. Specjalizuje się w takich kwestiach z nauk o bezpieczeństwie jak: bezpieczeństwo narodowe/państwowe, strategie bezpieczeństwa narodowego RP, strategie obronności RP, strategia bezpieczeństwa wewnętrznego, komponenty sił zbrojnych, obrona terytorialna, wojska obrony terytorialnej, działania nieregularne, działania hybrydowe, wojna hybrydowa, terroryzm, zarządzanie kryzysowe, imprezy masowe. Jest autorem/współautorem 34 publikacji o charakterze monografii dotyczacej zaprezentowanej wcześniej problematyki i promotorem 23 doktorów.

Dr Jarosław Cymerski to absolwent Wyższej Szkoły Policji w Szczytnie oraz Akademii Obrony Narodowej w Warszawie. Doktor nauk humanistycznych w zakresie nauki o polityce. Rozprawę doktorską obronił w Akademii Humanistycznej im. Aleksandra Gieysztora w Pułtusku. Absolwent Warszawskiej Wyższej Szkoły Biznesu, gdzie uzyskał stopień Master of Business Administration. Od 26 lat jest funkcjonariuszem Biura Ochrony Rządu, obecnie Służby Ochrony Państwa w stopniu podpułkownika. Pracownik naukowy na stanowisku adiunkta Wydziału Humanistycznego Akademii Finansów i Biznesu Vistula.

Jego zainteresowania naukowe dotyczą kwestii przeciwdziałania zagrożeniom, w tym – zagrożeniom natury hybrydowej. Prace badawcze J. Cymerskiego skupiają się na dwóch obszarach. Pierwszy dotyczy problematyki związanej z funkcjonowaniem podmiotów systemu bezpieczeństwa Rzeczypospolitej Polskiej realizujących zadania w obszarze przeciwdziałania terroryzmowi i zwalczania go. W tym obszarze misją jest poszukiwanie praktycznych rozwiązań w zakresie profesjonalnego funkcjonowania formacji zapewniających ochronę przedstawicielom organów władzy. Drugi obszar poświęcony jest problematyce szeroko rozumianego bezpieczeństwa osób prawych i jednostek posiadających zdolność prawną. Jego misją jest poszukiwanie rozwiązań organizacyjnych w zakresie szacowania ryzyka i tworzenia skutecznej polityki bezpieczeństwa organizacji. Członek Rady Naukowo-Technicznej Ministra Spraw Wewnętrznych opiniującej propozycje projektów naukowo-badawczych i badawczo-rozwojowych z obszaru „Bezpieczeństwo i Obronność" realizowanych na rzecz formacji nadzorowanych przez Ministra Spraw Wewnętrznych.

Dr Krzysztof Malesa to były dyrektor i wieloletni wicedyrektor Rządowego Centrum Bezpieczeństwa, który był odpowiedzialny za ochronę infrastruktury krytycznej i współpracę międzynarodową (w tym z NATO). Szef polskiej delegacji w Komitecie Planowania Cywilnego NATO, krajowy przedstawiciel w Komisji Europejskiej w pracach nad dyrektywą CER. Nauczyciel akademicki. Z pierwszego wykształcenia językoznawca, tłumacz przysięgły języka litewskiego. Obecnie dyrektor ds. strategii bezpieczeństwa w Microsoft Polska.

Dr Damian Szlachter jest absolwentem Wydziału Nauk Społecznych Uniwersytetu Wrocławskiego na kierunku stosunki międzynarodowe. Od 2006 r. pracuje w administracji państwowej w obszarze współpracy zagranicznej oraz bezpieczeństwa państwa m.in. w takich instytucjach jak MSZ, KPRM, MSWiA. W 2019 r. w Akademii Policyjnej w Szczytnie obronił rozprawę doktorską poświęconą roli centrów koordynacji działań antyterrorystycznych w systemie bezpieczeństwa wewnętrznego państwa. Prowadzone przez niego badania naukowe koncentrują się w obszarze bezpieczeństwa wewnętrznego RP oraz roli UE w budowaniu odporności na ryzyka dla bezpieczeństwa narodowego krajów członkowskich. Jest on również ekspertem regionalnym Komisji Europejskiej (DG HOME) w zakresie oceny bezpieczeństwa antyterrorystycznego przestrzeni publicznych

i infrastruktury krytycznej (EU PSA), jak również audytorem krajowym ochrony w lotnictwie cywilnym, licencjonowanym pilotem bezzałogowych statków powietrznych oraz redaktorem naczelnym czasopisma naukowego pt. „Terroryzm – studia, analizy, prewencja“. W latach 2020-2022 pełnił również funkcję wiceprezesa Polskiego Towarzystwa Bezpieczeństwa Narodowego.

2. Charakterystyka zagrożeń hybrydowych

Zagrożenia hybrydowe obejmują całe spektrum potencjalnych działań, w tym tych charakterystycznych dla wojny konwencjonalnej, nieregularnej, cybernetycznej. W związku z utrudnionym przypisaniem odpowiedzialności za określone wrogie działania, obszar ten nazywany jest czasem „szarą strefą". Pojęcie zagrożeń hybrydowych – jak zauważa Douglas C. Lovelace – zawiera w sobie także: rebelie i powstania (*insurgency*), wykorzystanie elementów przestępczych, szantaż gospodarczy, wojny etniczne (*ethnic warfare*), instrumenty nacisku prawnego (*lawfare*) i stosowanie tanich, ale skutecznych metod mających na celu unieszkodliwienie kosztownych, zaawansowanych technologicznie sił przeciwnika. Działania w opisanym zakresie mogą być prowadzone poniżej progu wojny (np. stosowanie nieoznakowanych, trudnych do zidentyfikowania żołnierzy czy grup paramilitarnych)[28].

2.1. Zdefiniowanie pojęć

Wojnę czy działania hybrydowe można określić, jako przejaw agresji danego państwa lub aktora pozapaństwowego (np. organizacji zbrojnej, terrorystycznej), która jest realizowana poniżej progu wojny i generalnie nie za pomocną tradycyjnych narzędzi wojny konwencjonalnej (przynajmniej, nie w sposób otwarty, jawny). Jako przykład wymienia się tu m.in. „wojnę" o Krym w 2014 r. (oficjalnie niewypowiedzianą) i pojawienie się na tamtym terenie tzw. „zielonych ludzików" – nieoznakowanych żołnierzy utrudniających identyfikację przynależności do konkretnego państwa. Eksperci zachodni wskazywali generalnie, że były to jednostki wojskowe Rosji, natomiast władze w Moskwie twierdziły, iż są to lokalne siły złożone z ludności nastawionej prorosyjsko oraz spontanicznie wyposażone we własnym zakresie (m.in. w sklepach z akcesoriami militarnymi).

Istota zagrożeń hybrydowych, jak zauważają Giovanni Faleg i Nada Kovalčíková, wpisuje się w tzw. „koncepcję parasolową" grupującą wiele różnych rodzajów użycia siły i działań wywrotowych. Metody te są wykorzystywane przez podmioty państwowe lub niepaństwowe do osiągnięcia określonych celów poniżej progu wojny. Co istotne,

[28] *Terrorism. Commentary on security documents, VOLUME 141 – Hybrid warfare and the gray zone threat,* Douglas C. Lovelace, Jr. (red.), Oxford University Press, 2016, s. 9-10 (ix-x).

wykraczają one poza najczęściej spotykane narzędzia obcej ingerencji takie jak manipulacja informacją i cyberataki[29].

Pojęcie definiujące zagrożenia hybrydowe nie jest nowe. Zmieniają się jednak parametry wojny, która coraz częściej oscyluje w tzw. szarej strefie. Sun Tsu twierdził, że pokonanie adwersarza bez użycia przemocy twierdził, że pokonanie adwersarza bez użycia przemocy jest najwyższą formą sztuki wojennej. Świadczy to o długiej historii zagrożeń znajdujących się poniżej progu wojny. W czasie Ziemnej Wojny stosowano intensywnie instrumenty określane dzisiaj, jako narzędzia walki hybrydowej takie jak dezinformacja[30] czy szpiegostwo. To, co jest nowego w tym zjawisku obecnie to:

- zwiększona szybkość wydarzeń (nowe technologie, współzależność). Akcje i reakcje mogą zaistnieć w bardzo wąskim przedziale czasowym jednakże rozbudowa potencjału, aby to zaistniało, może zająć lata);
- rozszerzone spektrum (szerszy katalog środków wpływu niż wcześniej – środowisko bezpieczeństwa ewoluuje);
- wysoki poziom penetracji kręgów opiniotwórczych i decydentów (od polityków wysokiego szczebla do szeregowych ekspertów, analityków i pracowników administracji państwowej). W Europie mieliśmy do czynienia m.in. z przypadkami ujawnienia kompromitujących materiałów pozyskanych nielegalnie z telefonów polityków, co zmieniało wynik wyborczy)[31].

Jednakże, mimo pewnych nowych elementów wynikających z wysokiego poziomu informatyzacji współczesnych społeczeństw, koncepcję wojny hybrydowej, jak ocenił Michał Wojnowski, „trudno uznać za nową formę prowadzenia wojen. Pojęcie to staje się raczej narzędziem walki informacyjnej toczącej się między Zachodem a Rosją (oraz Chinami) przy – mniej lub bardziej – aktywnym udziale reszty państw na arenie międzynarodowej. Przez jego użycie wyjaśnia się własnym społeczeństwom działania

[29] G., Faleg, N. Kovalčíková, *Rising Hybrid Threats in Africa. Challenges and implications for the EU*, 3 March 2022 https://www.iss.europa.eu/content/rising-hybrid-threats-africa [dostęp 13.4.2022].

[30] Dezinformacja, jak uważa były ambasador Polski w Chinach, Tadeusz Chomicki, jest siostrą cyberbezpieczeństwa i córką hybrydy (zagrożeń hybrydowych).

[31] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

geopolitycznego oponenta, potęgując atmosferę strachu przed rzekomo nową formą działań wojennych, którą dysponuje przeciwnik[32].”

Definicja zagrożeń hybrydowych w polskim systemie prawnym podjęto m.in. w Krajowym Planie Zarządzania Kryzysowego (KPZK), który jest dokumentem o charakterze planistycznym. W KPZK zostało zidentyfikowanych 19 zagrożeń, w tym – będące przedmiotem niniejszej rozprawy – działania hybrydowe[33]. Zagrożenia hybrydowe zostały określone w dokumencie w wyczerpujący sposób jako „działania zmierzające do osiągnięcia celów politycznych i strategicznych agresora. Prowadzone są w sposób wielowymiarowy, skryty, utrudniający identyfikację przeciwnika i przypisanie odpowiedzialności za nie sprawcy. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, często rozłożone w dłuższym czasie oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora. Mogą być prowadzone przy użyciu środków politycznych, ekonomicznych, prawnych, militarnych i społecznych, w tym z wykorzystaniem różnego rodzaju kanałów komunikacji społecznej. Mogą również być prowadzone pośrednio, z wykorzystaniem lokalnych podmiotów, organizacji i osób prywatnych, co utrudnia wykrycie i przeciwdziałanie im. W ramach działań hybrydowych mogą być realizowane operacje informacyjne, psychologiczne, działania o charakterze terrorystycznym, kryminalnym, działania mające na celu zakłócenie funkcjonowania sieci i systemów informatycznych, systemu energetycznego, systemu dostarczania paliw, systemów funkcjonowania i usług telekomunikacyjnych, systemu gazowego, zdarzeń związanych ze skażeniem chemicznym na lądzie, w wodzie i powietrzu, skażeniem promieniotwórczym, zakłócenia porządku publicznego, dezinformacji. Trudność w wykryciu i zdefiniowaniu, czy dane zdarzenie wystąpiło w obszarze działań hybrydowych, spowodowana jest często charakterem tych działań, tzn. działania hybrydowe mają zwykle charakter „pełzający”. Sprzyja to trudności w ich

[32] M. Wojnowski, *Mit „wojny hybrydowej”. Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku, Przegląd Bezpieczeństwa Wewnętrznego Wojna hybrydowa - WYDANIE SPECJALNE, ABW 05.11.2015 https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html.*

[33] Pozostałe to: powódź, epidemia, skażenie chemiczne, zakłócenie funkcjonowania systemów i usług telekomunikacyjnych, zakłócenie w systemach energetycznych, paliwowych, gazowych, silny mróz, intensywne opady śniegu, huragan, pożar wielkopowierzchniowy, epizootia, epifitoza, katastrofa morska, susza, upał, skażenie radiacyjne, zbiorowe zakłócenie porządku publicznego, zdarzenie o charakterze terrorystycznym, zakłócenie w funkcjonowaniu sieci i systemów informatycznych

początkowym rozpoznaniu i zdefiniowaniu. Działania te poddają się ocenie w perspektywie dłuższego przedziału czasowego. Hybrydowość niesie za sobą złożoność i wielopłaszczyznowość, a skutki działań mogą zaistnieć zarówno na terenie całego kraju, jak i na jego części. Działania te cechują się tym, że są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego jednoznaczne zidentyfikowanie progu wojny[34].”

Zagrożenia hybrydowe nie są więc związane tylko z prognozowaniem przyszłości, ale pojęcie to jest używane do opisu sytuacji związanej z konkretnymi atakami, które już się wydarzyły. Polityka przeciwdziałania zagrożeniom hybrydowym kształtuje się w odpowiedzi na zmieniające się środowisko bezpieczeństwa i ewoluujące zagrożenia. W miarę zmian w międzynarodowym otoczeniu bezpieczeństwa do powszechnego obiegu w środowisku eksperckim państw zachodnich wprowadzono nowe pojęcia, takie jak zagrożenia hybrydowe (*hybrid threats*) oraz inne pokrewne (atak / agresja / kampania / wojna hybrydowa). Natomiast wciąż nie są to pojęcia ścisłe, które nie mieszczą się w obowiązujących ramach prawnych. Niemniej jednak szereg organizacji międzynarodowych (UE, NATO) stara się wprowadzać na swoje potrzeby definicje, które mają za zadanie określić z czym mamy do czynienia.

Mimo, ze nie ma jednej oficjalnej definicji zagrożeń hybrydowych w UE, istnieje coraz większe zrozumienie ich natury zarówno w społeczeństwach Europy, jak i unijnych instytucjach. Jednocześnie, brak zainteresowania jedną, konkretną definicją w UE wynika z dążenia państw członkowskich do pozostawienia marginesu elastyczności w zakresie kwalifikowania zagrożeń hybrydowych, które dynamicznie ewoluują. To co dziś uważamy za zagrożenia hybrydowe dzisiaj, może przybrać zupełnie inną formę w bliższej lub dalszej przyszłości[35].

Jedna z definicji zagrożeń hybrydowych zawarta w dokumencie UE z 2016 r. określa, że pojęcie to oznacza: „(…) kombinację represyjnych i wywrotowych działań, konwencjonalnych i niekonwencjonalnych metod (tj. dyplomatycznych, militarnych, ekonomicznych

[34] *Krajowy Plan Zarządzania Kryzysowego, Rządowe Centrum Bezpieczeństwa, 2022* https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego [dostęp:21.10.2022].

[35] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

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. Zazwyczaj nacisk kładzie się na wykorzystanie podatności danego celu na zagrożenia i kreowanie dwuznaczności, by utrudnić procesy decyzyjne. Kampanie dezinformacyjne prowadzone na masową skalę przy wykorzystaniu mediów społecznościowych w celu kontrolowania dyskursu politycznego lub radykalizowania postaw, rekrutacji „grup-przykrywek" i kierowania nimi mogą być nośnikiem zagrożeń hybrydowych[36]."

Sojusz Północnoatlantycki definiuje wojnę hybrydową w paragrafie 72. Deklaracji końcowej szczytu NATO w Warszawie z 2016 r. stwierdzając, że określa się tak sytuację, w której: „(…) podmioty państwowe i niepaństwowe w sposób ściśle zintegrowany stosują szeroko zakrojone, złożone i elastyczne połączenie środków konwencjonalnych i niekonwencjonalnych oraz jawnych i niejawnych środków wojskowych, paramilitarnych i cywilnych do osiągnięcia swoich celów[37]."

Sojusz wskazał także na możliwości przeciwdziałania zagrożeniom hybrydowym w ramach wspólnego wysiłku obronnego zaznaczając jednak, że ciężar przeciwdziałania zagrożeniom hybrydowym spoczywa w głównej mierze na państwie napadniętym. Odpowiadając na to wyzwanie NATO przyjęło strategię w zwalczaniu zagrożeń hybrydowych uznając, iż: „(…) podstawowy obowiązek reagowania na zagrożenia lub ataki hybrydowe spoczywa na państwie, które jest ich przedmiotem. NATO jest gotowe wspomóc sojuszników na każdym etapie kampanii hybrydowej. Sojusz i sojusznicy będą gotowi do przeciwdziałania wojnom hybrydowym w ramach obrony zbiorowej. Rada może zdecydować o powołaniu się na artykuł 5 Traktatu Waszyngtońskiego. Zgodnie z ustaleniami Sojusz zobowiązuje się do skutecznej współpracy i koordynacji wysiłków z partnerami i właściwymi organizacjami międzynarodowymi, w szczególności UE, w celu przeciwdziałania wojnie hybrydowej[38]."

---

[36] *Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej*, Komisja Europejska 2016 (JOIN/2016/018 final) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52016JC0018 [dostęp: 1.09.2022].

[37] *Deklaracja końcowa szczytu NATO w Warszawie – wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r.,* BBN 2016 https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf [dostęp: 1.09.2022].

[38] Tamże.

Jeśli chodzi o podejście UE i NATO do zagrożeń hybrydowych, definicja unijna stwierdza, że są to działania poniżej progu wojny, natomiast NATO dopuszcza tego typu zagrożenia / atak, jako wojnę prowadzoną środkami pozamilitarnymi.

Według jednej z klasyfikacji działań hybrydowych można wyróżnić zintegrowane podejście do tej problematyki obejmujące aspekty: polityczne, wojskowe, ekonomiczne, społeczne, infrastruktury i informacyjne (ang. *Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time* – PMESII-PT), które uwzględnia otoczenie fizyczne oraz czynnik czasu. W ramach tych obszarów model ten zakłada możliwość dodania podobszarów na przykład w postaci migracji czy energii.

Narzędzia działań hybrydowych obejmują zróżnicowany katalog wrogich działań, m.in.:

- zdarzenia o charakterze terrorystycznym;
- cyberataki;
- dezinformacja;
- nielegalna migracji ludności;
- blokady i dyskryminacja gospodarcza;
- spekulacje finansowe;
- incydenty graniczne;
- niezapowiedziane ćwiczenia wojskowe przy granicy państwa;
- naruszeni granicy państwowej;
- wywoływanie napięć na tle narodowościowym;
- zakłócenia systemu zaopatrzenia[39].

Cele i skutki działań hybrydowych mogą dotyczyć poszczególnych sfer funkcjonowania atakowanego kraju poprzez:

- paraliż systemów finansowych (w tym bankowych), komunikacyjnych, opieki zdrowotnej, zaopatrzenia w energię, żywność i wodę;
- zakłócania funkcjonowania struktur państwa;
- spowolnienie rozwoju gospodarczego;
- zagrożenie bezpieczeństwa przemysłowego;

[39] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

- bezpośrednie zagrożenie dla zdrowia i życia ludności;
- zagrożenie integralności terytorialnej[40].

W skrajnym przypadku działania hybrydowe mogą doprowadzić również do wystąpienia kryzysu polityczno-militarnego i przyczynić się do utraty suwerenności.

Termin wojna hybrydowa zaczął pojawiać się w publikacjach autorów amerykańskich po roku dwutysięcznym, ale został upowszechniony zwłaszcza po 2014 r., tj. od momentu anektowania Krymu przez Rosję. Precyzyjną definicję wojny hybrydowej podał Frank Hoffman, według którego „zagrożeniem hybrydowym jest jakikolwiek adwersarz używający kombinacji broni konwencjonalnej, nieregularnej taktyki, terroryzmu i przestępczości w tym samym czasie i na tym samym polu bitwy celem osiągnięcia celów politycznych[41].” Warto odnotować jednak, że ten zdefiniowany na nowo rodzaj wojny, typ zagrożenia, występował już w przeszłości.

Z kolei, strona rosyjska – jak zauważył Dariusz Łuczak, szef Agencji Bezpieczeństwa Wewnętrznego w latach 2013–2015 – postrzega wojny hybrydowe jako „skutek rozwoju amerykańskich technologii mający na celu osłabienie strategicznych oponentów USA (vide: *kolorowe rewolucje*)”. Definicja „wojny hybrydowej” jest więc niejednoznaczna. Trudno precyzyjnie określić jej charakter (wymieszanie różnych typów działań zbrojnych przez kombinację strategii i taktyki czy tylko nowe pojęcie dla określenia tradycyjnych metod rozgrywania konfliktów z użyciem nowoczesnych narzędzi często bez użycia środków militarnych (np. działań w cyberprzestrzeni). Mimo trudności interpretacyjnych trudno nie zgodzić się z D. Łuczakiem, że wojna jest po prostu wojną albo – jak chce Clausewitz – kontynuacją polityki innymi środkami[42].

Warto przytoczyć zestaw elementów wskazujących na wojnę hybrydową, jaki przedstawili Albert Karolewski i Małgorzata Rejman-Karolewska, zdaniem których charakteryzuje się on:

---

[40] Tamże.

[41] F. Hoffman, *On Not-So-New Warfare: Political Warfare vs Hybrid Threats*, “War on the Rocks”, 28 July 2014, http://warontherocks.com [dostęp 20.12.2015], podaję za: J. Hajduk, T. Stępniewski, *Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty*, Studia Europejskie, 4/2015, https://journalse.com/pliki/pw/4-2015_hajduk.pdf [dostęp: 23.11.2022].

[42] D. Łuczak, *Wojna hybrydowa*, Przegląd Bezpieczeństwa Wewnętrznego, Agencja Bezpieczeństwa Wewnętrznego, 05.11.2015 https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html [dostęp: 11.06.2022].

a) „połączeniem wielu cech;

b) omijaniem prawa międzynarodowego;

c) wykorzystywaniem słabych stron przeciwnika (nawiązanie do działań asymetrycznych);

d) równoczesnym prowadzeniem działań militarnych i niemilitarnych;

e) działaniami konwencjonalnymi i niekonwencjonalnymi;

f) połączeniem militarnego i niemilitarnego komponentu sił przeciwnika;

g) połączeniem nowych (nieodkrytych) i starych (już nie używanych) metod, technologii, technik, itp.;

h) skrytym działaniem wojsk specjalnych (często występujących bez wyraźnych dystynkcji i przynależności państwowej);

i) prowadzeniem działań przeciwko innemu państwu bez oficjalnego wypowiedzenia lub deklaracji wojny;

j) prowadzeniem działalności kryminalnej i terrorystycznej;

k) naciskami ekonomicznymi i politycznymi;

l) działalnością propagandową we własnym państwie jak i na arenie międzynarodowej;

m) dążeniem do destabilizacji państwa przeciwnika[43].”

2.2. Specyfika konfliktu hybrydowego

Współczesne zmiany w sztuce wojennej, jak pisze ukraińska badaczka Olga Wasiuta, uwarunkowane są pojawieniem się „konfliktów asymetrycznych, wojen hybrydowych, tak zwanej czwartej generacji, zwanych też konfliktami wielowariantowymi[44].”

[43] A. Karolewski, M. Rejman-Karolewska, *Konflikt hybrydowy zagrożeniem dla bezpieczeństwa granic Rzeczpospolitej Polskiej*, [w:] Przegląd Naukowo-Metodyczny Edukacja dla Bezpieczeństwa, Rok XI Numer 3/2018 (40), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2018, http://www.przeglad.wsb.net.pl/uploads/1/0/3/7/10371016/pnm_3_2018_ca%C5%81o%C5%9A%C4%86_-_druk_ostateczny.pdf [dostęp: 29.11.2022], s. 94.

[44] O. Wasiuta, *Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym*, Przegląd Geopolityczny, 17, 2016, s. 34-35, https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-e0f98f4a-5d1d-45ed-a469-918a582bb2bf/c/02-Wasiuta.pdf [dostęp: 30.11.2021].

Wojna hybrydowa, jak przypomina O. Wasiuta, łączy „militarne zagrożenie, ukrytą interwencję, tajną dostawę broni i systemów uzbrojenia, szantaż ekonomiczny, hipokryzję dyplomatyczną i manipulację w mass-mediach oraz otwartą dezinformację[45].” Państwo prowadzące wojnę hybrydową może podejmować tym samym współpracę z podmiotami niepaństwowymi w postaci ugrupowań paramilitarnych. Zlecane jest im wykonanie zadań, których nie może wykonać państwo w sposób oficjalny, jawny. Aparat państwowy ucieka się do tego typu praktyki, ponieważ jest zwykle zobowiązany do przestrzegania zarówno umów zawartych z innymi krajami, jak i wiążącego go prawa międzynarodowego (np. Konwencji Genewskiej oraz Haskiej).

Kolejną cechą wojny hybrydowej jest brak formalnego wypowiedzenia wojny. Agresor, działający za pomocą nietypowych środków, ukrywa swój udział w konflikcie. Występuje także brak wyraźnie zarysowanego frontu działań zbrojnych oraz bezpośredniego starci a dużych grup wojsk. Prowadzone są natomiast, jak zauważyła ukraińska badaczka, „liczne działania sił specjalnych, jak choćby rosyjskiego wywiadu wojskowego GRU czy tzw. separatystów, gdzie nie występują umundurowane oddziały rosyjskie, choć wiadomo, że wśród nich jest wielu wojskowych rosyjskich sił zbrojnych.” Charakterystycznym zjawiskiem jest w tym kontekście pojawianie się żołnierzy, których nie można zidentyfikować lub jest to wysoce utrudnione. Działania wojenne, jak pisze O. Wasiuta, mogą być prowadzone np. przez żołnierzy wojsk specjalnych przebranych za przedstawicieli ludności lokalnej (lub nawet – za ekipy konwojów humanitarnych). Ponadto, przeciwnik w wojnie hybrydowej jest zdecentralizowany na wzór luźno powiązanej organizacji paramilitarnej partyzanckiej[46].

Zaliczana do zagrożeń hybrydowych dezinformacja zakłóca debatę publiczną, podważa zaufanie obywateli do instytucji i mediów – a w rezultacie – może destabilizować procesy demokratyczne. Dezinformacja to dystrybucja fałszywych, możliwych do zweryfikowania treści, które są udostępniane z intencją wyrządzenia szkody lub osiągnięcia innego konkretnego celu (np. korzyści politycznych i/lub finansowych – monetyzacja na portalach streamingowych, takich jak YouTube). Mówiąc o dezinformacji należy rozróżnić

[45] Tamże.
[46] Tamże.

to pojęcie od misinformacji, która charakteryzuje nieświadome działanie[47]. Istnieją próby, aby zastąpić pojęcie dezinformacji terminem bardziej precyzyjnym, którym jest Manipulacja Środowiskiem Informacyjnym i Zagraniczna Ingerencja (ang. *Foreign Information Manipulation and Interference*, FIMI).

Do narządzi dezinformacyjnych należy manipulowanie treścią i obrazem (np. fałszowanie informacji lub edytowanie obrazów w celu wprowadzenia w błąd), tworzenie fałszywych tożsamości (ukrywanie lub błędne przypisywanie źródła – np. fałszywemu kontu w mediach społecznościowych), wykorzystanie złośliwych lub nieprawdziwych argumentów w celu uzyskania reakcji (np. operatorzy online/hackerzy – tzw. trolle – prowokujący lub nawet zastraszający użytkowników na forach internetowych), wykorzystywanie technologii w celu uzyskania przewagi, np. używanie botów do wzmacniania przekazu lub instrumentalne użycie konkretnych wydarzeń (np. ataki terrorystyczne lub wydarzenia sportowe, aby dotrzeć do jak największej liczby osób). Ponadto, państwa mogą ukrywać swoje działania hybrydowe pod osłoną sztucznie stworzonych terrorystycznych grup bojowników, które stosują – niepodlegający żadnej cenzurze w internetowych środkach masowego przekazu – przekaz informacyjny (często nie tylko fałszywy, ale także bardzo drastyczny). Dociera on bezpośrednio do opinii publicznej państwa atakowanego, a co więcej – jest powielany przez media tradycyjne nieświadome manipulacji[48].

W wyniku przeprowadzonych badań stwierdzono, że pełnej charakterystyki działań hybrydowych dostarczają działania Rosji w tym zakresie. Specyfikę rosyjskiej wojny hybrydowej przedstawił rok po aneksji Krymu przez Rosję (2014 r.) amerykański badacz i wojskowy, W. J. Nemeth[49]. Przedstawił on poniżej wymienione cechy kierowanych przez aparat państwowy Federacji Rosyjskiej działań hybrydowych.

---

[47] *Dezinformacja jako główna oś kampanii hybrydowych,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

[48] Internet „zapewnia dostęp do najbardziej wykształconej, a więc opiniotwórczej części odbiorców (…) przekaz internetowy zapewnia możliwość samodzielnej i nieskrępowanej konstrukcji jego treści, która nie podlega przecież tzw. obróbce redakcyjnej ze strony dziennikarzy przygotowujących materiał (np. eliminujących treści ciągle jeszcze uznawane za zbyt drastyczne). Terroryści zyskali zatem nowe, niejako własne medium, uniezależniając się od mediów oficjalnych. Stanowi to wzmocnienie ich przekazu, zwłaszcza, iż media tradycyjne bez wątpliwości powtórzą i dodatkowo nagłośnią przekaz internetowy". T.R., Aleksandrowicz, *Terroryzm międzynarodowy*, Warszawa 2008, s. 32.

[49] W. J. Nemeth, *Russia's State-centric Hybrid Warfare,* ICDS Diplomaatia magazine, APRIL 17, 2015, https://icds.ee/en/russias-state-centric-hybrid-warfare/

[dostęp:13.08.2022].

A. Wymiar polityczny

1. Niedopuszczenie do ograniczania własnych działań nowoczesnymi normami i reżimami politycznymi oraz prawnymi:

a) szeroka, nieprecyzyjna interpretacja prawa międzynarodowego jako strategia polityczna;

b) wykorzystywanie retoryki pokoju w odniesieniu do Rosji i przypisywanie zła przeciwnikowi;

c) zapewnienie wsparcia finansowego podmiotom politycznym i społeczeństwa obywatelskiego, które destabilizują oraz podważają system polityczny wroga;

d) wykorzystywanie wydarzeń międzynarodowych jako przykrywki lub odwrócenia uwagi do działań przeciwko innemu państwu (na przykład – Letnie Igrzyska Olimpijskie w Pekinie 2008 i Zimowe Igrzyska Olimpijskie w Soczi 2014 zostały użyte przez Rosję do ataków hybrydowych);

e) pozorowane działania o wysokiej widoczności dla międzynarodowych obserwatorów i opinii publicznej (konwoje pomocy humanitarnej, faktyczne lub fikcyjne obozy uchodźców).

2. Silny nacisk na duże zaangażowanie agentów wywiadu i tajne działania na wczesnych etapach każdej operacji:

a) zaprzeczenie wrogim działaniom hybrydowym;

b) rozmycie odpowiedzialności (wróg niejasno określony).

3. Negocjowanie, ale nie wprowadzanie zmian operacyjnych:

a) wykorzystanie mylących lub nieprawidłowych powiązań w celu wyjaśnienia działań;

b) brak określonego stanu końcowego lub kryteriów zwycięstwa.

4. Dążenie do stworzenia bardziej korzystnego dla siebie alternatywnego systemu polityczno-gospodarczego/społecznego:

a) proponowanie i propagowanie alternatyw, takich jak Nowa Architektura Bezpieczeństwa Europejskiego lub Unia Eurazjatycka.

5. Długoterminowe planowanie z możliwością zmiany celów cząstkowych zgodnie z potrzebami realizacji planu głównego:

a) wykorzystanie rosyjskich sił zbrojnych, wspieranych przez Rosję separatystów, nieoznakowanego personelu wojskowego i różnych „milicji" zarówno z Rosji, jak i spoza nią;

b) zdolność do skierowania do walki sił rosyjskich, aby wesprzeć „separatystów" lub lokalne milicje.

B. Wymiar wojskowy

1. Stosowanie niekonwencjonalnych działań wojennych, w tym tzw. „zielonych ludzików":

a) wygenerowanie uwarunkowań wymagających od zachodnich przywódców podejmowania trudnych decyzji;

b) taktyka/polityka faktów dokonanych;

c) wykorzystywanie stronników („wolontariuszy") za wynagrodzeniem lub pozyskanie w inny sposób;

d) korzystanie z sił zastępczych, takich jak Czeczeni;

e) używanie regularnych oddziałów tylko w wyjątkowych okolicznościach, a wówczas zaprzeczanie ich zaangażowaniu;

f) blokowanie otwartej dyskusji w Rosji na temat wojny (w społeczeństwie, w wojsku);

g) przekazywanie separatystom sprzętu wojskowego, w tym tego zaawansowanego technologicznie;

h) dostawy nowoczesnego sprzętu wojskowego wraz z rosyjskimi operatorami.

2. Wzmocnienie oraz podniesienie prestiżu społecznego armii:

a) zwiększenie statusu i znaczenia sił zbrojnych poprzez efektowne i dobrze widoczne dla krajowej opinii publicznej szkolenia i operacje;

b) stosowanie ćwiczeń pozorowanych w celu odwrócenia uwagi od tego, gdzie wojsko faktycznie będzie działać;

c) wykorzystywanie armii do wywierania wpływu i wzbudzania strachu na arenie międzynarodowej;

d) stosowanie taktyki wojskowej z czasów zimnej wojny (lotnictwo dalekiego zasięgu, okręty podwodne, rozmieszczenie sił lądowych) w celu wpływania na decyzje polityczne.

C. Wymiar społeczny

1. Prowadzenie polityki pseudo-patriotycznej oraz jednoczenie społeczeństwa oraz mniejszości narodowych na bazie przekonań religijnych jako narzędzi polityki zagranicznej (soft power).

2. Angażowanie się w dyplomację paszportową (wydawanie rosyjskich paszportów każdemu etnicznemu Rosjaninowi).

3. Instrumentalne wykorzystywanie XIX-wiecznej koncepcji ochrony mniejszości etnicznych poza Rosją, niezależnie od tego, ich przedstawiciele faktycznie szukają ochrony.

4. Przedstawianie się w charakterze obrońców prawdziwych wartości i moralności (w kontrze do „zgniłego, zdemoralizowanego Zachodu").

D. Wymiar gospodarczy

1. Sprawowanie kontroli nad systemem gospodarczym:

a) obecność w biznesie klasy oligarchicznej (zgodnej z celami Rosji).

2. Ustanowienie wpływów finansowych i/lub kontroli w krajach „przeciwników".

3. Aktywne zaangażowanie w dyplomację energetyczną (energia – bronią hybrydową).

E. Komunikacja strategiczna/propaganda

1. Kontrola mediów:

a) stworzenie i podtrzymywanie korzystnej dla Rosji narracji (inni są tymi „złymi", „my" walczymy o wartości);

b) zapewnienie środków komunikacji dla odbiorców krajowych i zagranicznych.

2. Stworzenie sztucznych mediów „narodowych", eliminacja wszystkich mediów niezależnych.

3. Nadrzędny plan oszustwa i propagandy ukierunkowanej na odbiorców krajowych, jak i międzynarodową opinię publiczną i decydentów:

a) Świadome angażowanie się w rozpowszechnianie dezinformacji.

Ponadto, można zaobserwować związek między działaniami hybrydowymi, a kodami geopolitycznymi, które w ocenie teoretyków geopolityki, posiadają wszystkie kraje na świecie. Chociaż kod geopolityczny nie przesądza o naturze konfliktu warto odnotować jego znaczenie w kontekście przeciwdziałania zagrożeniom hybrydowym. Każde państwo ma swój własny, charakterystyczny kod geopolityczny, w którego jego skład – jak zauważa Leszek Sykulski – wchodzi „kilka podstawowych założeń: a) określenie aktualnych i potencjalnych sojuszników oraz przeciwników, b) wypracowanie sposobów na utrzymanie sojuszników, pozyskanie potencjalnych sojuszników oraz przeciwstawienie się aktualnym i potencjalnym przeciwnikom, c) opracowanie metod i form zakomunikowania wizji geopolitycznej, powstałej wskutek zaprezentowanych wcześniej punktów, własnemu społeczeństwu oraz społeczności globalnej[50]."

W kontekście obserwowanej obecnie masowej komunikacji, jak dowodzi Piotr Lewandowski, analiza kodów geopolitycznych mocarstw, jako „elementów ich oddziaływania perswazyjnego i propagandowego na inne kraje" ma istotne znaczenie. Odpowiednio poznane teoretycznie i zoperacjonalizowane metodologicznie kody geopolityczne, w jego ocenie, są i będą w przyszłości narzędziem walki informacyjnej.

[50] L. Sykulski, *Geopolityka. Skrypt dla początkujących*, Częstochowa 2014 s. 50-51, https://depot.ceon.pl/bitstream/handle/123456789/8626/Sykulski_Leszek_Geopolityka_Skrypt.pdf?sequence=1 [dostęp: 1.12.2021].

Wynika z tego bezpośredni związek kodów geopolitycznych z zagrożeniami hybrydowymi, w tym – tymi natury informacyjnej (walka informacyjna i propagandowa, np. dezinformacja)[51].

2.3. Przykłady zagrożeń hybrydowych i ich znaczenie dla bezpieczeństwa państwa

Analiza przykładów zagrożeń hybrydowych dostarcza cennych informacji o scenariuszach oraz skali zagrożenia dla bezpieczeństwa państwa w przypadku zaistnienia różnych form ataku tego typu. Ponadto, może ona także stanowić punkt wyjścia do oceny prognozowanych zagrożeń hybrydowych.

W dwóch studiach przypadku zostały zbadane metody wpływania na sytuację bezpieczeństwa za pomocą narzędzi hybrydowych. Elementy działań hybrydowych były widoczne w czasie wojny w Syrii, która toczyła się od 2011 r. między siłami prezydenta Baszara al-Asada, a zbrojną opozycją. Stanowiły one element konfrontacji nie tylko tych dwóch głównych stron konfliktu, ale także szeregu innych państw zaangażowanych w tę wojnę. Natomiast, w czasie konfliktu na Ukrainie (Krym, Donbas – od 2014 r.). działania hybrydowe stanowiły podstawowy oręż, który umożliwił Rosji szybkie przejęcie i aneksję części terytorium.

2.3.1. Elementy zagrożeń hybrydowych w czasie wojny w Syrii od 2011 r. (między siłami prezydenta Baszara al-Asada, a zbrojną opozycją)

Termin „zagrożenia hybrydowe", zgodnie z definicją europejskiego centrum zagrożeń hybrydowych Hybrid CoE, odnosi się do działań prowadzonych przez państwo lub podmioty niepaństwowe, których celem jest wyrządzenie szkody danemu krajowi przez wpływ na jego proces decyzyjny na poziomie lokalnym, regionalnym, państwowym lub instytucjonalnym. Te działania hybrydowe mogą być ukierunkowane na atakowanie m.in. państw demokratycznych i wykorzystanie słabych punktów ich instytucji. Jako narzędzia wykorzystuje się szeroki zakres metod znajdujących się poniżej progu wykrywalności i atrybucji[52].

[51] P. Lewandowski,. *Kod Geopolityczny – Koncepcja Teoretyczna i Metodologiczna*, Politeja 16 (4(61), 2019, s. 297-315. https://doi.org/10.12797/ [dostęp: 30.11.2021].

[52] *Hybrid CoE Research Report 5*, The European Centre of Excellence for Countering Hybrid Threats, March 2022, s. 7. https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf [dostęp: 12.4.2022].

Zgodnie z definicją Hybrid CoE i Połączonego Centrum Badawczego Komisji Europejskiej (*European Commission's Joint Research Centre*) aktywność hybrydowa jest wymierzona w organizm państwowy w trzynastu obszarach. Uznano za nie następujące domeny: infrastrukturę, cyber-przestrzeń, gospodarkę, wojskowość/obronę, kulturę, społeczeństwo, administrację publiczną, wymiar prawny, wywiad, dyplomację, domenę polityczną oraz informacyjną. Każde działanie hybrydowe tego typu może obrać za cel jeden lub kilka z tych obszarów[53].

Wojnę, w tym działania hybrydowe można określić jako przejaw agresji jednego państwa lub aktora poza-państwowego (np. organizacji zbrojnej, terrorystycznej). Agresja ta, nie jest realizowana jednak za pomocną tradycyjnych narzędzi wojny konwencjonalnej, ale poprzez ukryte, prowadzone różnymi metodami, działania podprogowe – poniżej progu wojny.

Zagrożenia hybrydowe dla bezpieczeństwa współczesnego państwa przejawiają się w całej gamie działań, które mogą być wymierzone w dany kraj. Może to dokonać się m.in. przez wykorzystanie instrumentów odziaływania na opinię publiczną danego państwa będącego obiektem ataku.

Pojęcie wojny hybrydowej, niebędące określeniem nowego zjawiska, jest w ostatnich latach coraz powszechniej używane wpisując się niejako w swego rodzaju modę w świecie środków masowego przekazu. Trudno konkretnie umiejscowić w czasie początek tego zjawiska, ale można stwierdzić, że nasiliło się ono po wydarzeniach na Krymie w 2014 r., które były szeroko komentowane w zachodnich mass mediach. Jednak elementy wojny hybrydowej można było dostrzec także w czasie wojny domowej w Syrii, która wybuchła w 2011 r.[54]

Wojna domowa w Syrii ukazuje szerokie spektrum zagrożeń dla bezpieczeństwa państwa, w tym zagrożeń hybrydowych. Do kategorii tych ostatnich można zaliczyć masowe, zorganizowane często z użyciem nowoczesnych technik komunikacyjnych (np. mediów społecznościowych, łączności komórkowej) zrywy społeczne określane, jako tzw. kolorowe rewolucje, w wyniku których dochodzi już od dziesięcioleci do zmian władzy

[53] Tamże, s. 85.

[54] T. Kijewski, *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa państwa na przykładzie wojny w Syrii w 2011 r.,* [w:] *Terroryzm/Antyterroryzm #20 lat po 9/11,* W. Zubrzycki, J. Cymerski (red.) 2022, s. 194-195.

w poszczególnych krajach na świecie, w tym w Europie. Wyzwania w zakresie bezpieczeństwa w kontekście zagrożeń hybrydowych mają także elementy asymetryczności, ponieważ aparat władzy wraz z siłami porządkowymi (policja, wojsko i inne służby) staje przed koniecznością konfrontacji z zupełnie odmiennym od siebie typem przeciwnika, dużymi grupami zorganizowanych cywilów, którzy dodatkowo są obywatelami tego kraju co nadaje ich działonom większej legitymizacji i utrudnia spacyfikowanie danego nielegalnego protestu (zakładając, że faktycznie nie jest on naturalny i zasadny, jako forma społecznego oporu wobec opresyjnej władzy). Przykład wojny hybrydowej w Syrii pokazuje także istotne znaczenie elementów związanych z działalnością terrorystyczną i jej przeciwdziałaniu w tego typu sytuacji.

Dla zrozumienia kontekstu zagrożeń hybrydowych w czasie wojny domowej w Syrii pomocne jest zidentyfikowanie genezy tego konfliktu. Syria uzyskała niepodległość od Francji po zakończeniu II wojny światowej[55], w 1946 r. Po klęsce w 1949 r. przeciwko Izraelowi[56]. Syria została dotknięta serią zamachów stanu, które destabilizowały i osłabiały kraj aż do 1967 r. W jednym z nich, w 1963 r. władzę zdobyła wspierana przez ZSRR partia Baath.

Po przegranej przez Damaszek Wojnie Sześciodniowej z Izraelem, w 1970 do władzy doszedł ojciec obecnego prezydenta Baszara al-Asada – Hafiz Assad. Umocnił on swoją pozycję
w czasie tzw. Wojny Yom Kippur w 1973 r., podczas której armia syryjska odbiła niewielką część okupowanych przez Izrael Wzgórz Golan. W międzyczasie reżim al-Asada zmagał się z opozycją wewnętrzną, co trwało do 1982 r., kiedy państwo krwawo stłumiło próby rewolty ze strony Bractwa Muzułmańskiego w mieście Hama (zginęło ok. 30 tys. osób). Hafiz Asad zmarł w 2000 r. i prezydentem został jego syn Bashar[57]. Część państw zachodnich miała nadzieję, na spełnienie przez niego roli modernizatora kraju. Oczekiwania te pozostały

[55] Nawiązanie stosunków dyplomatycznych między Rzeczpospolitą Polską (rząd RP na uchodźstwie w Londynie), a Syrią nastąpiło w efekcie złożenia listów uwierzytelniających przez posła Polski w Damaszku w 1944 r.

[56] Syryjczycy byli zaangażowani we wszystkie konflikty arabsko-izraelskie, a także w wojnę domową w Libanie.

[57] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat Actor*, [w:] *Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence, Hybrid CoE Research Report 5*, The European Centre of Excellence for Countering Hybrid Threats, March 2022, s. 35 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf [dostęp: 12.4.2022].

jednak niespełnione, ponieważ nowy prezydent z czasem zaczął kontynuować autorytarne podejście administracji swojego ojca (cenzurę, inwigilację oraz przemoc wobec przeciwników reżimu). Assad wprowadzał liberalizację gospodarki zdominowanej dawniej przez państwo, ale – jak zauważali krytycy reżimu – zmiany te służyły głównie wzbogaceniu się grup interesów z powiązaniami z reżimem[58].

Syria musiała się zmierzyć z narastającą izolacją międzynarodową, która zaczęła się uwidaczniać szczególnie po atakach terrorystycznych na USA 11 września 2001 r. Autorytarna rządy władz w Damaszku (brak zgody na demokratyczne reformy w stylu zachodnim, represje opozycji) oraz przychylność wobec antyzachodnio nastawionych krajów (np. Iranu) działały tu na niekorzyść Syrii[59]. W 2002 r. Syria, pod zarzutem dążenia do uzyskania chemicznej i biologicznej broni masowego rażenia, została dodana do amerykańskiej „Osi Zła" (obok krajów, takich jak Kuba, Libia, Irak, Iran i Korea Północna). Stany Zjednoczone i Syria współpracowały, co prawda w niektórych kwestiach regionalnych, ale bilateralne stosunki pogarszały się, co przyspieszyło zwłaszcza od ok. 2008 r.[60]

W dotkniętej suszą, zubożałej, wiejskiej prowincji Daraa w południowej Syrii[61], doszło w 2011 r. do pierwszych znaczących antyrządowych protestów społecznych. Pod koniec lutego 2011 r. USA skrytykowały incydent aresztowania w mieście Daraa kilkunastoosobowej grupy syryjskiej młodzieży za antyreżimową działalność[62]. Władze tłumaczyły, że chodziło o graffiti z napisem: *„Twoja kolej, doktorze. Wolność"*, co sugerowało, że prezydenta B. Assada – z wykształcenia lekarza nauk medycznych – spotkać

[58] O. Giles, *How did the Syrian Civil War Become a Proxy War? And will it ever end?*, National Interest, 13.09.2019, https://nationalinterest.org/blog/middle-east-watch/how-did-syrian-civil-war-become-proxy-war-80716 [dostęp: 28.04.2021].

[59] O. Giles, *How did the Syrian Civil War Become a Proxy…*

[60] USA zarzucało Syrii brak efektów w przeciwdziałaniu tranzytowi zagranicznych bojowników, destabilizowanie sytuacji w Iraku i ochronę przywództwa palestyńskich grup terrorystycznych. Sankcje z sierpnia 2008 r. zablokowały eksport amerykańskich usług do Syrii i zakazały firmom z USA zaangażowania w syryjskim sektorze naftowym. Wprowadzono też zakaz importu syryjskich produktów naftowych. *Informacja na temat relacji USA z Syrią…*

[61] Kryzys ekologiczny, w ocenie niektórych komentatorów, również odegrał pewną rolę w powstaniu w Syrii. W latach 2006–2010 Syria doświadczyła jednej z największych suszy w historii tego kraju. W jej wyniku setki tysięcy rodzin rolników zostało doprowadzonych do ubóstwa, powodując masową migrację ludności wiejskiej do miast (tzw. slumsów – dzielnic nędzy). O. Giles, *How did the Syrian Civil War Become a Proxy…*

[62] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 196.

może los innych obalanych w tamtym czasie dyktatorów w wyniku *Arabskiej Wiosny*[63]. W celu ochrony reżimu, syryjskie siły bezpieczeństwa zareagowały zdecydowanie przeprowadzając aresztowania, a czasem używając przeciwko demonstrantom broni palnej. Gwałtowność reakcji władz oraz medialne nagłaśnianie zajść, nasilało protesty w Homs. Przyłączali się do nich masowo demonstranci z innych miast Syrii: m.in. z Aleppo i Damaszku, którzy przybywali niosąc wsparcie[64]. Rozpropagowywanie informacji przez opozycję – oraz przez innych hybrydowych aktorów w konflikcie, miało miejsce także z użyciem mediów społecznościowych, co okazało się efektywne. Dla przykładu, jedna z grup zachęcających do antyrządowych strajków (*Syrian Revolution 2011*) zgromadziła na portalu Facebook ponad 100 tys. obserwujących.

Podziały społeczne i etniczne wśród Syryjczyków miały wpływ na powstanie ludności przeciwko władzom. Wielu protestujących należało do większości sunnickiej w tym kraju, podczas gdy rządząca rodzina Assada była członkami mniejszości alawickiej. Alawici zdominowali siły bezpieczeństwa i nieregularne milicje, które były oskarżane o akty przemocy wobec demonstrantów i przeciwników reżimu. Administracja Assada, jak wykazały wyniki badań, inspirowała powstawanie pozarządowych komando złożonych z mniejszość alawickiej celem siania terroru wśród sunnickiej większości (np. przypadki zabójstw całych rodzin w syryjskich miejscowościach). W miarę postępu konfliktu podziały te pogłębiły się. Assad, jak dowodzą niektórzy autorzy, starał się przedstawić opozycję, jako sunnickich islamskich ekstremistów na wzór Al-Kaidy i uczestników zagranicznych spisków przeciwko Syrii. Reżim wytworzył także propagandę, która podsyciła obawy mniejszości, że opozycja w przeważającej mierze sunnicka będzie przeprowadzać represje wobec społeczności nie-sunnickich zamieszkujących Syrię[65].

Latem 2011 r. grupy demonstrantów były lepiej zorganizowane i coraz więcej z nich używało broni palnej w starciach z siłami rządowymi. Następowała eskalacja konfliktu, do czego przyczyniała się pojawiająca się po obu stronach nienawiść i chęć zemsty. Emocje te wciągały coraz większe masy ludzkie do aktywności, często z użyciem siły. Mnożyły się porwania dokonywane przez obie strony w nadziei, że uda się uwolnić część z przetrzymywanych osób. Wskazywano na działalność inspirowanych przez aktorów

[63] O. Giles, *How did the Syrian Civil War Become a Proxy…*
[64] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 196.
[65] O. Giles, *How did the Syrian Civil War Become a Proxy…*

zewnętrznych jednostek lub grup, które strzelały do obu stron konfliktu podburzając je do zaciekłości i dalszego zaogniania fali przemocy. Mieli to być w większości radykalni islamiści[66].

Kulminacja protestów miała miejsce w centrum liczącego ponad 650 tys. Homs – trzeciego pod względem wielkości miasta kraju, gdzie rozpoczęły się masowe protesty. Były one inspirowane przez kampanię w mediach społecznościowych pod hasłem *Piątek Wściekłości (Friday of Rage*) i skłoniły tysiące muzułmańskich demonstrantów do wyjścia na ulice po piątkowych modłach 18 marca 2011 r. Od tego czasu sytuacja coraz bardziej się pogarszała.

17 kwietnia 2011 r. w Homs dokonano skutecznego zamachu na Abdo Khodr al-Tallawi – syryjskiego generała wiernego prezydentowi Assadowi (zabijając również jego dwóch synów i siostrzeńca oraz publicznie bezczeszcząc ich zwłoki). Generał podróżował prywatnym autem, które zostało ostrzelane z broni palnej wraz z dwoma synami i siostrzeńcem. Z kolei, inny syryjski dowódca, Iyad Kamel Harfoush, został zastrzelony w pobliżu swojego domu. Incydenty tego rodzaju niewątpliwie wpływały na brutalne podejście władz do demonstrantów / rebeliantów.

Na początku maja 2011 r. władze użyły ostatecznie siły w celu rozpędzenia demonstrujących tłumów, które – korzystając ze swego prawa do swobody wypowiedzi – paraliżowały przy tym życie metropolii. Przedłużające się protesty były także groźne dla lokalnych władz i reżimu Assada w świetle wizerunkowym (wewnętrznym i międzynarodowym)[67]. Zginęło wiele osób i szereg obserwatorów określa ten moment jako kluczowy do zaognienia protestów oraz w efekcie – wywołania wojny domowej.

Winne eskalacji konfliktu, w ocenie amerykańskiego ambasadora w Syrii Roberta Forda (2011-2014), były syryjskie władze na czele z Assadem, które zamiast reform, uciekły

[66] S. Abed, Syria 2011: A Four Month Timeline of the Western Manufactured Uprising, The Rabbit Hole, August 15, 2017 https://sarahabed.com/2017/08/15/syria-2011-a-four-month-timeline-of-the-western-manufactured-uprising/ [dostęp: 31.05.2022].

[67] W miarę, jak protesty rosły w siłę, reżim reagował coraz bardziej zdecydowanymi działaniami, takimi jak okrążanie miast lub dzielnic, które stały się ośrodkami protestu (np. Homs). Realizowane było to za pomocą czołgów, artylerii i helikopterów szturmowych, a także szeregu działań pacyfikujących (odcinanie mediów, łączności). Rodziło to zbrojny opór niektórych grup protestujących. Damaszek, stolica i centrum administracji prezydenta Assada, pozostawała długo względnie spokojnym miejscem. Wynikało to czesiowo ze sprawnego działania syryjskich służb specjalnych odpowiedzialnych za bezpieczeństwo narodowe (w tym przypadku głównie cywilnych – General Intelligence Directorate / Idarat al-Mukhabarat al-Amma). O. Giles, *How did the Syrian Civil War Become a Proxy…*

się do rozwiązań siłowych. Z kolei, jak zaznaczył ówczesny syryjski wiceminister spraw zagranicznych Faisal Mekdad demonstracje były sterowane przez specjalnych operatorów oraz były „*w znacznej mierze zorganizowane i finansowane* z zagranicy[68]*."* Same protesty, zapasy broni palnej i cała logistyka na potrzeby wzniecenia niepokojów społecznych – w jego ocenie – były wcześniej przygotowane.

Syryjska armia starała się powstrzymać rozprzestrzenianie się protestów w kraju. Jednak kluczowe dla eskalacji sporu, jak wynika z wypowiedzi walczącego po stronie rządowej generała Mohameda Khaddour, było strzelanie przez demonstrantów z broni palnej do sił porządkowych. Musiało to rodzić – w jego ocenie – adekwatną odpowiedź zaniepokojonych o swoje życie funkcjonariuszy i żołnierzy. Wojskowy, którego umieszczono na zachodniej liście osób objętych sankcjami, oznajmił, że był ranny trzykrotnie, co zaprzeczać miało – w jego ocenie – informacjom o pokojowym charakterze protestów[69].

W czerwcu 2011 r. starcia wojsk rządowych z rebeliantami w mieście Jisr al-Shugūr przyczyniły się do migracji tysięcy uchodźców w kierunku Turcji (miasto leży około 20 km od granicy z Turcją)[70]. Większość społeczności w Jisr al-Shughour stanowili sunniccy muzułmanie (ze znaczącą mniejszością chrześcijan). W przeszłości ludność ta stawiała opór władzom centralnym, które w 1980 r. brutalnie spacyfikowały bunt w Jisr al-Shughour. Zajścia z użyciem przemocy w tym mieście, zlokalizowanym w graniczącej z Turcją północno-zachodniej części Syrii, rozpoczęły się o świcie 4 czerwca 2011 r. Napastnicy mieli opanowywać małe, położone na obrzeżach miasta posterunki policji, zdobywać w ten sposób broń oraz używać cywilów jako żywych tarcz. Telewizja państwowa poinformowała, że napastnicy byli uzbrojeni w broń średniego kalibru i granaty oraz pięć ton materiałów wybuchowych, które ukradli z pobliskiej tamy. Fakt, że zbrojne grupy paramilitarne pojawiły się na zewnątrz miasta może świadczyć o tym, że nie byli to zwykli mieszkańcy tej miejscowości niezadowoleni z rządów Assada, ale rebelianci. Do Jisr al-Shughour zostały

[68] *Everyone Should Save Syria from Falling into Hell,* Interview with Syrian Deputy Foreign Minister Faisal al Mekdad – DER SPIEGEL, by Susanne Koelbl in Damascus, SPIEGEL Gruppe, 05.02.2013, https://www.spiegel.de/international/world/interview-with-syrian-deputy-foreign-minister-faisal-al-mekdad-a-881678.html [dostęp: 1.12.2022], za: T. Kijewski, *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa państwa na przykładzie wojny w Syrii w 2011 r.,* [w:] *Terroryzm/Antyterroryzm #20 lat po 9/11*, W. Zubrzycki, J. Cymerski (red.) 2022, s. 197.

[69] O. Giles, *How did the Syrian Civil War Become a Proxy…*

[70] Tamże.

wysłane posiłki. Syryjskie czynniki rządowe podały 5 czerwca, że uzbrojone grupy nawet kilkuset rebeliantów zorganizowały zasadzkę na przybywających jako wsparcie policjantów i dokonały masakry. Śmierć miało ponieść co najmniej 120 funkcjonariuszy rządowych. Po tym wydarzeniu, porządek w mieście przywróciły siły wojskowe.

Zajścia w Jisr al-Shugūr pokazują trudność oceny sytuacji w obliczu powszechnej dezinformacji i propagandy. Warto odnotować, iż ani doniesienia strony rządowej ani opozycji o atakach nie zostały niezależnie zweryfikowane przez niezależne źródła i były nacechowane przesadnym eksponowaniem wybranych elementów, w tym zawyżaniem liczby ofiar. Pojawiało się wiele sprzecznych wersji. Dane liczbowe dotyczące ofiar podawane przez władze były kwestionowane, choć stwierdzono, że część z poległych miała odcięte głowy, co wskazywało na fundamentalistów islamskich. Opozycyjne strony internetowe informowały tymczasem, że ich protesty były pokojowe, a demonstrujący nie mieli broni. Anonimowy rozmówcy informowali zachodnie mass media (m.in. Reuters'a), że ludzie podpalili pocztę po tym, jak snajperzy ostrzelali uczestników masowego pogrzebu w sobotę, 4 czerwca 2011 r.[71] Inne relacje mówiły, że członkowie lokalnych sił bezpieczeństwa Syrii przyłączyli się do antyrządowych protestów, na co nie było jednak dowodów. Informacje te były rozpowszechniane celowo, aby obniżyć morale syryjskiej armii. Niektórzy twierdzili również, że miasto było stosunkowo spokojne, aż do czasu buntu w siedzibie bezpieczeństwa, gdzie zgłoszono tak wiele ofiar śmiertelnych. Rozstrzelani mieli zostać rzekomo policjanci, którzy odmówili otwarcia ognia do demonstrantów. Jednak niemożliwe było zweryfikowanie sprzecznych relacji o przemocy ze strony rebeliantów i strony rządowej, ponieważ władze uniemożliwiły większości międzynarodowych mediów działalność w Syrii[72].

W zadziwiająco krótkim czasie od rozpoczęcia protestów opozycja względem Assada niespodziewanie zyskała potężnego sojusznika w postaci byłych wojskowych. W lipcu 2011 r. z sił zbrojnych Syrii, jak podały zachodnie źródła informacyjne, zbiegło siedmiu oficerów, którzy stworzyli uzbrojoną formację opozycyjną – Wolną Armię Syryjską (*Free Syrian Army, FSA*), która reprezentowała świeckie środowiska umiarkowane. Chociaż FSA nie zdołała w pełni

[71] M. Karouny, *Syria to send in army after 120 troops killed,* Reuters, JUNE 6, 2011 https://www.reuters.com/article/idCATRE7553AI20110606 [dostęp: 27.05.2022].

[72] J. Landis, *What happened at Jisr al-Shagour?,* SyriaComment.com, 13.06.2011 r., https://www.joshualandis.com/blog/what-happened-at-jisr-al-shagour/ [dostęp:30.05.2022].

scentralizować różnych grup rebeliantów to pozostała główną siłą nieradykalnej opozycji względem Assada[73].

Latem 2011 r. zaczęły wyraźne zaznaczać się różnice w podejściu względem polityki władz w Damaszku ze strony sąsiadów Syrii i mocarstw światowych. USA i Unia Europejska były coraz bardziej krytyczne wobec reżimu prezydenta Assada apelując nawet o jego ustąpienie. 18 sierpnia 2011 r. sekretarz stanu USA H. Clinton wezwała prezydenta Syrii do ustąpienia stwierdzając, iż proces zmian w stronę demokracji się rozpoczął i przyszedł czas dla syryjskiego przywódcy do *„zejścia z drogi”*. Stany Zjednoczone, UE i Liga Arabska wprowadziły sankcje wymierzone w wyższych przedstawicieli administracji Assada. W gronie krajów przeciwnych Assadowi znalazły się też m.in. Katar, Turcja i Arabia Saudyjska. Władze w Damaszku mogły liczyć jednak na przychylność niektórych państw na arenie międzynarodowej, m.in. Rosji i Chin. W październiku 2011 r. kraje te rozpoczęły blokowanie przyjęcia rezolucji Rady Bezpieczeństwa ONZ, która potępiłaby represje administracji prezydenta Assada. Natomiast, Rosja – jak podkreślał z kolei przewodniczący komisji spraw zagranicznych Rady Federacji Rosyjskiej Konstantin Kosaachev – nigdy nie twierdziła, że prezydent Assad jest dobrym przywódcą, ale *„opanowanie terroru w tym kraju wymaga funkcjonującego państwa*[74]*.”*

Tabela 1. Szacunkowa siła poszczególnych uczestników wojny domowej w Syrii

Aktor konfliktu	Zaangażowane siły
Siły zbrojne Syrii (prorządowe)	Syryjska Armia Arabska wierna Assadowi (Syrian Arab Army, SAA) dysponowała 220 tys. żołnierzy sił regularnych oraz 280 tys. rezerwistów. Dezercje oraz straty wojenne spowodowały utratę ok. połowy początkowego potencjału SAA. Stan liczebny syryjskiego wojska pod koniec 2017 r. wynosił według szacunków zachodnich nie więcej, jak 25 tys. żołnierzy zdolnych do działań ofensywnych (mimo

[73] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat…*
[74] Tamże.

	rządowych kampanii rekrutacyjnych). Warto jednak zauważyć, że prorządowe siły paramilitarne posiadały ok. 150-200 tys. bojowników.
Zbrojna opozycja antyrzadowa	Grupy rebeliantów Wolnej Armii Syryjskiej (Free Syrian Army, FSA) osiągnęły liczebność ok .15 tys. żołnierzy pod koniec 2011 r., ale w ciągu 2 lat urosły w siłę do 80 tys. (do 2013 r.). W 2019 r. ugrupowanie zmieniło nazwę na Syryjską Armię Narodową (SNA), ale ostatecznie uległo decentralizacji tracąc żołnierzy na rzecz innych grup. W międzyczasie, w 2015 r. arabskie milicje kurdyjskie utworzyły sojusz pod nazwą Syryjskie Siły Demokratyczne (SDF), które miały ok. 40 tys. (stan na 2019 r.).
Wojska rosyjskie	Zaangażowanie Rosji w konflikt rozpoczęło się od nalotów oraz działań nieokreślonej liczby wojsk specjalnych. Liczba żołnierzy rosyjskich osiągnęła w szczytowym okresie według niektórych szacunków ok. 13 tys. Ponadto, władze na Kremlu wykorzystały także przynajmniej 1500-2000 żołnierzy prywatnych firm wojskowych.
Iran i Hezbollah	Udział strony irańskiej w wojnie domowej w Syrii zaczął się od umiarkowanych działań w zakresie wsparcia finansowanego i dostaw uzbrojenia. Jednak od 2014 r. władze w Teheranie wysłały ok. 2,500 tysiąca bojowników celem wsparcia prezydenta Assada. Pośrednie wsparcie było jeszcze większe – sama tylko organizacja Hezbollah, uważana za jedno z wielu narzędzi irańskich, przysłała 8 tys. bojowników.
ISIS	Pod koniec 2014 r. w Syrii mogło działać nawet ponad 50 tys. bojowników ISIS. Chociaż od tego czasu ISIS utraciła zajęte wcześniej terytoria, liczba ich żołnierzy na terenie

	Syrii jest szacowana na ok. 10 tys. (może ona wzrosnąć, ponieważ ISIS kontynuuje rekrutację).

Źródło: J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat Actor,* [w:] Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence, Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf [dostęp: 12.4.2022].

Opór protestujących bardzo szybko stał się bardzo dobrze zorganizowany i groźny dla władz w Damaszku. Od września 2011 r., czyli w niespełna 6 miesięcy od wybuchu pierwszych poważniejszych protestów w Homs, uzbrojone bojówki regularnie angażowały się już w walki z wojskami rządowymi w wielu miastach Syrii. W lipcu 2012 r. rebelianci (w sile 400 ludzi uzbrojonych w karabiny AK-47 oraz granatniki) skutecznie zaatakowali Aleppo, liczące blisko 1,5 mln ludzi drugie największe miasto w Syrii, ustanawiając tam przyczółek[75]. Pod koniec 2012 r. siły rządowe odzyskały kontrolę nad częścią Aleppo, choć rebelianci utrzymali panowanie w niektórych dzielnicach (aktywni w mieście zaczęli być wówczas snajperzy).

Jednak na początku 2013 r. sytuacja wydawała się zbliżać do impasu. Antyreżimowi bojownicy umocnili się na północny kraju, ale powstrzymywały ich braki w wyposażeniu. Tymczasem siły rządowe, osłabione dezercjami, również wydawały się niezdolne do odzyskania kontroli nad utraconym terytorium[76].

Do połowy 2012 r. reżim Assada był w trudnej sytuacji: rząd stopniowo tracił kontrolę nad kolejnymi terenami, a coraz większa liczba żołnierzy dezerterowała z armii. W lipcu 2012 r., rebelianci zbliżyli się do centrum Damaszku zagrażając nawet bezpieczeństwu samego pałacu prezydenckiego. Odnotowano przypadki skutecznych ataków na osoby z najbliższego otoczenia

[75] Trudno dokładnie określić, kiedy przeważnie pokojowy ruch protestujących zmielił się w zmilitaryzowany bunt, ponieważ proces ten przebiegał płynnie. Starcia zbrojne stawały się coraz powszechniejsze. Wolna Armia Syryjska, grupa rebeliantów utworzona przez uciekinierów z armii syryjskiej, ogłosiła przywództwo nad zbrojną opozycją walczącą w Syrii, ale lokalne milicje jej nie uznawały. Latem i jesienią 2012 r. rebelianci odnieśli szereg taktycznych sukcesów. Wojska rządowe zostały zmuszone do wycofania się z obszarów na północy i wschodzie, co pozwoliło rebeliantom po raz pierwszy przejąć kontrolę nad znacznym terytorium. Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: *Syrian Civil War, Encyclopedia Britannica,* 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

[76] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 198.

Assada. W ataku bombowym zginął m.in. szwagier prezydenta, a także minister obrony i najwyższy rangą generał[77].

W miarę nasilenia walk i utraty personelu, reżim Assada doprowadził do powołania prorządowej organizacji paramilitarnej o nazwie Siły Obrony Narodowej (NDF). Były one tworzone z lokalnych milicji i chociaż początkowo miały chronić wybrane części dużych aglomeracji miejskich, to – w ramach Sił Obrony Narodowej – również zostały wysłane na linię frontu[78].

Zagraniczni sojusznicy prezydenta Assada, nie widząc szans na sukces, zwiększyli swoje poparcie dla reżimu. Przyczyniło się to do rozwoju sytuacji bezpieczeństwa w kierunku regionalnej wojny zastępczej (*proxy war*). Pod koniec 2012 i w 2013 r. działania Turcji, Arabii Saudyjskiej i Kataru w celu finansowania i zbrojenia rebeliantów stały się coraz bardziej widoczne. Cześć z zagranicznych pieniędzy trafiała do grup fundamentalistów islamskich, którzy przybywali coraz liczniej do Syrii (niektóre z nich, jak Front Nusrah, miała według zachodnich źródeł powiązania z Al. Kaidą).

Jednym z istotnych wydarzeń podczas syryjskiej wojny były wezwania do międzynarodowych działań wojskowych w Syrii po atakach z użyciem broni chemicznej na przedmieściach Damaszku 21 sierpnia 2013 r., w których miały zginać setki osób. Syryjska opozycja oskarżyła administrację Assada o przeprowadzenie ataków.

Władze syryjskie zaprzeczyły używaniu broni chemicznej i zasugerowały, że wina leży po stronie rebeliantów. Podczas gdy inspektorzy ONZ zbierali dowody w miejscach domniemanych ataków chemicznych, przywódcy USA, Wielkiej Brytanii i Francji potępili użycie broni chemicznej i poinformowali, że rozważają ataki odwetowe przeciwko reżimowi Assada. Rosja, Chiny i Iran wypowiadały się przeciwko działaniom militarnym. Prezydent Assad zapewniał tymczasem, że będzie kontynuował walkę, jak to określił, z agresją Zachodu[79].

W związku z zarzutami o stosowanie na terenie Syryjskiej Republiki Arabskiej broni chemicznej, w 2014 r. powołano misję rozpoznawczą (ang. *Fact-Finding Mission, FFM*)

[77] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat…*

[78] Tamże.

[79] Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: "Syrian Civil War", *Encyclopedia Britannica,* 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

Organizacji ds. Zakazu Broni Chemicznej (OPCW). Mandat misji określał cel w postaci ustalenia faktów dotyczących zarzutów stosowania w Syrii toksycznych chemikaliów (m.in. chloru) do wrogich celów. W styczniu 2022 r. miała miejsce publikacja dwóch raportów OPCW dotyczących użycia broni chemicznej w Syrii[80]. W pierwszym raporcie stwierdzono, że istnieją uzasadnione podstawy do uznania, iż substancje chemiczne z rodziny środków musztardowych zostały użyte w miejscowości Marea, 1 września 2015 r., w skutek czego poszkodowanych zostało ponad 50 osób. W drugim raporcie wskazano na uzasadnione podstawy do stwierdzenia, że w miejscowości Kafr Zaita w dniu 1 października 2016 r. pojemnik z chlorem został użyty jako broń chemiczna, co wywołało duszności i problemy z oddychaniem u 20 osób.

W kontekście pojawiających się w czasie wojny domowej w Syrii, jak i po zakończeniu jej najbardziej aktywnej fazy, zarzutów o użyciu broni chemicznej, strona rosyjska wielokrotnie zarzucała krajom Zachodu upolitycznienie kwestii użycia broni chemicznej oraz podważała wiarygodność raportów FFM. W podobnym duchu wypowiadały się też Chiny i Iran. Przedstawiciele Syrii podkreślali, że nie akceptują zarzutów kierowanych wobec Damaszku, wskazując na rzekomy brak legitymizacji OPCW do prowadzenia dochodzenia w sprawie użycia broni chemicznej.

Tymczasem, zagraniczne interwencje przekształciły z czasem Syrię w arenę konfliktu mocarstw. Od 2014 r. wojna domowa rozszerzyła się już do postaci międzynarodowego konfliktu, który obejmował kilka państw o rozbieżnych celach. Rosła liczba zagranicznych bojowników, rozpoczęły się otwarte, bezpośrednie interwencje obcych państw. Około 5 milionów Syryjczyków uciekło za granicę.

Stany Zjednoczone, które dotąd – zdaniem części ekspertów – generalnie niechętnie wysyłały broń w obawie przed nieumyślnym uzbrojeniem radykalnych dżihadystów (ryzyko, że zwrócą się przeciwko Zachodowi), ostatecznie rozpoczęły program szkolenia i wyposażenia kilku zweryfikowanych grup rebeliantów przeciwnych Assadowi. Natomiast, rząd syryjski nadal otrzymywał broń i wsparcie od Iranu i libańskiej grupy Hezbollah. Pod

[80] Zob. więcej: *OPCW issues Fact-Finding Mission report on chemical weapons use allegation in Kafr Zeita, Syria, on 1 October 2016*, Organisation for the Prohibition of Chemical Weapons 1.02.2022 https://www.opcw.org/media-centre/news/2022/02/opcw-issues-fact-finding-mission-report-chemical-weapons-use-allegation, [dostęp: 30.03.2022].

koniec 2012 r. Hezbollah zaczął także wysyłać swoich własnych bojowników do Syrii, by walczyć z antyassadowskimi rebeliantami[81].

Wsparcie poszczególnych stron konfliktu płynęło (także potajemnie) ze strony rozmaitych państwowych i niepaństwowych aktorów zewnętrznych. Rebeliantów przeciwnych Assadowi poparły m.in. Arabia Saudyjska i Stany Zjednoczone. Ponadto, USA dowodziły działaniami koalicji do walki z tzw. Państwem Islamskim w Iraku i Syrii (ISIS). Z kolei, Iran, Rosja i Hezbollah należały do największych sojuszników prezydenta Assada. Rosyjska interwencja w Syrii w 2015 r. była przełomem w konflikcie i dzięki niej, reżim był w stanie odzyskać inicjatywę i odbić większość terytorium kraju[82].

Latem 2015 r., po okresie względnego impasu w konflikcie syryjskim (2013-2014)[83], zaczęła rosnąć rola Rosji, co – z czasem – przechyliło w rezultacie szalę zwycięstwa na stronę Assada. Moskwa zdecydowała się na wysyłanie żołnierzy i sprzętu wojskowego do bazy w pobliżu Latakia – jednego z ważniejszych miast portowych w Syrii – położonego nad Morzem Śródziemnym zaledwie ok. 80 km od unijnego terytorium Cypru). Osłonę przeciwlotniczą zapewniały rosyjskie zaawansowane systemy obrony powietrznej S-300 i S-400.

Mimo, że Kreml wspierał Syrię dyplomatycznie na długo przed wybuchem wojny, to powyżej opisane zaangażowanie zachodnich krajów w Syrii posłużyło za pretekst dla Rosji

[81] Nagłe postępy ISIS w regionie, którym towarzyszyła intensywna propaganda, przyspieszyły działania zagranicznych aktorów. 8 sierpnia 2013 r. Stany Zjednoczone rozpoczęły naloty na Irak, aby uniemożliwić ISIL przedostanie się do autonomicznego regionu kurdyjskiego w północnym Iraku i chronić tamtejsze wspólnoty chrześcijan i jazydów. Naloty spowolniły ekspansję ISIL, ale seria filmów pokazujących bojowników ścinających głowy pracownikom pomocy i dziennikarzom z państw zachodnich potęgowała obawy, że ruch ten stanowi globalne zagrożenie. 23 września 2013 r. Stany Zjednoczone i koalicja państw arabskich rozszerzyły kampanię powietrzną na cele ISIL w Syrii.

Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: "Syrian Civil War", *Encyclopedia Britannica*, 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

[82] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat...*

[83] W 2013 r., wraz z procesem osłabiania się nie-islamistycznych frakcji, dominującą pozycję, jako przeciwnik władz w Damaszku zaczęli zajmować bojownicy islamscy. Front Nusrah, oddział Al-Kaidy działający w Syrii, współpracował z wieloma innymi grupami opozycyjnymi i był uważany za jedną z najskuteczniejszych lokalnych organizacji zbrojnych. Wkrótce jej pozycja została jednak przysłonięta przez nową grupę. W kwietniu 2013 r. przywódca Al-Kaidy w Iraku Abu Bakr al-Baghdadi zadeklarował, że połączy swoje siły w Iraku i Syrii pod nazwą Państwo Islamskie w Iraku i Lewancie (ISIL; znane również jako Państwo Islamskie w Iraku i Syrii ISIS). We wschodniej Syrii ISIS zajęło obszar w dolinie Eufratu (Al-Rakka). Stamtąd ugrupowanie rozpoczęło serię udanych operacji zarówno w Syrii, jak i Iraku, rozszerzając kontrolę nad rozległym obszarem terytorium leżącym na granicy iracko-syryjskiej. Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: "Syrian Civil War", *Encyclopedia Britannica*, 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

do oficjalnego włączenia się w konflikt. Dopiero jesienią 2015 r. rosyjskie samoloty, jak wynikało z oficjalnych informacji, zostały skierowane do nalotów na cele ISIS i Al Kaidy. Jednak siły rosyjskie często brały za cel także inne grupy rebeliantów, co pozwalało prezydentowi Assadowi na stopniowe odzyskiwanie kontroli nad terytorium. Po doprowadzeniu do fragmentacji rebeliantów, pod koniec 2019 r. wspierane przez rosyjskie lotnictwo siły wierne Assadowi były w stanie przypuścić ofensywę przeciwko ostatniemu bastionowi zbrojnej opozycji w rejonie Idlib[84].

Siły powietrzne Rosji rozpoczęły pierwsze naloty na cele w Syrii we wrześniu 2015 r. Rosyjscy urzędnicy początkowo twierdzili, że ataki miały charakter antyterrorystyczny i były wymierzone w ISIS, ale dla państw zachodnich szybko stało się jasne, że ich celem są głównie rebelianci walczący przeciwko Assadowi[85].

Natomiast, wczesną jesienią 2016 r., przerywając krótkie zawieszenie broni, Rosja i syryjskie siły rządowe rozpoczęły intensywne bombardowania zajętej przez rebeliantów wschodniej części Aleppo. Użyto do tego pełnego zakresu konwencjonalnych działań militarnych (stosowano m.in. bomby kasetowe i zapalające), co wiązało się z ofiarami wśród ludności cywilnej[86]. Zamierzonymi lub przypadkowymi celami stawały się nie tylko siły rebeliantów, ale też obiekty medyczne, zespoły poszukiwawczo-ratownicze oraz personel pomocniczy. Ataki te, potępione przez organizacje praw człowieka, trwały nieprzerwanie do upadku rebeliantów w Aleppo w grudniu 2016 r. Był to moment przełomowy, od którego reżim Assada – dzięki wsparciu Rosji i Iranu – zaczął odzyskiwać kontrolę nad terytorium kraju[87].

Izrael zaatakował irańskie wojsko w Syrii w 2018 r. Po tym, jak w odpowiedzi Iran ostrzelał Wzgórza Golan, Izrael przypuścił najcięższe ataki w Syrii od początku wojny

[84] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat...*

[85] *Tamże.*

[86] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 199.

[87] Podczas gdy siły rządowe Assada nadal umacniały swoje pozycje, zachodnie rządy coraz częściej interweniowały w konflikt. Po ataku bronią chemiczną w Khān Shaykhūn w kwietniu 2017 r. Stany Zjednoczone ostrzelały bazę lotniczą Shayrat niedaleko Homs przy użyciu 59 pocisków manewrujących Tomahawk. Rok później, po tym, jak rząd syryjski – według źródeł zachodnich – użył broni chemicznej w Doumie, siły amerykańskie, brytyjskie i francuskie przeprowadziły ponad 100 ataków na obiekty wojskowe w pobliżu Damaszku i Homs. Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: "Syrian Civil War", *Encyclopedia Britannica*, 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

domowej. Atakowano dziesiątki irańskich obiektów wojskowych. Izrael twierdził, że zniszczył prawie całą irańską infrastrukturę wojskową w Syrii.

W czerwcu 2018 r., po umocnieniu pozycji na terenach wokół Damaszku i Homs, syryjskie siły rządowe rozpoczęły kampanię mającą na celu odzyskanie terytoriów zajętych przez rebeliantów w południowo-zachodniej prowincji Dara, a następnie rozszerzyły działania na prowincję Al-Qunayṭirah. Gdy sukces operacji rządowej stał się jasny, z pomocą Rosji zawarto umowę, która umożliwiła rebeliantom bezpieczne przejście do prowincji Idlib na północy zajętej przez rebeliantów w zamian za kapitulację na południowym zachodzie kraju.

Idlib był ostatnim pozostałym regionem kraju, który utrzymywali rebelianci, a wszystkie wojujące strony zaczęły szykować się na nieuchronne starcie. Zarówno Turcja, jak i rząd Syrii zaczęły gromadzić wojska wzdłuż granic. Turcja wzmocniła swoją armię w prowincji, podczas gdy syryjskie i rosyjskie samoloty bojowe bombardowały miasta graniczne.

Rosja i Turcja próbowały działań mających na celu deeskalację sytuacji, uzgadniając i wprowadzając strefę buforową między siłami rebeliantów, a siłami rządowymi. Strefa buforowa wymagała wycofania całej ciężkiej broni i myśliwców z obszaru o szerokości około 9 do 12 mil (15 do 20 km). W tamtym czasie nie było jasne, czy wszystkie strony będą przestrzegać porozumienia. Rząd syryjski i główne grupy rebeliantów, takie jak Wolna Armia Syryjska, szybko przyjęły jednak porozumienie o strefie buforowej.

W ramach porozumienia Turcja była odpowiedzialna za powstrzymanie najbardziej radykalnych grup islamskich, takich jak Organizacja Wyzwolenia Lewantu (Tahrir al-Sham, HTS), w regionie. Jednak w styczniu 2019 r. grupa HTS rozpoczęła ofensywę przeciwko innym grupom rebeliantów i wkrótce stała się dominującą siłą w Idlibie.

W kwietniu 2019 r. siły syryjskie przekroczyły strefę buforową i przy pomocy rosyjskich nalotów powietrznych rozpoczęły ofensywę w Idlibie. Zdobyto kontrolę nad dodatkowymi częściami tego terytorium, zanim kontrofensywa rozpoczęta w czerwcu 2019 r. zdołała zepchnąć bitwę z powrotem na obszary kontrolowane przez rząd.

W październiku 2019 r. po niespodziewanym wycofaniu się USA z kurdyjskiego regionu k. granicy z Turcją, władze w Ankarze rozpoczęły ofensywę na kontrolowanym przez Kurdów regionie północno-wschodnim w Syrii. Celem było zdestabilizowanie

kurdyjskich separatystów w Syrii, którzy byli sojusznikami separatystycznej Partii Pracujących Kurdystanu (PKK) w Turcji. Reżimowi Assada udało się powstrzymać postępy Turków i ostatecznie prezydenci Rosji i Turcji uzgodnili zakres tureckiej strefy buforowej i podział stref wpływów w północnej Syrii. Umożliwiło to wizerunkowe wysunięcie się Rosji na czołową pozycję w konflikcie[88]. Siły kurdyjskie szybko zawarły umowę z Assadem, umożliwiając siłom rządowym ponowne wejście do tego regionu po raz pierwszy od 2012 r.[89]

Na początku 2020 r. siły rządowe wierne Assadowi kontynuowały ofensywę, która doprowadziła do odzyskania znacznego terytorium w północno-zachodniej części kraju, w tym kontroli nad całością strategicznej trasy (M5) łączącej dwie największe aglomeracje miejskie kraju – Damaszek i Aleppo.

Przedstawiony zarys głównych działań rozgrywających się podczas wojny w Syrii od 2011 r. dobrze obrazuje rolę zagrożeń hybrydowych dla bezpieczeństwa państwa. Wojna w Syrii miała miejsce w czasie wydarzeń tzw. *Arabskiej Wiosny*, czyli fali (prodemokratycznych) protestów i powstań, które nastąpiły na Bliskim Wschodzie oraz w Afryce Północnej począwszy od 2010 i 2011 r. i były skierowane przeciwko autorytarnym reżimom w regionie[90].

W marcu 2011 r. rząd Syrii stanął w obliczu poważnego wyzwania, gdy w kraju wybuchły prodemokratyczne protesty[91]. Zorganizowane i uzbrojone grupy antyreżimowej opozycji zaczęły ujawniać się od 2011 r., a do 2012 r. konflikt przerodził się w pełnowymiarową wojnę[92]. Wojna, jak ocenił Peter Metzger – były specjalny asystent prezydenta ds. bezpieczeństwa narodowego i zastępca starszego dyrektora ds. Bliskiego Wschodu i Afryki Północnej w Radzie Bezpieczeństwa Narodowego w Białym Domu –

[88] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat…*

[89] Chociaż Turcja w znacznym stopniu unikała bezpośredniej konfrontacji z rządem syryjskim podczas całego konfliktu, ofensywa rządu syryjskiego w Idlibie, wspierana przez rosyjskie naloty, prowadziła często do ofiar i odwetu. Pod koniec lutego 2020 r. konflikt nasilił się na krótko po tym, jak dziesiątki tureckich żołnierzy zginęło w nalocie, a siły tureckie wzięły odwet bezpośrednio na armii syryjskiej. Konfrontacja szybko się jednak zakończyła, po tym jak tydzień później Turcja i Rosja wynegocjowały generalne zawieszenie broni. Chronologiczny przebieg wydarzeń w trakcie wojny domowej w Syrii od 2011 r. opracowano za: "Syrian Civil War", *Encyclopedia Britannica,* 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War. [dostęp: 18 May 2021].

[90] Warto jednak odnotować, że prodemokratyczne powstania nie wybuchły przeciwko wszystkim autorytarnym reżimom w regionie.

[91] O. Giles, *How did the Syrian Civil War Become a Proxy…*

[92] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 200.

obejmowała konkurencyjne interesy nie mniej niż sześciu państw (syryjskiego reżimu Assada, Rosji, Iranu, Turcji, Stanów Zjednoczonych i Izraela)[93].

Kluczową rolę w odwróceniu wyniku konfrontacji Assada z opozycją odegrało wsparcie ze strony państw trzecich. Chodzi głównie o Rosję i Iran, na których coraz bardziej zaczęła polegać Syria. W świetle wyników przeprowadzonych badań należy stwierdzić, że w tym, między innymi, objawiła się hybrydowość syryjskiej wojny domowej. Iran zainwestował znaczące sumy pieniędzy we wspieranie reżimu Assada. Ponadto, siły zbrojne wierne Assadowi były trenowane przez irański Korpus Strażników Rewolucji (Revolutionary Guard Corps)[94].

Po stronie władz w Damaszku zaczęło walczyć coraz więcej sił, takich jak bojownicy paramilitarnych sił Iranu i zagraniczne milicje szyickie (Shia militias) takie jak np. libański Hezbollah (finansowany i szkolony przez Iran). Także Siły Obrony Narodowej miały otrzymywać irańskie fundusze oraz przeszkolenie.

Równocześnie, siły opozycyjne wobec prezydenta Assada także miały swoich zagranicznych darczyńców. USA szkoliły i uzbrajały rebeliantów bez podawania tej informacji do wiadomości publicznej. Od 2014 r. Stany Zjednoczone stały na czele tzw. globalnej koalicji państw mających za cel pokonanie ISIS (the Global Coalition To Defeat ISIS), do której weszły jeszcze 38 państwa z całego świata. Z kolei, Wielka Brytania i Francja, jak wskazują J. Schroefl i J. Välimäki dostarczały wsparcie wojskowe i logistyczne. Znacząca pomoc dla grup rebeliantów pochodziła także od Arabii Saudyjskiej. Ponadto, wzrost siły fundamentalistycznych grup islamskich także dał pretekst niektórym aktorom zagranicznym do interweniowania w Syrii. Prezydent Assad podkreślał przy tym konieczność respektowania norm prawa międzynawowego i niezależności Syrii wskazując, że nie wyraża zgody na wsparcie państw zachodnich w zakresie zwalczania zagrożenia ze strony ISIS[95].

Przeciwdziałanie zagrożeniom hybrydowym i szarej strefie wymaga, w ocenie D. Lovelace'a, bardzo wszechstronnych, elastycznych i skalowalnych sił zbrojnych[96].

---

[93] P. Metzger, *The Imperative to Maintain Focus in Syria, Newsweek 16.04.2021* https://www.newsweek.com/imperative-maintain-focus-syria-opinion-1583346 [dostęp 18.10.2021].
[94] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat...*
[95] Tamże.
[96] Tamże.

Konflikt w Syrii[97] doprowadził do śmierci pół miliona ludzi oraz masowych migracji. Był także źródłem katastrofalnych zniszczeń gospodarczych i pogorszenia wizerunku Syrii na arenie międzynarodowej[98]. Rozgrywające się tam wydarzenia ukazały, że zbrojna opozycja, dzięki wsparciu zewnętrznemu, jest w stanie wyprzeć żołnierzy regularnej armii nawet z terenu stałych baz wojskowych i czasowo przejąć kontrolę nad znacznymi terenami Syrii[99].

Podczas wojny w Syrii, co zauważył były specjalny asystent prezydenta USA ds. bezpieczeństwa narodowego Peter Metzger, zogniskowały się konkurencyjne interesy nie mniej niż sześciu państw: Rosji, Iranu, Turcji, Stanów Zjednoczonych, Izraela i wreszcie – syryjskiego reżimu Assada[100].

Elementem strategii wojny hybrydowej w Syrii było zastosowanie przez stronę rosyjską tzw. środków aktywnych (*active measures*), co – w ocenie analityka i kapitana armii amerykańskiej Gabriela Lloyda[101] – okazało się skutecznym instrumentem polityki zagranicznej i poważnym wyzwaniem dla USA i ich sojuszników[102].

Pełna wiedza o rosyjskich środkach hybrydowych stosowanych w Syrii nie jest możliwa do pozyskania i zaprezentowania z uwagi na niejawny charakter tego typu operacji oraz stosunkowo niewielki odcinek czasu, jaki upłynął od tych wydarzeń. Jednak cenne są badania metod stosowanych przez ZSRR, którego spadkobierczynią jest współczesna Rosja. Stosowanie środków aktywnych przez stronę rosyjską ma długie tradycje. Środki/działania aktywne w terminologii sowieckiej były definiowane, jako specjalne, ofensywne działania o charakterze agenturalno-operacyjnym prowadzone w obszarze polityki, gospodarki,

---

[97] Syria podlega sankcjom USA, a od wybuchu konfliktu wewnętrznego, w marcu 2011 r. na władze Syrii nałożono kolejne ograniczenia. Warto przypomnieć, że od 1979 r. Syria znajduje się na amerykańskiej liście sponsorów terroryzmu, była krytykowana przez USA za okupację Libanu oraz wysiłki na rzecz pozyskania broni masowego rażenia i środków jej przenoszenia. Informacja na temat relacji USA z Syrią na stronach Departamentu Stanu https://www.state.gov/u-s-relations-with-syria/ [dostęp:30.09.2021].

[98] *Uprising in Syria 2011*, *Encyclopedia Britannica*, 2020 https://www.britannica.com/event/Syrian-Civil-War/Uprising-in-Syria-2011 [dostęp: 18 May 2021].

[99] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 194.

[100] P. Metzger, *The Imperative to Maintain Focus in Syria, Newsweek 16.04.2021* https://www.newsweek.com/imperative-maintain-focus-syria-opinion-1583346 [dostęp 18.10.2021].

[101] Trudno nie zgodzić się z tym autorem obserwując wymykającą się spod kontroli, skomplikowaną i potencjalnie geopolitycznie śmiertelnie niebezpieczną sytuację wokół – jak wszystko na to wskazuje – sztucznie wytworzonego, hybrydowego kryzysu imigranckiego na granicy polsko-białoruskiej w 2021 r. Od skuteczności przeciwdziałania tego typu zagrożeniu może zależeć rozwój sytuacji w regionie i zapobieżenie otwarcia kolejnej, po Krymie i Donbasie (a od lutego 2022 r. – także na Ukrainie), rany w tkance bezpieczeństwa regionalnego w Europie Środkowej i Wschodniej. G. Lloyd, *Hybrid Warfare and Active Measures* Small Wars Journal *10.10.2021* https://smallwarsjournal.com/jrnl/art/hybrid-warfare-and-active-measures [dostęp 15.10.2021].

[102] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 206-207.

ideologii, nauki i techniki, a także w celach wojskowych, wywiadowczych i kontrwywiadowczych, ukierunkowane na osłabienie pozycji państw uznanych za wrogie i wzmocnienie międzynarodowej pozycji własnego kraju i państw sojuszniczych. Działania aktywne polegały m.in. na:

– udzielaniu materialnego i moralnego wsparcia danym grupom społeczno-politycznym (np. partiom, organizacjom i mediom) o ile działały one w interesie ZSRR;

– dezorganizowaniu oraz kompromitowaniu ugrupowań, organizacji i partii politycznych, które stanowiły przeszkodę dla realizacji polityki zagranicznej państw bloku komunistycznego;

– dezinformacji, czyli rozpowszechnianiu specjalnie przygotowanych informacji mających wprowadzić w błąd rządy i wrogie służby wywiadowcze[103].

Jak pokazały wyniki badań, podstawowe zadania rosyjskich służb wywiadowczych, polegające na pozyskiwaniu informacji o charakterze politycznym, gospodarczym, naukowo-technicznym i wojskowym oraz wywieraniu wpływu na politykę obcych państw za pomocą tzw. działań aktywnych nie uległy zmianie. W przeszłości, działania aktywne, jak wskazuje Michał Wojnowski, nie ograniczały się tylko do samych służb wywiadowczych, a obejmowały działalność praktycznie każdego elementu sowieckich struktur państwa i były uważane za uzupełnienie dyplomacji ZSRR. Dobrym przykładem tej taktyki były działania służb państw bloku komunistycznego podczas wyborów prezydenckich w USA w czasie Zimnej Wojny[104].

Wojsko rosyjskie uznało doświadczenia w czasie wojny domowej w Syrii za priorytetowe źródło usprawnień służących rozwojowi swoich sił zbrojnych. Szef rosyjskiego sztabu generalnego Walerij Gierasimow w marcu 2018 r. określił Syrię, jako prototyp „wojny nowego typu". Zaapelował on jednocześnie do dogłębnej analizy tego konfliktu w celu przygotowania rosyjskiej armii do przyszłych wojen[105]. W wojnie hybrydowej, której przykładem jest Syria,

[103] Tamże.

[104] M. Wojnowski, *Środki i metody wywierania wpływu na kampanie wyborcze i wybory w Stanach Zjednoczonych przez Związek Sowiecki w okresie Zimnej Wojny. Część I, Raport Warsaw Institute,* 4 czerwca 2021, https://warsawinstitute.org/pl/amerykanska-demokracja-jako-cel-rosyjskich-sluzb-specjalnych-srodki-metody-wywierania-wplywu-na-kampanie-wyborcze-wybory-w-stanach-zjednoczonych-przez-zwiazek-sowiecki-w-okresie-zimnej-wojny/ [dostęp: 26.05.2022].

[105] M. Clark, *The Russian Military's Lessons Learned in Syria*, Military Learning and the Future of War, Institute for the Study of War – ISW January 2021,

wszystkie działania – w tym operacje kinetyczne – są podporządkowane centralnie planowanej i koordynowanej kampanii informacyjnej na poziomie strategicznym.

W czasie wojny w Syrii stosowano szeroki zakres działań metod hybrydowych. Od czasu wybuchu rewolucji antyassadowej, jak wskazuje Sergei Repin analizujący podobieństwa konfliktów w Syrii i na Krymie w 2014 r., Rosja dostarczała reżimowi w Damaszku nie tylko broń, amunicję, ale i wsparcie dowódcze, żołnierzy oraz najemników. Oficerowie rosyjscy byli obecni na każdym szczeblu dowodzenia syryjskiej armii rządowej i, jak sugeruje on dalej, jest prawdopodobne, że to oni *de facto* kierowali działaniami zbrojnymi z użyciem „bezprecedensowo brudnych metod prowadzenia wojny z naruszeniem międzynarodowych norm dotyczących konfliktów zbrojnych[106]*."* Chodziło m.in. o zarzut stosowania nieprecyzyjnych rakiet typu SCUD czy wykorzystywanie schwytanych ludzi, jako tzw. żywych tarcz[107]. Około 85% nalotów przeprowadzanych przez rosyjskie siły powietrzne – jak twierdzi S. Repin – nie miało miejsca na terenach, gdzie aktywne były siły ISIS. Wskazuje to według niego, że celem były siły antyassadowskich, prodemokratycznych rebeliantów, a nie terroryści. Natomiast propaganda rządowa Assada oskarżała zbrojną opozycję o ostrzał cywilów[108].

Rosja, a także inne strony wojny w Syrii tłumaczyły swoje zaangażowanie koniecznością walki z ISIS, których aktywność rozwijała się m.in. dzięki zdestabilizowanej sytuacji w Syrii. Konsolidujące się grupy fundamentalistów islamskich były postrzegane, jako poważne zagrożenie dla bezpieczeństwa państw zachodnich w regionie i na świecie. ISIS (*Islamic State of Iraq and Syria*) miało, oraz nadal ma, na celu zbudowanie kalifatu, tworu państwowego zasadzonego na pojęciu boskiej prawomocności (*divine legitimacy*) w Syrii i Iraku, jednocześnie rzucając wyzwanie organizacji systemów politycznych na świecie w oparciu o model demokratyczny[109].

---

https://www.understandingwar.org/sites/default/files/The%20Russian%20Military%E2%80%99s%20Lessons%20Learned%20in%20Syria_0.pdf [dostęp: 12.04.2022].

[106] S. Repin S., *Syria and Ukraine. Key Features of the Kremlin's 'Hybrid' War*, Inform Napalm – News Syria, 22.10.2015 https://informnapalm.org/en/syria-and-ukraine-key-features-of-the-kremlin-s-hybrid-war/ [dostęp:1.12.2022].

[107] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 201.

[108] S. Repin, *Syria and Ukraine. Key Features of the Kremlin's 'Hybrid' War*, Inform Napalm – News Syria, 22.10.2015 https://informnapalm.org/en/syria-and-ukraine-key-features-of-the-kremlin-s-hybrid-war/ [dostęp: 15.10.2021].

[109] Radyklana organizacja ISIS usiłowała delegitymizować swoich wrogów w postaci głownie umiarkowanych religijnie państw muzułmańskich oraz zachodnich krajów, gdzie przeważa system polityczny w postaci demokracji i rozdziału władzy świeckiej od duchownej (względnie nowy w skali historii świata, bo liczący

Kolejne powstanie w ramach Arabskiej Wiosny przerodziło się w długotrwałą wojnę zastępczą, która przyciągnęła potęgi regionalne i światowe. Syria weszła w 11. rok wewnętrznego konfliktu, oznaczając jeden z najbardziej przeciągających się regionalnych konfliktów w historii. Ponad pół miliona Syryjczyków straciło życie w wyniku konfliktu, zrodzonego z powstania „arabskiej wiosny" w 2011 r.

Iran i Rosja wsparły rząd prezydenta Assada. Teheran, jak informowały USA, wydawał miliardy dolarów rocznie, aby wzmocnić syryjski reżim, zapewniając doradców wojskowych, broń, linie kredytowe i dostawy ropy. Moskwa z kolei dostarczała wparcia przeciwko antagonistom Assada w postaci m.in. działań lotnictwa i systemów obrony przeciwlotniczej. Ponadto, rząd syryjski, jak wskazywał Waszyngton, cieszył się również poparciem – oskarżanego o terroryzm – działającego z Libanu ruchu islamistycznego Hezbollah, którego bojownicy zapewniali ważne wsparcie na polu bitwy od 2013 r.[110]

Aby zrozumieć strategiczne cele Rosji w Syrii, jak oceniają J. Schroefl i J. Välimäki, należy rozpatrywać jej zaangażowanie w ten konflikt w szerszym kontekście. Jeśli chodzi o cele specyficzne to po pierwsze, Rosja – wspierając utrzymanie przy władzy przyjaznego sobie prezydenta Assada – liczyła na utrzymanie możliwości eksportu broni oraz kontrakty handlowe z partnerami syryjskimi. Do drugie, miała także na celu zlikwidowanie zagrożenia ekspansją islamskich grup terrorystycznych w Syrii (reżim Assada – przeciwwagą)[111].

Moskwa zdawała sobie sprawę, że obalenie reżimu Assada byłoby kolejnym – po odsunięciu przy wsparciu NATO od władzy libijskiego przywódcy M. Kadafiego – ciosem w sojuszników Rosji w regionie. Interwencja na rzecz ochrony reżimu w Damaszku była ponadto, jak oceniają J. Schroefl i J. Välimäki obliczona na podważenie roli USA na Bliskim Wschodzie. Strona rosyjska sygnalizowała, że odczytuje wspierane przez USA zmiany reżimów, jako wydarzenia destabilizujące Bliski Wschód i zagrażające pozycji lokalnych sojuszników Rosji. Kreml obawiał się przy tym, że może to doprowadzić w dłuższej perspektywie nawet do obalenia związanej z Putinem ekipy politycznej rządzącej Rosją. Po

sobie zaledwie kilkaset lat). J. Välimäki, *ISIS as A Hybrid Threat Actor: From Iraq And Syria To A New Rise In Africa,* [w:] *Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence,* Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf [dostęp: 12.4.2022].

[110] *Syria: historia konfliktu,* Lucy Rodgers, David Gritten, James Offer i Patrick Asare (red.), BBC, 11 marca 2016 https://www.bbc.com/news/world-middle-east-26116868 [dostep: 20.05.2021].

[111] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat*…

aneksji Krymu w 2014 r. i znajdując się pod presją zachodnich sankcji Rosja wykorzystywała swoje zaangażowanie w Syrii, jako element przetargowy w zakresie innych kwestii[112].

Ponadto, ważne dla Rosji było zachowanie wpływów w rejonie Morza Śródziemnego i Bliskiego Wschodu. Istotna w tym kontekście była ochrona morskiej bazy Tartus – jedynej bliskowschodniej bazy Rosji w tamtym czasie. Interwencja w Syrii dala Rosji pretekst do rozbudowy tej początkowo małej bazy naprawczo-logistycznej obsługującej rosyjskie okręty kursujące przez Morze Śródziemne. W rosyjskiej strategii, jak zauważają J. Schroefl i J. Välimäki, rejon M. Śródziemnego zabezpiecza południową flankę i rzuca wyzwanie dla morskiej supremacji USA i NATO. Siły zbrojne na tym obszarze pozwalają Rosji „przeciwdziałać zachodniej działalności w regionie, ułatwiają dostęp do światowych oceanów oraz umożliwiają projekcję siły w państwach regionu[113].”

Rosja stosowała działania związane z generowaniem zagrożeń hybrydowych w Syrii w szeregu wymiarach[114]. Na długo przed 2011 r. Rosja zacieśniała związki z władzami w Damaszku wychodząc z założenia, że ten bliskowschodni kraj ma kluczowe znaczenie dla zabezpieczenia globalnych interesów Moskwy. Temu służyło utworzenie baz w Tartus oraz prowincji Latakia.

W początkowej fazie wojny domowej w Syrii strona rosyjska nie szczędziła wysiłków dyplomatycznych, aby wspomóc swojego sojusznika. Jednocześnie nie ustawała w dostarczaniu broni dla reżimu Assada. Jak zaznaczył Rusłan Pukhov analityk think tanku CAST, Rosja nie widzi problemu w sprzedaży uzbrojenia do Syrii, jeśli państwa zachodnie (USA, Francja i Wielka Brytania wysyłają dostawy broni przez Turcję dla antyrządowych rebeliantów[115].

Istotne znaczenie miała także aktywność Rosji w zakresie wojny informacyjnej, której jednym z powszechnie stosowanych narządzi była dezinformacja. Kreml przedstawiał wszystkie siły walczące z władzami Syrii, jako czynniki terrorystyczne. Pozwalało to na legitymizację ataków na te siły.

Rosja wspierała także Syrię gospodarczo dostarczając produkty rolne oraz inne towary, które były niedostępne dla Syryjczyków z uwagi na zachodnie sankcje – głownie

[112] Tamże.
[113] Tamże.
[114] Tamże.
[115] Tamże.

uzbrojenie oraz drukowaną walutę (*printed currency*) dla syryjskiego banku centralnego. Towarzyszył temu rozwój relacji kulturalnych polegający m.in. na świętowaniu 75-lecia ustanowienia relacji dyplomatycznych pomiędzy Syrią i Rosją w marcu 2019 r.[116]

Działaniom hybrydowym towarzyszą kampanie propagandowe, które mogą wykorzystywać symboliczne obrazy zwiększające skuteczność danego przekazu. Jeden z przykładów takich zabiegów przytaczają Mervyn Frost i Nicholas Michelsen przypominając, że Rosja została gospodarzem koncertu muzyki klasycznej w starożytnych ruinach w mieście Palmyra w Syrii po odbiciu tego miejsca z rąk Państwa Islamskiego[117]. Było to próbą wykreowania etycznej zasadności rosyjskiej interwencji w tym kraju (Moskwa – protektorem światowego dziedzictwa kulturowego). W połączeniu z faktem podkreślenia przez Rosję, że jej interwencja jest autoryzowana przez suwerenny rząd Syrii (a więc legalna na mocy prawa międzynarodowego), argumentacja ta służyła, jako narzędzie komunikacji strategicznej oraz posiadała znaczący potencjał kształtowania pozytywnego wizerunku strony rosyjskiej[118].

Wygrana Rosji na syryjskim teatrze działań sprawiła zainteresowanie zacieśnianiem relacji z Moskwą przez państwa w regionie. Umożliwiło to zwłaszcza poprawę relacji z Turcją i Iranem[119].

Działania hybrydowe są realizowane poniżej progu wojny, ale – co zauważył R. Shirreff – mają jednak „zapewnić osiągnięcie takich samych celów politycznych i strategicznych jak tradycyjna wojna". W rezultacie, gwarancje bezpieczeństwa w ramach sojuszy są wystawiane na próbę. Możliwość zastosowania przez Rosję metod hybrydowych, co pokazała operacja Kremla na Krymie w 2014 r., przewartościowuje sposób postrzegania

[116] Tamże.

[117] Położony w środkowej Syrii, około 215 km na północny wschód od Damaszku obiekt archeologiczny z czasów rzymskich (jedne z najważniejszych i największych na świecie wykopalisk) wpisany był na listę światowego dziedzictwa UNESCO. W latach 2015-2016 bojownicy z Państwa Islamskiego kilkukrotnie zajmowali miasto. Dokonywali wtedy zniszczeń starożytnych budowli na obszarze archeologicznym detonując tam ładunki wybuchowe (m.in. 16-kolumnowy palmyreński tetrapylon, Świątynię Baalszamina). Zapis wideo z tych aktów barbarzyństwa wzbudzał oburzenie opinii publicznej na świecie. Rosja ukazując, że walczy z tego typu opozycją antyassadowską usiłowała przedstawić się jako cywilizowana siła chroniąca światowe dziedzictwo kulturowe.

[118] M. Frost, N. Michelsen, *International Ethics and Information Warfare*, [w:] *Hybrid Conflicts and Information Warfare. New Labels, Old Politics,* O. Fridman V. Kabernik J. C. Pearce (red.), Boulder-Colorado, USA 2019, s. 100-101.

[119] Tamże.

mechanizmów wynikających z członkostwa w NATO. Gwarancje bezpieczeństwa niestety mogą być w ten sposób w praktyce w pewnym stopniu zniwelowane[120].

Jak wykazały wyniki badań, państwa zachodnie muszą liczyć się z wykorzystaniem sił specjalnych i prorosyjskiej wewnętrznej opozycji (np. mniejszości rosyjskiej na Łotwie) do budowania przez hybrydowego agresora specyficznej strefy frontowej na całym obszarze kraju postrzeganego przez Rosję jako wrogi. Nie można wykluczyć scenariusza upozorowania ataku ludności kraju A na tamtejszą mniejszość rosyjską, co może zostać wykorzystane jako pretekst interwencji zbrojnej (konieczność obrony praw mniejszości rosyjskiej do interwencji[121].

Dodatkowym czynnikiem jest tu możliwość zastosowania przez stronę rosyjską groźby użycia broni nuklearnej, jako elementu mającego odstraszyć kraje chcące przyjść z pomocą zaatakowanemu sojusznikowi. Na realność takiej wizji wpływają obserwacje wojny z Ukrainą w 2022 r., kiedy prezydent W. Putin zagroził atakiem atomowym przestrzegając kraje trzecie – w tym NATO – przed zbyt jaskrawym angażowaniem się w konflikt zbrojny.

Pewne elementy działań hybrydowych były też obserwowane lokalnie w czasie omawianego konfliktu. W 2012 r., mniej więcej rok po rozpoczęciu wojny domowej w Syrii, jeden z dowódców ISIS Samir Abd Muhammad al-Khlifawi znany jako Haji Bakr, ulokował swoja bazę w miasteczku Tell Rifaat, na północ od Aleppo. Ten były oficer wywiadu Saddama Husajna w stopniu pułkownika rozpoczął stamtąd przejmowanie kontroli nad kolejnymi rejonami w owładniętej wojną domową Syrii. Jego taktyka walki hybrydowej zakładała m.in. zbieranie kompromitujących informacji o najważniejszych rodzinach, osobach oraz grupach zbrojnych w poszczególnych miasteczkach i wsiach. Tego typu działalność, która przewidywała także możliwość szantażu wymienionych wcześniej osób i grup, była ukierunkowana na rozszerzanie wpływów ISIS w Syrii i w Iraku[122].

Od czasu zmaterializowania się zagrożenia fundamentalizmem islamskim w Syrii i w regionie, rząd USA ściśle współpracował z Globalną Koalicją na rzecz Pokonania ISIS[123].

---

[120] R. Shirreff, *Wojna z Rosją*, 2017, s. 90-91.

[121] Tamże.

[122] P. Roell, *Migration – A New Form of "Hybrid Warfare"?* Institut für Strategie - Politik-Sicherheits - und Wirtschaftsberatung ISPSW, May 2016, https://www.ispsw.com/wp-content/uploads/2016/05/422_Roell_RINSA.pdf [dostep: 30.09.2021].

[123] Informacja na temat relacji USA z Syrią…

Mimo, że Ambasada USA w Syrii zawiesiła działalność w lutym 2012 r., a interesy Waszyngtonu w Syrii powierzono Czechom (za pośrednictwem ambasady tego kraju w Damaszku), Stany Zjednoczone były największym pojedynczym darczyńcą pomocy humanitarnej w Syrii od początku kryzysu. Wybranym przez siebie organizacjom, jak wynika z danych Departamentu Stanu, przekazały, ponad 12 mld dolarów. Wsparcie Stanów Zjednoczonych docierało każdego miesiąca do 4,8 mln osób w 14 prowincjach Syrii, a także do ponad 5 mln z 5,65 mln syryjskich uchodźców w regionie. W latach 2012-2018 w północno-zachodniej Syrii USA zapewniały pomoc dla syryjskiej opozycji. Pomoc ta obejmowała m.in. wspieranie lokalnych aktywistów i organizacji społeczeństwa obywatelskiego w przeciwdziałaniu wpływom grup ekstremistycznych, takich jak Al-Kaida. Waszyngton udzielał też wsparcia w zakresie wyposażenia *Wolnej Armii Syryjskiej* i *Wolnej Policji Syryjskiej* w nieśmiercionośną broń[124].

Istotnym wymiarem konfrontacji hybrydowej w Syrii były kwestie kontroli granicznej i współpracy w regionie. Turcja, członek NATO, była na przykład oskarżana przez niektórych ekspertów zachodnich o brak woli współdziałania na rzecz pokonania ISIS. Pojawiały się nawet oskarżenia o pośrednie wsparcie Ankary dla fundamentalistów islamskich w wyniku braku odpowiedniego nadzoru na granicy syryjsko-tureckiej[125]. Konfliktogenna była także kwestia współpracy władz Turcji z popieranymi przez USA Kurdami, którzy – wbrew interesom Turcji – usiłowali stworzyć zalążki swojego państwa w ogarniętej destabilizacją północnej Syrii[126].

W działaniach hybrydowych, co warto zaznaczyć, zastosowanie znajdują powszechnie m.in. prywatne firmy wojskowe, które można określić, jako siły najemników. Syria nie była tu wyjątkiem. Dla przykładu, tacy kontraktorzy, działający w interesie strony rosyjskiej, jak zauważa F. Bryjka, ochraniali m.in. infrastrukturę energetyczną w Syrii. Byli oni także wykorzystywani do projekcji wpływów niektórych krajów w Afryce i ochrony przyjaznych względem określonych rządów reżimów w Ameryce Łacińskiej[127]. Obecność

[124] Tamże.

[125] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 202.

[126] M. Yeşiltaş, *Neighboring A Civil War Turkey's Border Security With Syri*a, SETA 10.2015 20151028162016_analysis_17.pdf (setav.org) [dostęp: 18.10.2021].

[127] F. Bryjka, *Rosyjscy „kontraktorzy" w służbie Kremla*, Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2019/08/ROSYJSCY-%E2%80%9EKONTRAKTORZY%E2%80%9D-W-S%C5%81U%C5%BBBIE-KREMLA-Warsaw-Institute.pdf [dostęp: 9.06.2021] , s. 2, 14.

rosyjskich prywatnych firm wojskowych w Syrii wyszła na jaw pod koniec października 2015 r., zaledwie miesiąc po rozpoczęciu otwartej rosyjskiej interwencji wojskowej w tym kraju. W wyniku ataku moździerzowego rebeliantów w Latakii zginęło wówczas od trzech do dziewięciu najemników[128].

Na początku konfliktu w Syrii, Stany Zjednoczone, które wspierały zbrojną opozycję w postaci bojowników określanych jako Wolna Armia Syryjska (FSA), jak przyznał Mark Ward – dyrektor US Team of Assistance to Syria (2012-2016), zakładały upadek reżimu Assada w ciągu kilku miesięcy (najdalej do świat Bożego Narodzenia 2012). USA rozważały jakie wsparcie zapewnić FSA. Służby wywiadu cywilnego (CIA) działały już wówczas z terenu Turcji monitorując przepływy broni i środków finansowych do Syrii z państw arabskich[129]. Waszyngton rozpoczął intensywne wsparcie szkoleń rebeliantów, ale USA – w przeciwieństwie np. do Arabii Saudyjskiej – nie były początkowo zainteresowane dostawami broni dla zbrojnej opozycji. Prezydent Obama zapowiedział jednak, że może zmienić zdanie w przypadku „użycia broni chemicznej przez reżim Assada", co później władzom w Syrii faktycznie zarzucono.

Znaczenie wojny w Syrii w kontekście przeciwdziałania zagrożeniom hybrydowym można rozpatrywać na wielu płaszczyznach. Zaangażowanie Rosji w wojnie domowej w Syrii było przykładem aktywności związanej z zagrożeniami hybrydowymi. Rosyjskie siły zbrojne, jak dowodzi Mason Clark z amerykańskiego think tanku Institute for the Study of War, od czasu wojny w Syrii wykorzystują tamte doświadczenia, aby rozwinąć elastyczne i skuteczne wojska ekspedycyjne. Dla Rosji operacja w Syrii była prototypem przyszłej wojny (rozmieszczenie wojsk miało na celu wsparcie działań hybrydowych). Rosyjski Sztab Generalny traktował Syrię, jako poligon doskonalący metody prowadzenia „ograniczonych działań" za granicą. Znalazło to odzwierciedlenie w rosyjskich ćwiczeniach wojskowych od 2015 r.[130] Wiele rozwiązań, jak ocenia M. Clark, prawdopodobnie zostało włączonych już do doktryny Rosji, w tym do tajnego rosyjskiego Narodowego Planu Obrony na lata 2021-

[128] Tamże.

[129] E. Londoño, G. Miller, *U.S. starts delivering weapons to Syrian rebels*, Toronto Star, 11.09.2013 https://www.thestar.com/news/world/2013/09/11/us_starts_delivering_weapons_to_syrian_rebels.html, [dostęp: 15.03.2022].

[130] M. Clark, *The Russian Military's Lessons Learned in Syria*, Military Learning and the Future of War, Institute for the Study of War – ISW January 2021, https://www.understandingwar.org/sites/default/files/The%20Russian%20Military%E2%80%99s%20Lessons%20Learned%20in%20Syria_0.pdf [dostęp: 12.04.2022].

2025. Rozwój zdolności Rosji osiągany dzięki operacjom takim jak w Syrii (a także na Ukrainie w 2022 r.) zlikwiduje ważne luki w zakresie zdolności i technologii w zestawieniu z krajami zachodnimi (NATO). Chodzi tu m.in. o usprawnienia systemu dowodzenia i łączności. Będzie to wymagać jednak czasu, co pokazują problemy Rosji w czasie inwazji Ukrainy w 2022 r. Warto nadmienić, że Rosja, według doniesień medialnych, miała wycofać część swoich wojsk obecnych w Syrii celem rozmieszczenia ich na terytorium Ukrainy[131].

W Syrii miało też miejsce zastosowanie przez Rosję niekonwencjonalnych metod i użycia sprzętu wojskowego w tym zbudowanego na podwoziu samobieżnej haubicy 2S1 Goździk rosyjskiego pojazdu UR-77 Meteorit. Wieżę z haubicą zastąpiono na nim wyrzutnią ładunku wydłużonego – wystrzeliwanej za pomocą rakiety – wybuchowej liny. Po wystrzeleniu lina rozwija się w powietrzu (na długość ok. 90 metrów) i opada na ziemię. Siła wybuchu powoduje detonację pobliskich min lądowych, dzięki czemu w polu minowym tworzy się bezpieczne przejście o szerokości około 6 metrów. Podczas walk w Syrii, Rosjanie używali ładunków wydłużonych do ataków na przeciwnika w zabudowie miejskiej. Pojedyncza rakieta tego typu powodowała zniszczenie kilkudziesięciu metrów zabudowy wzdłuż atakowanej ulicy. UR-77 Meteorit został użyty do atakowania zabudowań także na Ukrainie w 2022 r.[132]

Oficerowie rosyjscy prawdopodobnie wykażą się w przyszłości większą kreatywnością i elastycznością działania niż ich poprzednicy. W tym kontekście nieuzasadnione są stereotypowe oceny rosyjskiej kultury dowodzenia, która miałaby rzekomo zatrzymać się w czasach sowieckich. Przykład skutecznej interwencji Rosji w Syrii

[131] Bazy wojskowe opuszczone przez Rosjan miały zostać przekazane w użytkowanie organizacjom IRGC i Libańskiego Hezbollahu. Ten krok może wpłynąć na zwiększenie potencjału irańskiej obecności na terenie Syrii. Opisany aspekt jest podkreślany w szczególności przez prasę izraelską, wskazującą na względnie pozytywną (z punktu widzenia Tel Awiwu) rolę rosyjskiej obecności w Syrii – skutkującą dotychczas ograniczaniem wpływów Teheranu w zakresie zajmowanych pozycji strategicznych oraz stopnia infiltracji syryjskiej armii i służb bezpieczeństwa (pomimo pewnego stopnia kooperacji Moskwy z siłami irańskimi). Na uwagę zasługuje fakt, iż dotychczasowe współoddziaływanie obu państw na terytorium Syrii funkcjonowało w oparciu o tzw. mechanizm dekonfliktacji, pozwalający uniknąć starć pomiędzy siłami rosyjskimi i izraelskimi.

[132] Ł. Michalik, *Rosyjski UR-77 Meteorit zniszczony jednym granatem*, MSN 20.10.2022 https://www.msn.com/pl-pl/wiadomosci/polska/rosyjski-ur-77-meteorit-zniszczony-jednym-granatem-dos%C5%82ownie-wyparowa%C5%82/ar-AA13aD21?ocid=msedgntp&cvid=087693ba5a244e4492dbb0783d8860c5 [dostep: 20.10.2022].

czy – mimo znacznych strat własnych – unieszkodliwienie większości głównych ofensywnych si zbrojnych Ukrainy w 2022 r. potwierdzają słuszność tej tezy[133].

Rosyjskie wojsko wykorzystuje naukę płynącą z Syrii, aby zlikwidować kilka luk w zdolnościach (capability gaps) z państwami zachodnimi, które powinny przygotować się na dalszą modernizację rosyjskich sił zbrojnych w następujących obszarach:

1. udoskonalenie sieciowych systemów dowodzenia (networked command systems) przez wojsko rosyjskie, jeśli zostanie osiągnięte, osłabi jedną z kluczowych przewag technologicznych NATO. Starania Rosji w tym zakresie będą wymagały dużych nakładów, ale rosyjska armia robi postępy, co pokazały w 2020 r. testy systemów, które były w fazie teoretycznej jeszcze w 2018 r.);
2. podniesienie jakości kultury dowodzenia. Rosyjskie wojsko wspiera technologiczną modernizację systemów dowodzenia kampanią mającą na celu przebudowę rosyjskiej kultury dowodzenia. Objawia się to w stymulowaniu inicjatywy i kreatywności w oparciu o zmianę pokoleniową rosyjskiego korpusu oficerskiego;
3. rosyjskie wojsko zmierza w kierunku zwiększenia zdolności ataków precyzyjnych (precision-strike capabilities), ale osiągnięcie tych celów wymaga dalszych kosztownych inwestycji technologicznych. Stany Zjednoczone i ich sojusznicy powinni dodatkowo utrzymywać presję sankcyjną w celu pozbawienia Kremla zasobów niezbędnych do realizacji tego rodzaju zaawansowanych programów zbrojeniowych;
4. rosyjska armia prawdopodobnie rozwija zdolności do przeciwdziałania użyciu bezzałogowych statków powietrznych (UAV). Może to wymagać konieczności przygotowania się do zwiększenia obsługi dronów w coraz bardziej niebezpiecznym otoczeniu. Przeciwstawienie się zagrożeniu z tego kierunku musi uwzględniać rosnące wyrafinowanie strony rosyjskiej w zakresie bezzałogowych statków powietrznych i broni antydronowej;

[133] M. Clark, *The Russian Military's Lessons Learned in Syria*…

5. nie można także nie doceniać potencjału Kremla wysyłania wojsk ekspedycyjnych wzorowanych na interwencji w Syrii. Sukces tej operacji zapewnił władzom w Moskwie dodatkowy instrument realizacji polityki zagranicznej[134].

Zaprezentowane wcześniej rekomendacje, co warto odnotować, były zaproponowane na rok przed inwazją Rosji na Ukrainę w 2022 r.

W świetle wyników przeprowadzonych badań należy stwierdzić, że przeciwdziałanie wzrostowi zagrożeń ze strony Rosji, także w sferze hybrydowej, wymaga podjęcia szeregu działań, do których M. Clark zalicza m.in.:

1. utrzymanie przez kraje zachodnie elastycznych sił zbrojnych zdolnych przeciwstawić się wojsku rosyjskiemu. Rosyjskie zagrożenie militarne nie ogranicza się do Europy. Stany Zjednoczone wraz z sojusznikami nie muszą rozmieszczać własnych sił zbrojnych wszędzie tam, gdzie Kreml może prowadzić operacje ekspedycyjne. Natomiast powinno się rozwinąć partnerskie siły wojskowe, aby przeciwdziałać rosyjskiemu zagrożeniu lokalnie;
2. USA wraz z sojusznikami muszą nadać priorytet przeciwdziałania rosyjskim wysiłkom zmierzającym do usprawnienia systemu dowodzenia. Zachodni sojusznicy muszą rozwinąć zrozumienie tego, co rosyjska armia postrzega jako kluczowe zadanie bojowe swoich oficerów – zwiększenie szybkości podejmowania decyzji i ograniczenie zdolności dowodzenia i kontroli przeciwnika (*command and control capabilities*);
3. uwzględnienie w sojuszniczym planowaniu faktu, że nowa kadra doświadczonych bojowo rosyjskich oficerów może zmienić skuteczność wojskową Rosji (większość kadry dowódczej Rosji posiada doświadczenie z Syrii);
4. Stany Zjednoczone i ich sojusznicy powinny podjąć kroki w celu wzmocnienia współpracy z NATO i rozszerzenia zasięgu tej organizacji na inne państwa w celu ograniczenia zdolności Kremla do rozwijania sieci powiązań wojskowych. Należy także opracować metody rozbijania wrogich zachodowi koalicji;

[134] Tamże.

5. rosyjska armia wykorzystuje naukę płynącą z Syrii, aby zlikwidować luki w zdolnościach ze Stanami Zjednoczonymi i NATO. Stany Zjednoczone i ich sojusznicy powinni przygotować się na dalszą modernizację wojsk Rosji;

6. Stany Zjednoczone i ich sojusznicy mogą dodatkowo kontynuować presję sankcyjną w celu pozbawienia Kremla zasobów niezbędnych do realizacji kosztownych programów nakierowanych na zbrojenia, w tym rozwój zdolności niekonwencjonalnych[135].

Gen. Gierasimow częściowo przypisał sukces rosyjskich operacji w Syrii wykorzystaniu Centrum Kontroli Obrony Narodowej (National Defense Control Center, NDCC). NDCC to wojskowe centrum dowódcze uruchomione w kwietniu 2014 r. pod auspicjami rosyjskiego resortu obrony. Utworzono je w celu wypełnienia luki w rosyjskich zdolnościach planowania strategicznego i foresightu po upadku Związku Radzieckiego. Powołanie NDCC, w ocenie strony rosyjskiej, zmieniło podejście do zarządzania organizacją wojskową państwa, zwłaszcza w zakresie dostępności informacji i komunikacji. Rosyjscy oficerowie uważają NDCC za zautomatyzowany system kontroli, który pełni rolę centralnego węzła umożliwiając dowódcom działanie w zunifikowanej przestrzeni danych i łączności. Wyjątkowość operacji rosyjskiej w Syrii polegała na dobrze zorganizowanym zarządzaniu różnorodną grupą sił, zarówno bezpośrednio na teatrze działań, jak i z centrum NDCC. Centrum, zdaniem części rosyjskich polityków, stało się nie tylko instrumentem zarządzania działaniami sił zbrojnych, ale i koordynatorem wszystkich federalnych departamentów odpowiedzialnych za bezpieczeństwo państwa[136].

Strona rosyjska podkreśla znaczenie kreatywności w nowoczesnej wojnie, także z użyciem metod niekonwencjonalnych. W sensie taktycznym w wojnach hybrydowych, takich jak Syria dowódcy są zobowiązani do korzystania z niezależności działania, co nie jest wymagane w przypadku wojny konwencjonalnej. Podczas interwencji w Syrii, rosyjskie siły zbrojne stworzyły ekspedycyjną kwaterę główną, której funkcjonowanie zakładało dużą elastyczność. To właśnie z tego jednego miejsca, z centrum w bazie Humajmim (ang. Hmeimim) przy porcie lotniczym Latakia nad M. Śródziemnym koordynowano aktywa

[135] Tamże.
[136] Tamże.

w całej Syrii. Terytorium kraju podzielono na strefy odpowiedzialności, z których każda była zarządzana przez grupy operacyjne w Humajmim złożone z 15-20 oficerów (w szczytowym momencie). Skład dowództwa był często zmieniany w zależności od potrzeb sytuacji bojowej i rosyjskich zasobów na teatrze działań[137].

Rosyjskie koncepcje wojny hybrydowej definiują sukces w przewadze powietrznej. Kreml początkowo koncentrował się na zapobieżeniu rzekomemu powtórzeniu się sytuacji z Libii, w której naloty NATO umożliwiły upadek reżimu. Generałowie Aleksander Dwornikow[138], Walery Gierasimow, a także wybitny teoretyk wojny hybrydowej Aleksander Bartosz wszyscy postrzegają Syrię, jako trwającą zachodnią kampanię hybrydową. Rosyjscy analitycy oceniają, że ich środki powietrzne i obrona przeciwlotnicza zapobiegły zmianie przychylnego Moskwie reżimu Assada w Syrii. Siły NATO mogły zniszczyć obronę przeciwlotniczą i instalacje Rosji w Syrii, ale byłoby to okupione prawdopodobnie dużym kosztami politycznymi i być może także wojskowymi[139].

Syryjskie doświadczenia wojskowe, także z uwzględnieniem doskonalenia metod hybrydowych, zostały wykorzystane podczas zaangażowania strony rosyjskiej w Libii oraz konflikcie o Górski Karabach w 2021 r., a także – w inwazji na Ukrainie w 2022 r.

USA oraz ich stronnicy kontynuują wysiłki na rzecz demokratyzacji Syrii[140]. W 2022 r. miały miejsce kolejne spotkania Globalnej Koalicji do walki z Daesz, której grupy robocze są kierowane wspólnie przez Stany Zjednoczone, Niemcy i Zjednoczone Emiraty Arabskie, a w spotkaniach biorą udział przedstawiciele kilkudziesięciu państw, agend ONZ (UNITAD, UNDP), a także organizacji pomocowych. Starania są prowadzone na rzecz stabilizacji obszarów wyzwolonych z rąk Daesz w Syrii i Iraku oraz reintegracji osób wewnętrznie przesiedlonych. Planowane są kolejne konferencje darczyńców celem wsparcia i wzmocnienia partnerów lokalnych w wybranych obszarach (m.in. wsparcie budowy społeczeństwa obywatelskiego i niezależnych mediów oraz zapewnienie pełnego udziału

[137] Tamże.

[138] Na początku kwietnia 2022 r, gen. Gierasimow wyznaczył wsławionego operacjami w Syrii gen. Aleksandra Dwornikowa na naczelnego dowódcę rosyjskiej operacji na Ukrainie.

[139] M. Clark, *The Russian Military's Lessons Learned in Syria*…

[140] Sytuacja w Syrii w 2022 r. nadal jest trudna w aspekcie humanitarnym. Około 12 milionów Syryjczyków znajduje się na granicy głodu, a blisko dwie trzecie syryjskich domów otrzymuje dostawy prądu tylko przez dwie godziny dziennie. W ciągu 11 lat śmierć poniosło około 350 tysięcy osób, a blisko 14 milionów zostało przesiedlonych. Kryzys gospodarczy w dalszym ciągu się pogłębia. Obserwowane są rekordowe wzrosty cen żywności i energii.

w życiu politycznym i społecznym wszystkim grup społecznym, a także pomoc dla centrów rehabilitacji młodzieży, zapewnienie podstawowych usług publicznych, lokalne programy rozwojowe.

Działania wojenne od początku historii ludzkości cechowała różnorodność i dostosowywanie – zależnie od sytuacji – zarówno instrumentów walki defensywnej, jak i ofensywnej (tarcza i miecz). Współcześnie pojęcie wojny hybrydowej robi międzynarodową „karierę", ale warto zauważyć nie jest to nowa tematyka w wojskowości. Choć zagrożenia hybrydowe nie są nowym zjawiskiem, ewoluują one i okresowo zwiększają intensywność występowania wraz z poszczególnymi konfliktami międzynarodowymi i regionalnymi. Podobnie do wojny hybrydowej ma się sprawa jeśli chodzi o tzw. wojny zastępcze oraz – w mniejszym stopniu – zagrożenia asymetryczne[141].

Wojna hybrydowa w Syrii w 2011 r. ukazała znaczenie współczesnych zagrożeń tego typu w kontekście bezpieczeństwa narodowego. Te hybrydowe obszary ryzyka (*szara wojna)*, mogą generować poważne konsekwencje w postaci np. utraty kontroli nad znacznym obszarem kraju oraz grozić destabilizacją kraju lub nawet upadkiem rządu (w tym przypadku reżimu Assada) w wyniku siłowych działań opozycji wspieranej z zagranicy[142].

W oparciu o studium przypadku, przedstawiono zagrożenia hybrydowe na przykładzie wojny w Syrii w 2011 r., mając na uwadze wypracowanie metod przeciwdziałania w tym zakresie. Przypadek ten jest o tyle wartościowy badawczo, że w konflikcie Syria była zarówno stroną wykorzystującą metody hybrydowe, jak i broniącą się przed ich zastosowaniem. Analiza konfliktu hybrydowego w Syrii, abstrahując od kwestii tyranii reżimu prezydenta Assada, ukazuje, że nawet państwo stosunkowo silne militarnie i wewnętrznie (autorytaryzm z rozwiniętymi formacjami odpowiedzialnymi za bezpieczeństwo – m.in. policja, służby specjalne)[143] może być podatne na zagrożenia hybrydowe (z elementami tzw. wojny zastępczej – *proxy war*). Ponadto, wsparcie sojuszników może być kluczowe dla skutecznej obrony przez zagrożeniami hybrydowymi. Po trzecie, brak efektywnej kontroli granic stanowi jeden z kluczowych czynników

[141] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 202-203.
[142] Tamże, s. 203.
[143] M. Ward, *Refugees Forced to Return to Syria Face Imprisonment, Death at the Hands of Assad,* Atlas Institute for International Affairs March 14, 2019 https://www.internationalaffairshouse.org/refugees-forced-to-return-to-syria-face-imprisonment-death-at-the-hands-of-assad/ [dostęp: 18.10.2021].

zwiększających zagrożenie działaniami hybrydowymi, zwłaszcza zagranicznie inspirowanymi[144].

Przykład Syrii ukazał wyzwania w zakresie skutecznego zwalczania współczesnych zagrożeń hybrydowych. Władze w Damaszku, mimo autorytarnych rządów i względnie wysokiej odporności na zagrożenia wewnętrzne i zewnętrzne, nie były w stanie spacyfikować powszechnego niezadowolenia społecznego, które było dodatkowo zasilane z zewnątrz. Na protesty krajowej opozycji politycznej nałożyły się ambicje państwowych i pozapaństwowych aktorów zewnętrznych. Ich zaangażowanie niewątpliwie uniemożliwiło władzom w Damaszku szybką pacyfikację protestów oraz – w efekcie – umiędzynarodowiło i przedłużyło trwanie tego konfliktu. Konsekwencją była m.in. dewastacja gospodarcza kraju oraz – jeszcze większe niż poprzednio – pogorszenie jego wizerunku w relacjach międzynarodowych z wieloma krajami świata[145].

Wojna domowa w Syrii pokazała ponadto, że w obliczu poważnych zagrożeń hybrydowych (gwałtowne protesty społeczeństwa wspierane z zagranicy) realne, a nie deklaratywne wsparcie sojuszników może mieć kluczowe znaczenie dla skutecznej obrony. Wreszcie, brak efektywnej kontroli granic w Syrii umożliwił rozmaitym stronom zewnętrznym penetrowanie terytorium syryjskiego i stanowił jeden z ważnych czynników zwiększających zagrożenie działaniami hybrydowymi. Konflikt w regionie dotknął także kraje sąsiednie (Turcja, dla przykładu, w celu przeciwdziałania napływowi uchodźców, planowała m.in. wybudowanie muru na granicy z Syrią)[146].

Reżimowi Assada największe wsparcie zapewniły Iran i Rosja. Teheran, w ocenie państw zachodnich, wydawał miliardy dolarów rocznie, aby wzmocnić Syrię (zapewniano m.in. doradców wojskowych, broń, linie kredytowe i dostawy ropy). Moskwa z kolei dostarczyła wparcia przeciwko przeciwnikom Assada w postaci m.in. działań lotnictwa i systemów obrony przeciwlotniczej. Ponadto, rząd syryjski, jak wskazywał Waszyngton, cieszył się również poparciem – oskarżanego o terroryzm – działającego z Libanu ruchu

[144] T. Kijewski, *Znaczenie zagrożeń hybrydowych…,* s. 194.
[145] Tamże, s. 203.
[146] Tamże, s. 203.

islamistycznego Hezbollah, którego bojownicy zapewniali ważne wsparcie na polu bitwy od 2013 r.[147]

Rosja, jak wynika z przeanalizowanych informacji, odegrała kluczową rolę w zakresie ochrony reżimu Assada, którego niektórzy komentatorzy (m.in. S. Repin) określali – na równi z byłym prezydentem Ukrainy Janukowyczem – mianem marionetki prezydenta Putina. Równie ważną rolę miało także wsparcie dla władz w Damaszku ze strony irańskiej.

Rosja, jak zauważyli Josef Schroefl i Jarno Välimäki, była jednym z głównych aktorów zagranicznych w tym konflikcie, a także wpływała politycznie na Syrię na długo przed 2011 r. Strona rosyjska wykorzystała Syrię, jako narzędzie do zdobywania, zachowania i potwierdzenia statusu supermocarstwa oraz swojej obecności w regionie Morza Śródziemnego. Efekty wojny domowej w Syrii (utrzymanie u władzy Assada) pokazują, że Rosja odniosła sukces w działaniach hybrydowych odgrywając w Syrii kluczową rolę. Sprawiło to, jak oceniają J. Schroefl i J. Välimäki, że działania Kremla nie mogą być już ignorowane przez państwa zachodnie lub główne kraje w regionie[148].

W zakresie wsparcia żołnierzami, głównym sprzymierzeńcem Assada była jednak nie Rosja, a Iran. Władze w Teheranie, według niektórych szacunków mogły dostarczyć do Syrii nawet 80 tys. zależnych od siebie zagranicznych bojowników. Nastąpiło to w kluczowym momencie konfliktu, kiedy reżim w Damaszku przegrywał[149].

Bez wsparcia z zewnątrz, jak wykazały wyniki badań, prodemokratyczna rebelia w Syrii zostałaby prawdopodobnie stłumiona przez siły rządowe. Jednak zasilanie protestów z zagranicy i włączenie się do tego konfliktu aktorów zewnętrznych – nie wdając się w kwestie moralnej słuszności opozycji względem autorytarnego reżimu prezydenta Assada – doprowadziło do wieloletniej, wyniszczającej kraj wojny „domowej", choć zdecydowanie lepszym określeniem jest tu konflikt hybrydowy. Wsparcie prezydenta Assada ze strony

[147] *Syria: historia konfliktu*, L. Rodgers, D. Gritten, J. Offer i P. Asare (red.), BBC, 11 marca 2016 https://www.bbc.com/news/world-middle-east-26116868 [dostep: 20.05.2021].

[148] J. Schroefl, J. Välimäki, *The Syrian Civil War: Russia As A Hybrid Threat*…

[149] R. S. Ford, *The Syrian Civil War. A New Stage, But Is It The Final One?* April 2019 Policy Paper 2019-8 https://www.mei.edu/sites/default/files/2019-04/Ford_The_Syrian_Civil_War.pdf [dostęp: 18.10.2021].

Rosji oraz Iranu, jak wskazuje na to przebieg wypadków, zapobiegło siłowej zmianie władzy w Damaszku, jak wynika z oceny przebiegu wydarzeń od początku konfliktu w 2011 r.[150]

Pewną rolę w konflikcie, w zakresie biernego wsparcia reżimu Assada, odegrały także Chiny, które pośrednio popierały na forum międzynarodowym stanowiska przychylne władzom w Damaszku.

Działania hybrydowe różnych państw i organizacji w czasie wojny w Syrii, co trzeba podkreślić, należy analizować w kontekście szerszego wymiaru polityk poszczególnych państw związanych z dążeniami do zapewnienia bezpieczeństwa sobie oraz w swoim najbliższym otoczeniu w regionie Bliskiego Wschodu. Także geopolityczny wymiar tej rozgrywki wydaje się mieć istotne znaczenie, co wymagać może w przyszłości oddzielnych badań, które będą zapewne utrudnione z uwagi na niejawny charakter tematyki bezpieczeństwa i zakulisowych działań hybrydowych poszczególnych państw w tym wymiarze[151].

Ponadto, w czasie działań hybrydowych, wiele stron konfliktu uciekało się do używania metod charakterystycznych dla terroryzmu (ataki bombowe z ukrycia, porwania, działalność grup bojówkarzy, dezinformacja i propaganda).

Pomiędzy interwencją Rosji w syryjskiej wojnie domowej oraz innymi konfliktami z udziałem strony rosyjskiej (m.in. wojną na Ukrainie w 2022 r.), jak oceniają niektórzy badacze, istnieje szereg podobieństw. Rosyjskie działania wojskowe, w tym hybrydowe – jak zauważa stypendysta *University of Oxford* i badacz pochodzenia syryjskiego Marwan Safar Jalani – reżim Baszara al-Assada przy wsparciu Moskwy prowadził od 2015 r. masowe kampanie dezinformacyjne. Przedstawiano w nich działania władz państwowych przeciwko demonstrantom i zbrojnym bojówkom syryjskim, jako „wojnę z terroryzmem" oraz zaprzeczano użyciu broni chemicznej przeciwko ludności cywilnej. Rząd syryjski był także odpowiedzialny, zadaniem M. S. Jalaniego, za wysiedlenia milionów Syryjczyków; zbrodnie wojenne, bombardowania obiektów cywilnych (szpitale i szkoły w prowincjach Idlib i Aleppo) oraz śmierć co najmniej pół miliona ludzi, którzy zginęli w wyniku masowych ostrzałów, masakr, tortur i przemocy seksualnej[152].

---

[150] T. Kijewski, *Znaczenie zagrożeń hybrydowych…*, s. 204.

[151] Tamże, s. 204.

[152] M. Safar Jalani, *The Russian invasion of Ukraine happened because the world gave Vladimir Putin a free pass in Syria*, MENA Source, Atlantic Council, March 9, 2022,

Z wojny domowej w Syrii można wyciągnąć wnioski służące wzmocnieniu skutecznej obrony w tym wymiarze w Sojuszu Północnoatlantyckim. Wrażliwość krajów NATO na działania hybrydowe poniżej progu wojny (*below-threshold hybrid threats)* należy ocenić, jako wysoką, zwłaszcza na tzw. wschodniej flance. Próbę wytypowania możliwych zagrożeń hybrydowych w tym obszarze podjął w 2021 r. m.in. waszyngtoński ośrodek CEPA przy współpracy ze stałym przedstawicielstwem USA przy NATO. Próbę tę należy ocenić, jako cenny wkład w podniesienie zdolności obronnych NATO w zakresie reagowania na zagrożenia hybrydowe[153]. Skuteczne przeciwdziałanie zagrożeniom hybrydowym ze strony Rosji, Chin i aktorów pozapaństwowych, jak wynika z tego badania powinno obejmować działania w następujących ośmiu dziedzinach:

a) podniesienie świadomości zagrożeń hybrydowych – zrozumienie istoty tego ryzyka zwłaszcza w zakresie dezinformacji i cyber-bezpieczeństwa. Mimo, że istnieje wiedza o występowaniu tych zagrożeń w ujęciu wyizolowanym, ich kombinacyjne zastosowanie może być wyjątkowo groźne i wymaga dogłębnych badań w kontekście wzajemnych powiązań (*interconnectivity*);

b) zwiększenie szybkości reagowania NATO na zagrożenia hybrydowe – co może być dokonane w oparciu o inwestycje w agencje wywiadowcze, monitoring otwartych źródeł informacji oraz budowanie skomputeryzowanych zespołów przeciwdziałających dezinformacji;

c) przećwiczenie działań aktywnych poniżej progu wojny – zaznajomienie sił sojuszniczych odpowiedzialnych za bezpieczeństwo z sytuacjami nie mieszczącymi się w artykule 5 Traktatu Waszyngtońskiego i wypracowanie praktyki zbiorowych działań wyprzedzających (*hunt forward*). NATO może także pomagać krajom członkowskim w budowaniu odporności na zagrożenia hybrydowe (*resilience standards, capability targets*);

d) zwiększanie zaufania między instytucjami rządowymi i społeczeństwem (*trust-building exercises*) – umożliwienie władzom skutecznych

https://www.atlanticcouncil.org/blogs/menasource/the-russian-invasion-of-ukraine-happened-because-the-world-gave-vladimir-putin-a-free-pass-in-syria/ [dostęp: 8.04.2022].

[153] T. Kijewski, *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa państwa na przykładzie wojny w Syrii w 2011 r.* [w:] *Terroryzm/Antyterroryzm #20 lat po 9/11*, W. Zubrzycki, J. Cymerski (red.nauk) 2022, s. 205-207.

działań dotyczących hybrydowych obszarów ryzyka. Brak obecnie pełnego zaufania w tym wymiarze w krajach natowskich, co wynika z badania CEPA, działa na korzyć wrogów Sojuszu wykorzystujących narzędzia walki hybrydowej;

e) intensyfikacja współpracy publiczno-prywatnej w zakresie zwalczania zagrożeń hybrydowych. Sektor prywatny zarządza większością infrastruktury krytycznej będącej często celem ataków hybrydowych (rurociągi paliwowe, sieci elektroenergetyczne, ale i np. systemy informatyczne online). Strona rządowa powinna przy tym zapewnić ramy prawne oraz zachęty finansowe dla sektora prywatnego;

f) innowacje w zakresie minimalizacji zagrożeń hybrydowych w sferze technologicznej (*tech-enabled hybrid threats*) – próba wytypowania miejsca kolejnego ataku. W badaniu CEPA wykazano, że w przyszłości obszarami takimi mogą być m.in. systemy autonomiczne (np. pojazdy, transport), sztuczna inteligencja, biotechnologia. NATO powinno w tym wymiarze odgrywać większą rolę w zakresie ustanawiania standardów bezpieczeństwa;

g) trening praktyczny w zakresie realnych zagrożeń hybrydowych (*train and exercise to failure*) – realistyczne ćwiczenia, które mają przetestować scenariusze kryzysowe i mechanizmy odpowiedzi. Zapewnienie eksperymentalnych, innowacyjnych metod realizacji ćwiczeń z udziałem sektora prywatnego, społeczeństwa obywatelskiego i instytucji transatlantyckich. Obecnie ćwiczenia tego typu są generalnie zbyt powierzchowne, „bezpieczne" i nieadekwatne do potrzeby wypracowania prawdziwej odporności;

h) zwiększenie roli NATO, jako koordynatora ogólnospołecznej odpowiedzi w zakresie zagrożeń hybrydowych (*whole-of-society coordination*). Z uwagi na specyfikę ataków hybrydowych działania pojedynczych rządów mogą być niewystarczające w sytuacji kryzysu. Władze narodowe, powinny mieć nadal wyłączne kompetencje i suwerenność w zakresie decyzji o zastosowaniu danej strategii odpowiedzi na zagrożenia hybrydowe, ale struktury sojusznicze powinny ułatwiać krajom członkowskim dostęp i obieg informacji, zorganizowanie

dodatkowych sił wsparcia, zapewnienie zasobów i wybór optymalnych instrumentów działania[154].

O złożoności problemu konfliktu na terenie Syrii świadczą także wydarzenia, które rozgrywały się później. W 2021 r. pojawiły się doniesienia o rzekomych atakach bronią mikrofalową na przebywających tam żołnierzy amerykańskich. Chodzi o ataki wykorzystujące promieniowanie elektromagnetyczne, w przypadku których przypisanie komukolwiek odpowiedzialności za jej użycie jest bardzo trudne. Żołnierz piechoty morskiej w Syrii miał rzekomo zostać zraniony tzw. bronią energii skierowanej. Mimo, że wskazywano na możliwość zaangażowania strony rosyjskiej w tym przypadku, Pentagon ostatecznie zdementował te informacje utrzymując, że przyczyną dolegliwości żołnierzy nie była tego typu broń, a dolegliwości pokarmowe. Warto odnotować, iż podobnego typu domniemane ataki na obywateli amerykańskich obserwowano wcześniej m.in. na Kubie.

Kwestia syryjska stanowi istotny obiekt zainteresowania USA mimo upływu ponad 10 lat od czasu rozpoczęcia wojny domowej w tym kraju. Temat ten był poruszany w czasie zorganizowanego 05.04.2022 r. przez *The Woodrow Wilson Center* webinarium. Mimo, że priorytetami USA – jak zauważono – jest obecnie strategiczna rywalizacja z Chinami i powstrzymywanie agresywnej polityki Rosji, Waszyngton zmuszony jest do ochrony swoich interesów na Bliskim Wschodzie, w tym poprzez działania względem Syrii. USA odrzucają możliwość normalizacji relacji z władzami w Damaszku podkreślając konieczność pociągnięcia do odpowiedzialności winnych zbrodni wojennych w Syrii. Waszyngton krytykuje także państwa regionu dążące do odprężenia w relacjach z Syrią (np. wizyta prezydenta Assada w Zjednoczonych Emiratach Arabskich 18.03.2022 r.). Za priorytetowe działania w Syrii, co podkreśliła Zastępca Asystenta Sekretarza Obrony ds. Bliskiego Wschodu Dana Stroul, USA uznają: rozszerzenie dostępu pomocy humanitarnej; utrzymanie obecności wojskowej i lokalnych partnerstw w celu utrzymania presji na ISIS; wspieranie i promowanie praw człowieka i odpowiedzialności reżimu al-Asada za popełnione zbrodnie (także poprzez sankcje) oraz powstrzymanie eskalacji przemocy poprzez utrzymanie lokalnych rozejmów. Ponadto, wyzwaniem stojącym przed USA jest też zwalczanie

[154] *Hybrid Warfare of the Future*, CEPA July 28, 2021 https://cepa.org/hybrid-warfare-of-the-future-sharpening-natos-competitive-edge/ [dostęp: 18.10.2021].

produkcji i dystrybucji narkotyku Captagon (opartego o fenetylinę, środek stymulujący), w którą zaangażowany jest reżim al-Assada oraz bojówki wspierane przez Iran. Zyski pochodzące z nielegalnej dystrybucji tego narkotyku wspierają działania władz w Damaszku i służą także wzmacnianiu interesów Iranu[155].

Stale prowadzona jest przez rząd w Damaszku narracja dot. zewnętrznych przyczyn wojny domowej. W tym duchu, reżim Baszara al-Asada jest uważany za jedyny gwarant bezpieczeństwa kraju. W maju 2022 r. miała miejsce zorganizowana przez UE tzw. konferencja Bruksela VI, w trakcie której zadeklarowano przeznaczenie na rzecz pomocy mieszkańcom Syrii 4,3 mld USD w roku 2022 oraz 2,4 mld USD w kolejnych latach. W spotkaniu ministerialnym wzięło udział 81 delegacji – w tym reprezentujących 55 państw, 7 organizacji regionalnych i międzynarodowych instytucji finansowych, 13 agencji ONZ i 3 organizacji humanitarnych. Warto odnotować tok rozumowania władz syryjskich w tym zakresie. Wydarzenie zostało negatywnie ocenione przez władze w Damaszku. Skrytykowano również fakt, iż do udziału w konferencji nie zaproszono Rosji i innych krajów wyrażających – jak to określono – umiarkowane stanowisko. Wskazano również, iż zanim Syria została zaatakowana przez terroryzm wspierany przez Zachód, była samowystarczalnym krajem o wysokim poziomie wzrostu ekonomicznego, nie potrzebującym jakiegokolwiek wsparcia zewnętrznego ani pożyczek zagranicznych[156].

2.3.2. Działania hybrydowe w czasie konfliktu na Ukrainie (Krym, Donbas – od 2014 r.)

Po zakończeniu Zimnej Wojny i dekadzie względnego odprężenia w relacjach między krajami zachodnimi i Rosją, nastąpił stopniowy wzrost napięć. Brak poważnych sporów, do czego przyczyniała się polityczno-gospodarcza słabość Rosji, trwał do czasu

[155] *The future of Syria. ISIS, the Iranians and the displaced millions, w*ebinarium *The Woodrow Wilson Center,* Apr. 5, 2022, https://www.wilsoncenter.org/event/future-syria-isis-iranians-and-displaced-millions [dostęp: 14.04.2022].

[156] Syryjskie MSZ podkreśliło, że zarówno ta, jak i inne podobne konferencje nie są ukierunkowane na realną pomoc, natomiast są organizowane w formule niezgodnej z zasadami ONZ dot. międzynarodowych akcji humanitarnych, tj. bez udziału głównego zainteresowanego państwa – ponadto przy udziale państw okupujących syryjskie terytorium i rabujących jego zasoby w kooperacji z separatystycznymi ugrupowaniami zbrojnymi, a także przy udziale państw nakładających na mieszkańców Syrii niesprawiedliwe blokady ekonomiczne, które skutkują brakiem możliwości zaspokojenia podstawowych potrzeb Syryjczyków, takich jak zaopatrzenie w żywność, paliwo i leki. W wydanym oświadczeniu strona syryjska podkreśliła ponadto, że ww. państwa w sposób jawny upolityczniają kwestię zapewnienia pomocy humanitarnej.

wojny w Kosowie w 1999 r. Z czasem stało się jasne, że aspiracje szeregu nowopowstałych lub odradzających się suwerennych państw w Europie Środkowej i Wschodniej nie są przez Kreml uważane za korzystne. Aspiracje te starły się więc z geopolitycznymi realiami walki o kontrolę i strefy wpływów w Europie i szerzej – w skali globalnej.

Wiele z państw, znajdujących się nadal w geograficznej oraz często społeczno-kulturowej bliskości (mniejszość rosyjska, związki historyczne) i zasięgu odziaływania władz w Moskwie, podjęło próbę pełnego uniezależnienia się od nich poprzez dołączenie do struktur euroatlantyckich (UE, NATO). Te dążenia spowodowały sekwencję wydarzeń o charakterze konfliktu zbrojnego w poszczególnych krajach (Gruzja, Ukraina). Wydarzenia te skutecznie wstrzymały albo przynajmniej opóźniły perspektywy szybkiej akcesji niektórych z tych państw do struktur świata zachodniego[157].

Część badaczy określa rok 2014, jako przełomowy w historii globalnego bezpieczeństwa z uwagi na dwa wydarzenia w tamtym czasie: rosyjskie zaangażowanie na Ukrainie i powstanie Państwa Islamskiego w Syrii i Iraku. Do ich urzeczywistnienia przyczyniło się wykorzystanie nowych możliwości komunikacyjnych w przestrzeni informacyjnej oraz zastosowanie metod hybrydowych – charakterystycznych także dla działań terrorystycznych[158].

Wydarzenia na Krymie w 2014 r. można określić mianem niewypowiedzianej wojny hybrydowej. Był to kolejny – po wojnie w Gruzji w 2008 r. – przykład ukazujący współczesne zagrożenia dla integralności terytorialnej państw w Europie. Był też pierwszym tak dobitnym przykładem naruszenia suwerenności terytorialnej i zmiany granic dużego kraju w Europie Środkowej i Wschodniej po zakończeniu Zimnej Wojny[159].

Jak wykazały wyniki badań, w świetle prawa międzynarodowego, Federacja Rosyjska została uznana przez kraje zachodnie za okupanta na Krymie. Jednak aneksja

[157] W innych krajach, gdzie również wpływy środowisk prorosyjskich są znaczne (np. Mołdawia), a także w części państw zachodnich, trwa polityczna rywalizacja zwolenników większego zbliżenia z Zachodem, środowisk orientujących się (świadomie lub poprzez poddanie się wpływom dezinformacji) na kooperację z Rosją (Serbia) oraz tych, którzy są zainteresowani prowadzeniem bardziej zrównoważonej polityki zagranicznej (balansując między USA, UE, Rosją i Chinami – jak do pewnego stopnia czynią Węgry). Zob. T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa na przykładzie konfliktu na Krymie w 2014 r. z uwzględnieniem aspektu przeciwdziałania terroryzmowi,* XX-lecie walki z terroryzmem – bilans i konsekwencje, Tom I., Współczesne zagrożenia – Strategie reagowania – Edukacja, B. Wiśniewska-Paź, D. Szlachter (red.), Wyd. A. Marszałek w Toruniu, 2022, s. 32.

[158] O. Fridman, V. Kabernik, J. C. Pearce (red.), *Hybrid Conflicts And Information Warfare. New Labels, Old Politics, Londyn 2019.*

[159] T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa…, s. 32.*

Krymu stała się też powodem do dumy Rosji, gdzie popularność Putina wzrosła. Brak uznania jakichkolwiek roszczeń prawnych Kremla do półwyspu oraz płynące z różnych krajów na świecie głosy sprzeciwu wobec rosyjskiej polityki tylko podsyciły nacjonalizm Rosjan[160].

Działania obserwowane na Krymie w 2014 r. oraz późniejsza wojna we wschodniej Ukrainie (m.in. w Donbasie) są przykładami operacji hybrydowych, które potwierdziły zagrożenia generowane przez skoordynowane operacje Federacji Rosyjskiej i prorosyjskich lokalnych separatystów[161]. W stosunkowo krótkim czasie i – w przypadku aneksji Krymu – bez otwartej agresji (brak użycia broni wobec ludności cywilnej) przeciwnik był w stanie całkowicie zablokować działanie ukraińskiej administracji państwowej na Krymie i ostatecznie przejąć kontrolę nad spornymi obszarami. *Modus operandi*, który powtarzał się w wielu przypadkach zajmowania miast, mniejszych skupisk ludności czy ważnych obiektów w odniesieniu do Krymu był następujący. Na danym terenie ukraińskim pojawiały się dobrze wyszkolone i uzbrojone osoby (w większości żołnierze sił specjalnych lub najemnicy), które wraz z prorosyjsko nastawionymi mieszkańcami przejmowały budynki administracji publicznej oraz siedziby sił porządkowych (m.in. komendy policji). Do publicznej wiadomości separatyści podawali komunikaty stwierdzające, że lokalne społeczności rzekomo nie zgadzają się z polityką nowych władz w Kijowie[162].

Specjalne operacje hybrydowe – o ile dobrze je przygotowano – są początkowo niemożliwe do jasnego zidentyfikowania inaczej niż pośrednio – po specyficznych cechach czy wrogich naszemu interesowi działaniach. Akcje hybrydowe są formą groźnego, bo skrytego ataku danego państwa lub aktora pozapaństwowego (np. organizacji zbrojnej,

[160] Fiasko Ukrainy w zakresie skutecznej obrony swojego terytorium było ewidentne. Rząd ukraiński twierdził, że Krym jest terytorium Ukrainy, ale zainicjował ewakuację kilkudziesięciu tysięcy żołnierzy z półwyspu. Kwatera główna ukraińskiej marynarki wojennej została w pośpiechu przeniesiona z Sewastopola do Odessy. Większość ukraińskiej floty została przejęta przez wojska rosyjskie (niektóre okręty zostały później zwrócone Ukrainie, ale inne, w tym jedyny okręt podwodny ukraińskiej marynarki, zostały włączone do rosyjskiej Floty Czarnomorskiej).

History of Crimea. Early history to the Crimean War, https://www.britannica.com/place/Crimea/History [dostep: 27.09.2021].

[161] Wspieranych przez powiązane, w ocenie części zachodnich analityków, z Kremlem najemników określanych, jako tzw. psy wojny, którzy działają indywidualnie lub przez prywatne firmy wojskowe (ang. PMC).

[162] Zmienionych wcześniej – co trzeba odnotować – także w trybie poza-wyborczym – przez antyrządowe, prodemokratyczne strajki „Euromajdanu". T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa*…, s. 33.

w tym o charakterze paramilitarnym lub terrorystycznym), który jest realizowany poniżej progu wojny. Odbywa się to generalnie nie za pomocną tradycyjnych narzędzi wojny konwencjonalnej. Jako przykład wymienić tu można m.in. nigdy oficjalnie niewypowiedzianą „wojnę" na Półwyspie Krymskim w 2014 r., która objawiła się przez pojawienie się spornym terenie nieoznakowanych sił zbrojnych (tzw. „zielonych ludzików"), które były jednostkami wojskowymi Rosji. Kreml rozpowszechniał dezinformację, że są to lokalne siły złożone z prorosyjsko nastawionej ludności[163].

Warto zauważyć, że rosyjsko-ukraiński konflikt o Krym nie zaczął się od tzw. Euromaidanu, ale miał swoją długą historię. Jego geneza sięga czasów wyodrębnienia Ukrainy z ZSRR po zakończeniu Zimnej Wojny. Społeczeństwo zamieszkujące Ukrainę po upadku tzw. Żelaznej Kurtyny przez szereg lat pozostawało rozdarte między dwoma kierunkami: wschodnim oraz reform w stylu zachodnim. Stan ten odzwierciedlał się w częstych zmianach ekip rządzących o różnych zapatrywaniach względem przyszłości politycznej kraju, co miało miejsce od czasów tzw. pomarańczowej rewolucji w 2004 r., która po raz pierwszy w tak wyraźny sposób utorowała drogę prozachodnim siłom w Kijowie. Był to szok dla elit politycznych na Kremlu, który przyrównywano nawet do wydarzenia o takim znaczeniu, jak ataki terrorystyczne na USA 9/11[164]. Moskwa pod żadnym pozorem nie przyjmowała argumentacji, iż Ukraińcy świadomie i niezależnie coraz bardziej zwracają się ku Zachodowi.

Próba otrucia lidera ukraińskiej opozycji Wiktora Juszczenki przed Pomarańczową Rewolucją w 2004 r., o co Zachód oskarżył stronę rosyjską, była jednym z pierwszych widocznych i znaczących działań hybrydowych ze strony Federacji Rosyjskiej. Był to sygnał, że w celu obrony swojej strefy wpływów Kreml jest w stanie posunąć się do bezwzględnego wyeliminowania każdego prozachodniego lidera politycznego. Jednak przypadki działań uderzających w wiarygodność Ukrainy pojawiały się wcześniej. Chodziło m.in. o próby fałszerstw wyborczych czy posądzenie Ukrainy o sprzedaż systemów

[163] Tamże.

[164] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea and Eastern Ukraine,* Jun 25 2018, https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/ [dostęp: 27.08.2021].

antyrakietowych Kolczuga objętemu sankcjami Irakowi Saddama Husajna, co miało to skompromitować Kijów przed szczytem NATO w Pradze[165].

Jednak od czasu pomarańczowej rewolucji, siły prozachodnie nie zawsze były dominujące na ukraińskiej scenie politycznej. Gdy w 2010 r. prezydentem Ukrainy został lider prorosyjskiej Partii Regionów Wiktor Janukowycz, naturalne było, że będzie on dążył do ponownego zacieśnienia relacji z Moskwą. I tak też się stało. Głowa państwa przedłużyła wkrótce dzierżawę na rzecz Rosji strategicznie ważnego dla bezpieczeństwa w regionie portu w Sewastopolu na Półwyspie Krymskim. Flota Czarnomorska miała stacjonować na Krymie do 2017 r., ale 21 kwietnia 2010 r. prezydent Janukowycz podpisał ze stroną rosyjską umowę przedłużającą podstawy prawne do stacjonowania okrętów Federacji Rosyjskiej na terytorium Ukrainy. Okres dzierżawy był tak długi (ponad 30 lat), że w praktyce oznaczało to nadanie stałego charakteru tej morskiej bazie Rosji w Sewastopolu do 2042 r. W zamian Ukraina miała otrzymywać rosyjski gaz o 30 proc. taniej od ceny bazowej. Dzięki nowej umowie Rosja mogła przedłużyć stacjonowanie 25 tys. żołnierzy i funkcjonowanie swoich instalacji wojskowych na Krymie.

Był to wielki sukces Moskwy, która w ten sposób cementowała swoje wpływy na terytorium ukraińskim i pośrednio wprowadzała poważną przeszkodę dla prozachodnich aspiracji Kijowa (UE, NATO)[166]. Przedłużeniu dzierżawy dla Floty Czarnomorskiej sprzeciwiał się poprzedni, prezydent Wiktor Juszczenko, który był zorientowany prozachodnio i zabiegał o wstąpienie Ukrainy do NATO[167]. Zalegitymizowanie *de facto* na stałe obecności wojskowej Federacji Rosyjskiej na Ukrainie powodowało też komplikację w kontekście ewentualnych planów zacieśniania przez Kijów integracji ze strukturami unijnymi /lub natowskimi w przyszłości. Rosyjska ludność Krymu (pozostająca tam większością) była zwolennikami prorosyjskiej polityki W. Janukowycza[168]. W odróżnieniu od Donbasu, gdzie później przeniosły się działania zbrojne, Krym od zawsze miał dla Rosji historyczne, symboliczne znaczenie, jako ważny element tożsamości narodowej[169]. Tym

[165] Z. Parafianowicz, *O co chodzi w wojnie na Ukrainie?,* wywiad dla telewizji internetowej https://www.youtube.com/watch?v=uqo_9_fG3dA [dostęp: 14.11.2022].

[166] Tamże.

[167] W. Juszczenko jest od 1998 r. mężem Kateryny Juszczenko (z domu Czumaczenko) – Ukrainki urodzonej w Chicago, która pracowała m.in. w Departamencie Stanu USA, w Białym Domu. W grudniu 1999 r. W. Juszczenko objął stanowisko premiera, a w 2005 r. – prezydenta Ukrainy.

[168] T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa*…, s. 33.

[169] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea*...

można tłumaczyć fakt, że decyzja ta nie została powstrzymana w wyniku protestów na półwyspie.

Napięcia polityczne w kraju wzrosły na tle sporu i różnicy zdań w społeczeństwie odnośnie tego czy Ukraina ma integrować się ze strukturami zachodnimi, w tym z UE czy też nie. W. Janukowycz ostatecznie odrzucił możliwość zawarcia porozumienia o bliższej współpracy z UE, co zainicjowało miesiące gwałtownych, proeuropejskich protestów społecznych. Ostatecznie, doprowadziły one do obalenia Janukowycza, który w lutym 2014 r. uciekł z Kijowa[170]. Prezydent Janukowycz postanowił wyjechać z kraju po krwawych zajściach w Kijowie, kiedy zginęło około 70 protestujących (tzw. Czarny czwartek). 22 lutego 2014 r. miało miejsce formalne usunięcie W. Janukowycza z urzędu przez Radę Najwyższą. Zmiana ta, podobnie jak wiele innych rewolucji, była krwawa i przyniosła wiele ofiar, także wśród cywilów. W czasie tych wydarzeń, które zachodni komentatorzy zaczęli nazywać tzw. Euromaidanem, zginęło 130 antyrządowych demonstrantów oraz 18 funkcjonariuszy policji.

Wraz z tymi wydarzeniami wzmagało się niezadowolenie tych mieszkańców Ukrainy, którzy byli przeważnie przychylni polityce Kremla i opowiadali się za zachowaniem legalności prorosyjskich wówczas władz Ukrainy. Tworzyli oni ruch społeczny określany jako tzw. „Antymajdan" i rozpoczęli coraz bardziej aktywne protesty, które zgromadziły nawet po kilkanaście tysięcy osób w dużych ośrodkach miejskich – m.in. w Charkowie i Doniecku (1 marca 2014 r.). Naturalnie ruch ten był wspierany przez Federację Rosyjską i stanowił podstawę do rozwinięcia działań hybrydowych przez stronę rosyjską. Oprócz Doniecka i Charkowa, prorosyjskie wiece odbyły się m.in. w Ługańsku, Dniepropietrowsku, Odessie i Mikołajewie. W Doniecku usiłowano wedrzeć się na teren siedziby Służby Bezpieczeństwa Ukrainy, a w Charkowie protestowano m.in. pod polskim konsulatem wyrażając sprzeciw wobec polityki Zachodu.

W kontekście eskalacji przemocy po zajęciu Krymu na kolejnych obszarach państwa ukraińskiego, władze w Kijowie określiły bojowników lojalnych prorosyjskim republikom ludowym (DNR, LNR), jako terrorystów. Ukraina postanowiła tym samym, że działania wojenne będą prowadzone, jako operacja antyterrorystyczna zgodnie z zapisami ustawy

[170] W opracowaniu wykorzystano informacje o chronologicznym przebiegu wypadków na Krymie na podstawie: *Crisis in Crimea, Britannica* https://www.britannica.com/place/Crimea/History#ref341465 [dostęp: 28.09.2021].

antyterrorystycznej z 2003 r. Zabieg ten miał na celu unikniecie prawnych konsekwencji pozostawania Ukrainy w stanie wojny, z uwagi na niebezpieczeństwo niemożności otrzymania pożyczek. Dodatkowo, władze w Kijowie nie zdecydowały się na określenie konfliktu, jako wojny ponieważ wymagało by to mobilizacji zasobów wojskowych i masowego poboru, na co nie było poparcia społeczeństwa[171].

Euromaidan w 2014 r. stanowił klęskę planów prezydenta Putina, który był wcześniej o krok od włączenia Ukrainy do Unii Euroazjatyckiej[172]. W czasie protestów przeciwko prorosyjskiemu prezydentowi Janukowyczowi, Rosja dostarczała doradztwa oraz sprzętu służącego tłumieniu zamieszek. Co więcej, jak wskazują *Taras Kuzio i Paul D'Anieri,* rosyjskie służby specjalne organizowały w późniejszym czasie transport tzw. „politycznych turystów" – prorosyjskich protestujących, którzy mieli za zadanie działanie na rzecz Rosji w największych ośrodkach miejskich Ukrainy, w tym Doniecku, Ługańsku i Charkowie. Udało im się w znacznej mierze zradykalizować rosyjskojęzyczne tłumy nastawione przychylnie względem Kremla i przejąć obiekty użyteczności publicznej, centra władzy lokalnej. Dezintegracja służb porządkowych w Doniecku i Ługańsku spowodowała, że w ręce separatystów dostała się znaczna ilość broni, co dodatkowo pogorszyło szanse Ukrainy na przeciwdziałanie destabilizacji w regionie[173]. Przybycie w kwietniu 2014 r. na te tereny rosyjskich służb specjalnych w postaci Specnazu wzmocniło pozycję separatystów poprzez zdyscyplinowanie ich, zapewnienie im przeszkolenia oraz sprzętu wojskowego[174].

Odsunięcie od władzy prezydenta Janukowycza, którego wiele decyzji było korzystnych dla Rosji, spowodowało szybki ciąg zdarzeń. W ich centrum znalazł się mający ogromne znaczenie dla Rosji Półwysep Krymski, gdzie stacjonuje Flota Czarnomorska. Aneksja Krymu przez Rosję miała miejsce 18 marca 2014 r. Doprowadziła to niej błyskawiczna operacja strony rosyjskiej z intensywnym wykorzystaniem elementów hybrydowych.

W nocy z 26 na 27 lutego 2014 r. żołnierze bez dystynkcji zajęli budynki parlamentu i rządu Republiki Autonomicznej Krymu w Symferopolu. Grupy uzbrojonych mężczyzn,

[171] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea*...

[172] Unia Eurazjatycka (EAU) to planowany projekt zacieśnienia współpracy gospodarczej i politycznej Rosji, Kazachstanu, Białorusi, Kirgistanu i Tadżykistanu, który był wzorowany na strukturach Unii Europejskiej (głównym organem EAU miałaby być Komisja Eurazjatycka, a siedzibą – Moskwa.

[173] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea*...

[174] Tamże.

których mundury nie miały znaków identyfikacyjnych, otoczyły lotniska w Symferopolu i Sewastopolu. Zamaskowani sprawcy zajęli budynek krymskiego parlamentu i umieścili na nim rosyjską flagę. Połączenia telefoniczne i transmisji danych między Krymem a Ukrainą zostały zerwane. W ciągu kilku dni, zamaskowane zbrojne grupy (później zidentyfikowane przez zachodnich ekspertów, jako siły rosyjskie) zajęły kluczowe lokacje na Krymie. Rosyjskie wojska rozpoczęły operację przejmowania baz na całym półwyspie, w tym dowództwa ukraińskiej marynarki w Sewastopolu (Ukraina zainicjowała ewakuację 25 000 żołnierzy i ich rodzin z Krymu).

Prorosyjscy deputowani na Krymie zwołali sesję parlamentu (niejawną), zdymisjonowali lokalny rząd i wybrali na premiera lidera Rosyjskiej Partii Jedności – Siergieja Aksjonowa, który oświadczył, że to on, a nie rząd w Kijowie, posiada kontrolę nad siłami policyjnymi i wojskowymi na Krymie[175].

Prezydent W. Putin uzyskał w marcu 2014 r. zgodę parlamentu na wysłanie wojsk na Krym. Krok ten tłumaczono koniecznością ochrony tamtejszej etnicznej ludności rosyjskiej i zasobów wojskowych na Krymie. Siły rosyjskie i lokalne prorosyjskie grupy paramilitarne były w stanie w zaledwie kilka dni przejąć *de facto* kontrolę nad kluczowymi obszarami półwyspu.

1 marca 2014 r. samozwańczy premier Republiki Autonomicznej Krymu, Siergiej Aksionow, zwrócił się z prośbą do prezydenta Federacji Rosyjskiej o zapewnienie spokoju i bezpieczeństwa mieszkańcom Krymu. Tego samego dnia Rada Federacji Rosyjskiej przyjęła wniosek prezydenta w sprawie wydania zgody na użycie rosyjskich sił zbrojnych na terytorium Ukrainy. Rada Federacji Rosyjskiej wyraziła 1 marca 2014 r. zgodę, by na wniosek prezydenta Putina użyć sił zbrojnych na terytorium Ukrainy aż do momentu – jak zakomunikowano – ustabilizowania się tam sytuacji. Konieczność interwencji na Ukrainie, rosyjscy deputowani tłumaczyli bratnimi więzami ich kraju z Krymem. Obarczyli jednocześnie winą za napiętą sytuację na Ukrainie państwa zachodnie na czele z USA. Przypomnieli punkty zapalne na świecie, gdzie, w ich ocenie, także zawinili zachodni decydenci (m.in. Syrię i Egipt). We wniosku stwierdzono, co następuje: „W związku z nadzwyczajną sytuacją, powstałą na Ukrainie, zagrożeniem życia obywateli Federacji

[175] *The crisis in Crimea and eastern Ukraine, Encyclopaedia Britannica* https://www.britannica.com/place/Ukraine/The-Poroshenko-administration [dostęp: 13.06.2022].

Rosyjskiej, naszych rodaków, składu osobowego kontyngentu Sił Zbrojnych Federacji Rosyjskiej, stacjonującego zgodnie z międzynarodowym układem na terytorium Ukrainy (Autonomiczna Republika Krymu), na podstawie punktu +g+ części 1. artykułu 102. Konstytucji Federacji Rosyjskiej przedkładam Radzie Federacji Zgromadzenia Federalnego Federacji Rosyjskiej wniosek o użycie Sił Zbrojnych Federacji Rosyjskiej na terytorium Ukrainy do czasu normalizacji sytuacji społeczno-politycznej w tym kraju[176].”

Na wniosek władz Ukrainy odbyło się posiedzenie Rady Bezpieczeństwa ONZ. Działania Rosji na Krymie potępiły m.in. kraje NATO oraz G7.

Codzienność na zajętych w wyniku działań hybrydowych terenach Krymu ukazywała utrudnienia w funkcjonowaniu usług dla ludności, ale i presję okupanta. Nowe władze krymskie rozpoczęły cenzurowanie i zastraszanie lokalnych mediów. Ponadto, strona rosyjska była oskarżana o blokowanie połączeń telefonii komórkowej w niektórych miejscach na Krymie. Na Krymie pojawiły się problemy z niedostarczającą przesyłek pocztą oraz z bankomatami (nie działały lub zezwalały na wypłatę tylko niewielkich sum). Większość transakcji na półwyspie odbywała się z użyciem gotówki.

Czynni byli też prorosyjscy aktywiści w cywilnych ubraniach, którzy zakłócali pracę dziennikarzy chcących relacjonować wydarzenia na Krymie stosując groźby oraz używając siły. Wpisując się w kontekst walki informacyjnej, rosyjskie media podawały, że Ukraina nie opłaca bieżących rachunków za gaz ziemny i nie uregulowała długu za 2013 r. Ogłoszono także, że Krym jest gotowy przyjąć jako walutę rosyjskiego rubla, a ukraińska własność państwowa na półwyspie zostanie znacjonalizowana.

Żołnierze bez dystynkcji byli przerzucani na teren Krymu początkowo z użyciem m.in. cywilnych mikrobusów i ciężarówek. Siły rosyjskie na Krymie stopniowo zajmowały kolejne obszary, w tym ośrodki stacjonowania wojsk Ukrainy, które zgodnie z rozkazem z Kijowa były generalnie bierne (miały nie prowokować działań zbrojnych). Pojawiły się także sygnały, że separatyści podejmowali próby przekupienia ukraińskich żołnierzy, proponując im awanse i mieszkania (m.in. w Sewastopolu).

Biorąc pod uwagę fakt, że w momencie kryzysu armia ukraińska liczyła kilkaset tysięcy żołnierzy (na Krymie pełniło służbę ok. 13 tys. żołnierzy ukraińskich), warto

[176] *Rada Federacji Rosyjskiej za operacją na Ukrainie*, TVP Info, 01.03.2014, https://www.tvp.info/14214218/rada-federacji-rosyjskiej-za-operacja-na-ukrainie [dostęp: 13.06.2022].

odnotować użycie przez Rosję stosunkowo ograniczonych sił zbrojnych. Liczba żołnierzy działających na rzecz Federacji Rosyjskiej na Krymie, według szacunków wynosiła ok. 20 tys. wraz ze sprzętem (samochody ciężarowe, transportery opancerzone) oraz ok. 11 tys. żołnierzy z Floty Czarnomorskiej.

Między 8 lutego i 4 marca 2014 r. siły zbrojne Rosji i samoobrony Krymu zajęły większość obiektów o znaczeniu strategicznym na półwyspie, m.in. przeprawę promową w Kerczu, lotniska: wojskowe w Kirowskoje i zapasowe w Dżanko oraz port lotniczy w Symferopolu. Strona rosyjska zajęła także bazę lotnictwa taktycznego w Sewastopolu, w tym lotnisko Belbek wraz ze stacjonującymi tam samolotami. Ponadto, rosyjskie posterunki rozmieszczono przy kluczowych polaczeniach drogowych na Krymie. Działaniom wojskowym towarzyszyła wojna informacyjna z nasilonymi działaniami celowej dezinformacji[177].

Ukraińcy podjęli decyzję o postawieniu sił zbrojnych w stan najwyższej gotowości (2 marca 2022 r.) i rozpoczęli mobilizację. Najszybciej pełną zdolność bojową osiągnęły jednostki sił szybkiego reagowania liczące około 20 tys. żołnierzy, które były jedyną dobrze wytrenowaną i wyposażoną strukturą armii ukraińskiej. Część z tych sił (m.in. batalion piechoty morskiej), jak informował A. Wilk, pozostawała jednak zablokowana przez stronę rosyjską na Krymie[178].

7 marca 2014 r. żołnierze agresora szturmowali ukraińską bazę wojskową w Sewastopolu (sforsowano bramę ciężarówką KAMAZ i usiłowano się przebić do siedziby dowództwa; nie doszło do wymiany ognia). Nieoznakowani żołnierze przejęli też broń z bazy wojskowej w Sudaku. Separatyści umiejętnie wykorzystywali także propagandowo niektóre wydarzenia. Kontradmirał Denis Berezowski przysiągł wierność narodowi krymskiemu podczas konferencji zorganizowanej z premierem Republiki Autonomicznej Krymu, za co został odwołany ze stanowiska przez władze Ukrainy. Nośność tego incydentu była znacząca z uwagi na fakt, że był to sam dowódca ukraińskiej marynarki wojennej, który jeszcze w 2012 i 2013 r. był odpowiedzialny za przeprowadzenie wspólnych, ukraińsko-amerykańskich ćwiczeń wojskowych na morzu (Sea Breeze).

[177] A. Wilk, *Rosyjska interwencja wojskowa na Krymie,* Analizy – Ośrodek Studiów Wschodnich, 2014-03-05, https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [odstęp 13.06.2022].

[178] Tamże.

11 marca 2014 r. deputowani Republiki Autonomicznej Krymu przyjęli deklarację niepodległości Republiki Krymu, w której powołano się na przypadek Kosowa argumentując, iż nawet jednostronna deklaracja tego typu ze strony określonej społeczności czy terytorium nie narusza prawa międzynarodowego. W dokumencie stwierdzono: „My, deputowani Rady Najwyższej Autonomicznej Republiki Krymu i Rady Miejskiej Sewastopola, przyjęliśmy tę wspólną decyzję zgodnie z postanowieniami Karty Narodów Zjednoczonych i szeregiem innych dokumentów międzynarodowych, które potwierdzają prawo narodów do samostanowienia, a także uwzględniając uchwałę międzynarodowego trybunału ONZ w sprawie Kosowa z 22 lipca 2010 r. potwierdzającą, że jednostronna deklaracja niepodległości przez część danego państwa nie narusza żadnych norm prawa międzynarodowego[179].”

16 marca 2014 r. na Krymie rozpoczęło się referendum ws. przyłączenia półwyspu do Rosji. Do głosowania było uprawnionych około 1,5 mln osób. Ponad 96% głosujących miało opowiedzieć się za przyłączeniem terytorium Autonomicznej Republiki Krymu oraz miasta wydzielonego Sewastopola do Federacji Rosyjskiej (przy 83% frekwencji). Plebiscyt ten – jak wskazują analitycy OSW – nie był prawomocny i miał zalegalizować oderwanie Krymu od Ukrainy.

Dwa dni po referendum, prezydent Putin podpisał traktat włączający Krym do Federacji Rosyjskiej. Natomiast, 21 marca 2014 r., po ratyfikacji traktatu aneksyjnego przez rosyjski parlament, prezydent Federacji Rosyjskiej podpisał ustawę formalnie integrującą Krym z Rosją. Dokonano zmian w konstytucji dopisując do niej dwa nowe podmioty federacji – Republikę Krymu i miasto federalnego znaczenia Sewastopol[180].

Referendum odbywało się z problemami (m.in. Tatarzy krymscy zbojkotowali proces wyborczy i nie znaleziono chętnych do zasiadania w komisjach w zamieszkanych przez nich osiedlach). W trakcie trwania referendum zauważono liczne nieprawidłowości w procesie głosowania, w tym – obecność w lokalach wyborczych uzbrojonych mężczyzn. Niezależnym dziennikarzom i obserwatorom utrudniano monitorowanie procesu liczenia głosów.

[179] *Crimea parliament passes independence declaration*, Interfax News Agency, 11 Mar 2014, https://interfax.com/newsroom/top-stories/44577/ [dostęp: 23.06.2022].

[180] A. Wilk, T. A. Olszański, W. Górecki, Porozumienie mińskie – rok gry pozorów, OSW, 2016-02-10 https://www.osw.waw.pl/pl/publikacje/analizy/2016-02-10/porozumienie-minskie-rok-gry-pozorow [dostęp: 20.06.2022 r.].

Kilkutysięczny tłum zebrał się w Symferopolu, aby zademonstrować poparcie dla przyłączenia Krymu do Rosji. Podczas odbywających się później innych referendów lokalnych na terenach opanowanych przez separatystów prorosyjskich także zaobserwowano poważne nieprawidłowości: wyborcy oddawali wiele kart do głosowania, a ukraińska policja twierdziła, że przechwyciła 100 tys. wstępnie wypełnionych kart do głosowania[181]. Jednocześnie, cały czas trwały działania propagandowe separatystów.

Krymskie referendum nie zostało uznane przez rząd w Kijowie, który uznał propozycję przyłączenia części swojego terytorium do Federacji Rosyjskiej za niezgodną z konstytucją. W krajach zachodnich zostało ono uznane za nielegalne, natomiast Rosja zapowiedziała, że uzna jego wyniki. Stany Zjednoczone i Unia Europejska przystąpiły do nałożenia sankcji na rosyjskich urzędników, członków samozwańczego rządu i parlamentu krymskiego (zamrożenie aktywów i zakaz podróżowania). Aneksja Krymu była złamaniem przez Rosję podpisanego w grudniu 1994 r. porozumienia, które gwarantowało integralność terytorialną Ukrainy[182]. Organizacja Narodów Zjednoczonych wielokrotnie potwierdzała, że Krym pozostaje integralną częścią Ukrainy Zasadność rosyjskiej aneksji uznało kilka przychylnych wówczas rosyjskiej polityce krajów: Afganistan, Kuba, Korea Północna, Kirgistan, Nikaragua, Sudan, Syria, Zimbabwe, a także pozostające poza ONZ zależne od Moskwy byty para-państwowe Abchazja i Osetia Południowa[183].

Aneksja Krymu miała cechy ataku hybrydowego. Co więcej, operacja wojskowa, która rozpoczęła się w nocy z 27 na 28 lutego 2014 r. na Krymie mająca na celu przejęcie kontroli nad półwyspem przez Rosję, jak ocenił A. Wilk, spełniała kryteria agresji zbrojnej. Rosjanie użyli stacjonujących tam jednostek Floty Czarnomorskiej oraz przerzucanych na półwysep innych formacji armii rosyjskiej. Były one wspierane przez oddziały tzw. samoobrony Krymu i przejęły kontrolę nad większością strategicznych obiektów: lotnisk, znaczących dróg i przepraw, a także infrastruktury armii i struktur bezpieczeństwa Ukrainy (głównie straży granicznej). Większość ukraińskich jednostek wojskowych została

[181] T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa…, s. 34.*

[182] To tzw. Memorandum budapeszteńskie podpisane zostało przez Rosję, USA, Wielką Brytanię i Ukrainę. W memorandum Kijów zobowiązał się do przekazania broni nuklearnej Rosji i przystąpienia do układu o nieproliferacji broni masowego rażenia.

[183] Po nowej agresji rosyjskiej na Ukrainę w 2022 r. i ogłoszeniu niepodległości przez kolejne terytoria Ukrainy, oprócz Rosji, niepodległość separatystycznych – Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej – uznała Syria i Korea Północna.

zablokowana przez Federację Rosyjską w miejscach dyslokacji. Obie strony uchylały się przy tym od bezpośredniego użycia broni[184].

W momencie rozpoczęcia operacji siły rosyjskie i ukraińskie na Krymie były względnie wyrównane (po około 15 tys. żołnierzy), z zastrzeżeniem, że kontyngent Floty Czarnomorskiej miał przewagę w zakresie potencjału morskiego i lotniczego, jakości wyposażenia i wyszkolenia.

Za wysoce prawdopodobne analityk OSW uznał również możliwość, iż część samoobrony Krymu stanowili żołnierze rosyjscy z etatowym wyposażeniem (tylko bez dystynkcji). Ponadto, pozostałą część samoobrony mogli stanowić w przeważającej mierze mieszkający lokalnie byli żołnierze Floty Czarnomorskiej i funkcjonariusze oddziałów specjalnych ukraińskiej milicji Berkut[185].

Na marginesie warto odnotować, że w czasie utrzymującego się zainteresowania zachodnich mediów sytuacją na Krymie, strona ukraińska negocjowała z Międzynarodowym Funduszem Walutowym pakiet ratunkowy o wartości 35 miliardów USD. Premier Jaceniuk podpisał także część umowy stowarzyszeniowej z UE, która w listopadzie 2013 r. została odrzucona przez Janukowycza[186].

Rosja umacniała swoją pozycję na Krymie i stosowała szeroki wachlarz działań hybrydowych – także w postaci nacisków energetycznych. Z uwagi na zajęcie całego półwyspu, Moskwa unieważniła traktat z Ukrainą na dzierżawę portu w Sewastopolu i Kijów utracił – wynikającą z tej umowy – zniżkę na gaz ziemny. W ciągu zaledwie kilku tygodni cena gazu dla Ukrainy wzrosła o ok. 8%. Rosja otwarcie wywierała tym samym presję ekonomiczną na rząd tymczasowy w Kijowie oraz osłabiała gospodarczo swojego przeciwnika[187].

Rosja nie tylko manipulowała obawami społecznymi występującymi w społeczeństwach sąsiadujących z Ukrainą, ale także tworzyła informacje, które nie miały pokrycia w rzeczywistości. Przykładem, który przytoczyli Jurij Hajduk i Tomasz Stępniewski, było podanie 5 marca 2014 r. przez stację „Rossija 1" informacji, że do Kijowa przyjechało 300 uzbrojonych amerykańskich najemników w celu przygotowania „czystek

[184] A. Wilk, *Rosyjska interwencja wojskowa na Krymie…*
[185] Tamże.
[186] *The crisis in Crimea and eastern Ukraine...*
[187] Tamże.

etnicznych" ludności rosyjskiej w Odessie i Lwowie (wykonawcą miał być ukraiński Prawy Sektor)[188].

Co warte odnotowania w kontekście skuteczności metod hybrydowych, przejęcie Krymu odbyło się w sposób prawie bezkrwawy. Przyczyniła się do tego bardzo dobrze przygotowana operacja Rosji oraz – nastawiona w większości prorosyjsko – ludność na Krymie.

Po przejęciu Krymu, przedstawiciele Rosji publicznie twierdzili, że nie mają dodatkowych planów na terytorium Ukrainy, ale okazało się to celową dezinformacją wpisaną w operację hybrydową. Na początku kwietnia 2014 r. źródła natowskie ujawniły obecność ok. 40 tys. żołnierzy rosyjskich, którzy byli zgrupowani w stanie wysokiej gotowości tuż przy granicy z Ukrainą. Był to element wojny psychologicznej mającej sparaliżować władze w Kijowie i zablokować ich potencjalną reakcję obronną w obawie przed eskalacją działań na teren całej Ukrainy. Uzbrojeni prorosyjscy rebelianci zaatakowali następnie budynki rządowe we wschodnio-ukraińskich miastach Donieck, Ługańsk, Gorłówka i Kramatorsk. Relacje świadków mówiły o działających z wojskową precyzją mężczyznach w mundurach bez insygniów posługujących się rosyjskim sprzętem[189].

Gdy w Genewie rozpoczęły się rozmowy między Stanami Zjednoczonymi, UE, Rosją i Ukrainą, krwawe starcia trwały m.in. w Mariupolu. Wszystkie strony w Genewie zgodziły się z koniecznością deeskalacji konfliktu we wschodniej Ukrainie. Jednak w praktyce prorosyjscy bojownicy rozszerzali strefę wpływów zajmując kolejne budynki rządowe i ustanawiając punkty kontrolne. Dodatkowo, Rosja rozpoczęła manewry wojskowe po swojej stronie granicy. Trwały także działania terroryzujące społeczność lokalną i jej elitę. Pod koniec kwietnia 2014 r. przedstawiciel rady miejskiej Horłówki Wołodymyr Rybak został porwany i zabity przez prorosyjską milicję. Łącznie odnotowano w tamtym czasie kilkudziesięciu uprowadzonych i przetrzymywanych przez siły prorosyjskie, w tym ośmiu członków misji obserwacyjnej Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE), szereg ukraińskich i zachodnich dziennikarzy oraz kilku członków ukraińskiej policji i służb bezpieczeństwa. Miał miejsce także przypadek zamachu na mera Charkowa, Giennadija Kernesa. Ten członek prorosyjskiej Partii Regionów został poważnie zraniony

[188] J. Hajduk, T. Stępniewski, *Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty*, Studia Europejskie, 4/2015 https://journalse.com/pliki/pw/4-2015_hajduk.pdf [dostęp: 23.11.2022].

[189] Tamże.

przez snajpera po tym, jak zadeklarował poparcie dla prozachodniego kierunku Ukrainy[190]. Wszystko to pokazuje skalę działań hybrydowych stosowanych w konflikcie o Krym a później także w czasie wojny w Donbasie.

Szybkie opanowanie Krymu przez stronę rosyjską wynikało, w ocenie A. Wilka, z dobrego przygotowania sił Federacji Rosyjskiej do prowadzenia działań – w tym zwłaszcza hybrydowych. Realizacja celu Kremla była możliwa także z uwagi na dezorientację żołnierzy ukraińskich, którzy rozkazy utrzymania pozycji otrzymali dopiero 1 marca. Ponadto, odsiecz ze strony Ukraińców była utrudniona w związku ze zgromadzeniem wojsk Rosji wzdłuż lądowej granicy rosyjsko-ukraińskiej i groźbą interwencji militarnej na całym terytorium Ukrainy[191].

Rosja złamała przy tym szereg zapisów bilateralnych porozumień z Ukrainą w tym m.in. dotyczących naruszenia integralności terytorialnej, zasady niestosowania siły lub groźby jej użycia, a także nieingerowania w sprawy wewnętrzne. Ponadto, działania formacji samoobrony Krymu na początku rosyjskiej operacji mogły być traktowane, jako działająca na terytorium Ukrainy organizacja przestępcza o charakterze zbrojnym. Inicjując operację wojskową na Krymie i eskalując sytuację w południowo-wschodnich obwodach Ukrainy, Federacja Rosyjska, jak dowodzi A. Wilk, naruszyła trzy porozumienia dwustronne:

a) „o przyjaźni, współpracy i partnerstwie *z 31 maja 1997 r.* (stanowiące podstawę prawną stosunków rosyjsko-ukraińskich);

b) o statusie i warunkach przebywania Floty Czarnomorskiej Federacji Rosyjskiej na terytorium Ukrainy *z 28 maja 1997 r.;*

c) o parametrach podziału Floty Czarnomorskiej [sowieckiej] *z 28 maja 1997 r.*[192]*”*

Poza aneksją Krymu w 2014 r. cennych lekcji w zakresie *modus operandi* rosyjskiej wojny hybrydowej (elementy, sposoby działania, oryginalność rozwiązań ofensywnych) dostarcza wojna w Donbasie we wschodniej Ukrainie.

[190] Tamże.
[191] A. Wilk, *Rosyjska interwencja wojskowa na Krymie…*
[192] Tamże.

Wybuch starć w Donbasie[193] datuje się na 6 kwietnia 2014. Dokonano wówczas próby siłowego zajęcia najważniejszych ośrodków administracji lokalnych donieckiego zagłębia węglowego. Trzy tygodnie po zakończeniu przez Rosję operacji na Krymie, protestujący zajęli przemocą budynki rządowe w miastach Donieck, Ługańsk i Charków wzywając do niezależności tych terenów od Ukrainy. Dziesięć dni później, jak przypomina K. DeBenedictis, w Mariupolu zginęło trzech prorosyjskich separatystów, którzy próbowali przejąć instalację wojskową. Konflikt wkrótce stał się bardziej krwawy niż aneksja Krymu, gdzie odnotowano łącznie po obu stronach zaledwie kilka ofiar śmiertelnych. Ukraiński rząd odpowiedział operacją wojskową na pełną skalę, która musiała stawić czoła zaciekłemu oporowi ze strony separatystów otrzymujących znaczące wsparcie wojskowe z Rosji[194].

W maju 2014 r. ogłoszono powołanie konfederacji nowoutworzonych republik w postaci tzw. Federacyjnej Republiki Noworosji. Stosując metodę faktów dokonanych prorosyjscy separatyści ogłosili utworzenie samozwańczych tworów para-państwowych Donieckiej Republiki Ludowej i Ługańskiej Republiki Ludowej.

Między marcem i majem 2014 r. w wielu miejscach Ukrainy strona rosyjska, w ocenie części ekspertów, podjęła próby powtórzenia scenariusza krymskiego: przejmowania budynków państwowych i tworzenia prorosyjskich republik ludowych. Mogło to świadczyć nawet o woli podporządkowania sobie większej części wschodniej Ukrainy[195]. Rosyjscy nacjonaliści określili ten okres mianem "Rosyjskiej Wiosny". Jednak sentymenty prorosyjskie okazały się za słabe m.in. w Charkowie, Dnietropawłowsku czy Odessie, gdzie przeważyli prozachodnio nastawieni protestujący[196]. W maju 2014 r. starcia sił ukraińskich

[193] Donbas to najbardziej wysunięta na wschód, graniczącą z Rosją część Ukrainy, a równocześnie kraina historyczna i bogaty w złoża węgla i innych surowców okręg przemysłowy (obwód doniecki i ługański) i w południowo-zachodniej Rosji (obwód rostowski). Leżący nad Dońcem Donbas jest regionem o największej gęstości zaludnienia na Ukrainie (wyłączając Kijów). Donieck i Ługańsk są najważniejszymi miastami odpowiednio obwodu donieckiego i ługańskiego. Donieck jest przy tym uważany za nieoficjalną stolicę całej krainy (Donbasu). Od połowy XIX w. rozwijał się tu przemysł hutniczy, elektromaszynowy, taboru kolejowego i maszyn budowlanych, do czego przyczyniali się m.in. inwestorzy z krajów zachodnich m.in. z Niemiec, Wielkiej Brytanii, Francji i Walii.

[194] K. DeBenedictis, *Russian Hybrid Warfare and the Annexation of Crimea The Modern Application of Soviet Political Warfare*, Londyn 2022.

[195] Na marginesie warto odnotować, że ten *modus operandi* obserwowany był także w czasie tzw. „wyzwalania" przez Rosję Polski i innych krajów w czasie i po II wojnie światowej. De facto zostały one zagarnięte siłą na radziecką stronę *Żelaznej Kurtyny*. Także w tamtych przypadkach Moskwa powoływała się na konieczność ochrony ludności rosyjskojęzycznej.

[196] W strategicznie ważnym Dniepropietrowsku walkę przeciwko prorosyjskim separatystom wspierał oligarcha – posiadający ukraiński, izraelski oraz cypryjski paszport – Ihor Kolomoyskyy, który oferował duże sumy pieniędzy za schwytanie rosyjskich żołnierzy. Sfinansował on także szereg batalionów

i prorosyjskich separatystów miały miejsce m.in. w Słowiańsku oraz w Odessie, gdzie dziesiątki prorosyjskich demonstrantów zginęło w pożarze zajmowanego przez nich budynku.

Rosji udało się wesprzeć proces przekształcania milicji złożonych z prorosyjskich separatystów w liczącą 40 tys. armię republik: Donieckiej i Ługańskiej. Działania hybrydowe strony rosyjskiej na Ukrainie niewątpliwie ułatwiały dekady zaniedbań w zakresie reform wzmacniających państwo, poważna korupcja, które uzupełniała skuteczne rozgrywanie wywiadowcze przy bierności spenetrowanych obcą agenturą służb ukraińskich[197]. To też bardzo ważne czynniki osłabiające możliwość przeciwdziałania zagrożeniom hybrydowym.

Po przejęciu głównych budynków proklamowano utworzenie dwóch (nieuznawanych wówczas międzynarodowo) bytów para-państwowych: Ługańskiej Republiki Ludowej i Donieckiej Republiki Ludowej. Towarzyszyła temu dobrze skoordynowana kampania z użyciem środków dyplomatycznych, gospodarczych oraz medialnych na Ukrainie oraz za granicą. Dodatkowym elementem presji było rozlokowanie rosyjskich wojsk wzdłuż granicy z Ukrainą[198].

19 maja 2014 r. – po długim milczeniu – oligarcha Rinat Achmetow poparł władze w Kijowie i próbował zorganizować akcje protestacyjne wymierzone w separatystów. Oświadczenie Achmetowa wywołało eskalację w Donbasie. Separatyści obawiali się zmobilizowania pracowników zakładów przemysłowych i kopalń oligarchy. W odpowiedzi prorosyjscy rebelianci przeprowadzili demonstrację siły pod Wołnowachą, gdzie 22 maja 2014 r. spowodowali straty w liczbie 50 żołnierzy ukraińskich (zabici i ranni). Były to najdotkliwsze straty sił zbrojnych Ukrainy w ich 23-letniej historii. Ponadto, nasiliły się akcje

złożonych z najemników (np. Azow). Jego działania, oraz podobne kroki przedsięwzięte przez innych Ukraińców pochodzenia żydowskiego, stanowiły pożywkę dla rosyjskiej propagandy informującej o rzekomym spisku z ich udziałem z czynnym zaangażowaniem Zachodu. Komentatorzy przychylni stronie rosyjskiej wskazywali, że Kolomoysky stał także za wsparciem finansowym Euromaidanu (2013 / 2014 r.). Media DNR i LNR potępiały przy tym sojusz "żydowskich oligarchów" ukraińskich faszystów i zachodnich rządów. Pojawiały się w tym kontekście nazwiska Petra Poroshenki, Yatsenyuka i Julii Tymoshenko. *T. Kuzio, P. D'Anieri, Annexation and Hybrid Warfare in Crimea…*

[197] Tamże.

[198] W kwietniu 2014 r., jak zauważa A. Racz, we wschodniej Ukrainie (w Doniecku i Ługańsku) rozpoczęła się wzmożona aktywność separatystów, która bardzo przypominała schematy obserwowane wcześniej na Krymie. Zob. A. Rácz, *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf [dostęp: 28.09.2021].

separatystów w miastach leżących na przecięciu głównych szlaków transportowych, sparaliżowany został ruch lotniczy i częściowo kolejowy[199].

Chociaż strona rosyjska nadal zaprzeczała udziałowi w konflikcie, w sierpniu 2014 r. Moskwa potwierdziła, że oddział rosyjskich spadochroniarzy został schwytany na Ukrainie. Po tym, jak władze ukraińskie opublikowały wideo-wywiady więźniów, przedstawiciele Federacji Rosyjskiej oświadczyli, że żołnierze przekroczyli granicę przypadkowo.

Pod koniec sierpnia 2014 r. sytuacja diametralnie zmieniła się na niekorzyść Ukrainy. Siły rebeliantów otworzyły nowy front na południu, zdobywając miasto Nowoazowsk i zagrażając kluczowemu portowi Donbasu – Mariupolowi nad Morzem Azowskim. Analitycy NATO oszacowali, że w konflikcie aktywnie uczestniczyło w tamtym czasie ponad 1000 żołnierzy rosyjskich. 5 września 2014 r. rządy Ukrainy i Rosji spotkały się z przywódcami separatystów w Mińsku na Białorusi i zgodziły się na zawieszenie broni, które tymczasowo spowolniło, ale – jak się wkrótce okazało – nie powstrzymało przemocy. 2 listopada 2014 r. separatyści przeprowadzili wybory samorządowe w Doniecku i Ługańsku z naruszeniem porozumienia mińskiego. Władze ukraińskie i państw zachodnich odrzuciły wyniki, które faworyzowały kandydatów prorosyjsko nastawionych separatystów[200]. 5 września 2014 r. w Mińsku Ukraina, Rosja i OBWE (członkowie tzw. trójstronnej grupy kontaktowej) oraz przedstawiciele separatystów podpisali zawieszenie broni. Porozumienie miało charakter ogólny i nie przesądziło o stabilizacji sytuacji na ukraińskim wschodzie.

W reakcji na ofensywną postawę sił separatystów wspieranych przez Federację Rosyjską, nastąpił kontratak. Siły zbrojne Ukrainy rozpoczęły – jak to określono – operację antyterrorystyczną (ATO). Władze w Kijowie przedstawiały w swoich komunikatach działania Rosji jako wojnę przez pośredników (proxy) określając rosyjskie jednostki na terytorium Ukrainy, jako terrorystów. Na początku 2015 r., prawie rok od rozpoczęcia operacji zajęcia Krymu, parlament Ukrainy oficjalnie uznał Rosję za agresora, a separatystyczne „republiki" za organizacje terrorystycznie. W styczniu 2015 r. Organizacja

[199] A. Wilk, P. Żochowski, W. Konończuk, *Konflikt w Donbasie – wymuszona deeskalacja?* ANALIZY OSW, 2014-06-11 https://www.osw.waw.pl/pl/publikacje/analizy/2014-06-11/konflikt-w-donbasie-wymuszona-deeskalacja [dostęp: 29.06.2022].

[200] *The crisis in Crimea and eastern Ukraine*...

Narodów Zjednoczonych oszacowała, że od początku działań wojennych zginęło ponad 5000 osób.

Pod koniec stycznia 2015 r. rebelianci zajęli sporne lotnisko w Doniecku, które ostatecznie – po miesiącach ciężkich walk – zostało kompletnie zniszczone. Zwrócili się następnie w kierunku zdobycia kontrolowanego przez Ukrainę miasta. W tym samym czasie trwały rozmowy na szczeblu politycznym, które toczyły się niemal równocześnie ze starciami zbrojnymi. Zdobywanie przez jedną ze stron przewagi na froncie było naturalnie wykorzystywane jako argument w negocjacjach, 12 lutego 2015 r. przywódcy Ukrainy, Rosji, Francji i Niemiec uzgodnili 12-punktowy plan pokojowy, w którym zaproponowano m.in. zaprzestanie walk, wycofanie ciężkiej broni, uwolnienie więźniów i usunięcie obcych wojsk z terytorium Ukrainy. Zapanował kruchy pokój, a ciężka broń została wycofana przez obie strony (na początku września 2015 r.). Częste naruszenia rozejmu spowodowały jednak, że do końca roku odnotowano ponad 9 000 zabitych i ponad 20 000 rannych. Rosja nadal zaprzeczała swojemu udziałowi w konflikcie. W maju 2015 r. prezydent Putin podpisał dekret zakazujący upubliczniania informacji o przypadkach śmierci żołnierzy rosyjskich podczas „operacji specjalnych”[201].

Mimo podejmowania prób politycznego rozwiązania konfliktu zakończyły się one niepowodzeniem. Zawarte 12 lutego 2015 r. przez przedstawicieli Rosji i Francji, Niemiec i Ukrainy porozumienie mińskie okazało się nieskuteczne. Pełne wycofanie ciężkiego uzbrojenia ze strefy buforowej nie nastąpiło. Sytuacja w niekontrolowanej przez Kijów części Donbasu była patowa.

Rosji udało się spowolnić, ale nie zatrzymać proces integracji Ukrainy ze strukturami zachodnimi – zwłaszcza gospodarczymi. 1 stycznia 2016 r. zaczęła obowiązywać umowa o pogłębionej i kompleksowej strefie wolnego handlu (DCFTA), którą UE i Ukraina wstępnie podpisały w czerwcu 2014 r. Utrzymujący się przez długi czas stan zamrożonego konfliktu, z okresami eskalacji starć i ofiar po obu stronach, był korzystny dla Rosji, gdyż osłabiał Ukrainę wewnętrznie. Ponadto, postępowała gospodarcza i społeczna degradacja terytoriów objętych konfliktem[202].

[201] Tamże.
[202] A. Wilk, T. A. Olszański, W. Górecki, Porozumienie mińskie...

Celem strategicznym wojny hybrydowej Rosji, w ocenie ekspertów OSW, było narzucenie stronie ukraińskiej rozwiązań politycznych gwarantujących jej kontrolę nad państwem ukraińskim, co zablokowałoby Ukrainę w strefie wyłącznych wpływów rosyjskich i na trwałe uniemożliwiłoby jej integrację z UE i z NATO. Sposobem na osiągnięcie tych celów miała być tzw. federalizacja Ukrainy (obdarzenie jej regionów szeroką autonomią) oraz międzynarodowe (w tym rosyjskie) gwarancje niezmienności neutralnego statusu Ukrainy. W tym kontekście aneksja Krymu miała być właśnie elementem presji na władze w Kijowie, by skłonić je do akceptacji rosyjskich warunków. Ich przyjęcie przez Kijów (i wspierający go Zachód) oznaczałoby *de facto* przekształcenie Ukrainy w rosyjski protektorat[203].

Pomimo operacji antyterrorystycznej na wschodzie Ukrainy Kijów utracił kontrolę nad znaczną częścią regionu, w tym – Donieckiem i Ługańskiem. Nieskuteczność sił ukraińskich oraz pomoc wojskowa z Rosji znacząco wzmocniły potencjał separatystów. Do Donbasu przybyło około 3 tys. działających na rzecz Federacji Rosyjskiej uzbrojonych najemników, co – w opinii badaczy z krajów zachodnich – oznaczało potwierdzenie faktycznego wsparcia zbrojnego ze strony Rosji[204].

Operacja antyterrorystyczna w Donbasie, która w zamyśle Ukraińców, miała wykazać zdecydowanie władz w walce z inspirowanym przez Rosję separatyzmem na wschodzie, przyniosła słaby efekt propagandowy. Po początkowych sukcesach (m.in. zablokowanie przez siły ukraińskie szlaku transportowego między wschodnią Ukrainą i Krymem), nie udała się próba odbicia z rąk separatystów Mariupola (7–9 maja 2014 r.), gdzie żołnierze wysłani przez władze w Kijowie napotkali opór wrogo nastawionej miejscowej ludności i byli zmuszeni wycofać się.

Próba oceny ukraińskiej operacji antyterrorystycznej wypada na korzyść prowadzącej wojnę hybrydową Rosji. Działania rządowych sił ukraińskich, jak piszą A. Wilk, T. A. Olszański, W. Górecki: „ujawniły w krótkim czasie nieprzygotowanie żołnierzy Sił Zbrojnych i funkcjonariuszy MSW Ukrainy do prowadzenia nieregularnych walk z rozproszonym i zachowującym dużą mobilność przeciwnikiem. (…) Pomimo stopniowego

[203] Tamże.
[204] A. Wilk, P. Żochowski, W. Konończuk, *Konflikt w Donbasie…*

napływu nowych pododdziałów i szerszego włączenia do działań lotnictwa (prowadzenie pozorowanych ataków na cele naziemne), opór separatystów nie uległ osłabieniu[205].”

Istotny wymiar miała hybrydowa wojna informacyjna. Strona ukraińska nie prowadziła kampanii informacyjnych wśród mieszkańców, dla których głównym dostarczycielem informacji stały się kreujące w wielu przypadkach nieprawdziwy obraz sytuacji w Doniecku media prorosyjskie[206]. Ważnym czynnikiem działającym na korzyść Rosji był też fakt, że ewentualna próba wyparcia separatystów wiązałaby się z koniecznością walk miejskich przekładających się prawie zawsze na duże straty wśród ludności cywilnej.

W dokumentach USA, wydarzenia na Krymie były przedstawiane jako przykład zagrożeń hybrydowych objawiających się w kombinacji działań sił konwencjonalnych oraz nieregularnych. W amerykańskiej strategii wojskowej (*The National Military Strategy of the United States of America 2015)* eksperci Pentagonu, oskarżyli Rosję o użycie tego typu taktyki zaznaczając, że „działania hybrydowe mogą polegać na wykorzystaniu państwowych sił zbrojnych udających afiliację z organizmami pozapaństwowymi tak jak zrobiła to strona rosyjska na Krymie[207].”

Podejście rosyjskie, które wypracowało latami skuteczne metody działań hybrydowych i umożliwiło przejęcie Krymu w 2014 r. kształtowało się w czasie innych konfliktów z udziałem Kremla. Przedstawiając doświadczenia z Syrii, gen. Gierasimow zwrócił uwagę na główne elementy rozwoju rosyjskiej strategii wojskowej. Chodziło o ograniczone działania poza granicami Rosji noszące znamiona uderzenia wyprzedającego[208]. Mają one na celu przeciwdziałanie zagrożeniom dla rosyjskich interesów narodowych przez selektywne zastosowanie interwencji militarnej poza granicami[209].

Na pierwszy plan wysuwają się tu asymetryczne i nieliniowe metody działania z uwzględnieniem czynnika przewagi siły i zaskoczenia, co ma znaczenie dla uzyskania

---

[205] Tamże.

[206] Tamże.

[207] G. Filimonov, *The Color Revolutions in the Context of Hybrid Wars, Hybrid Conflicts And Information Warfare New Labels, Old Politics* [w:] O. Fridman, V. Kabernik, J. C. Pearce (z-lib.org) s. 27.

[208] M. Boulègue A. Polyakova, *The Evolution of Russian Hybrid Warfare*, 29 stycznia 2021 r. https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/ [dostęp: 28.09.2021].

[209] Warto zauważyć, że podobne cechy wydaje się mieć m.in. sztucznie wywołany kryzys migracyjny na granicy białorusko-polskiej w 2021 r., stanowiący jawny przykład użycia demograficznej broni hybrydowej w postaci rzekomych uchodźców głównie z Afganistanu. Celem mogło być ukaranie Polski za wsparcie białoruskiej opozycji i próby odsunięcia przez nią od władzy stronnika Kremla w Mińsku – prezydenta Łukaszenki.

dominacji informacyjnej. Strategia czynnej (aktywnej) obrony ma na celu „zapobiegawczą neutralizację zagrożeń przez aktywne działania". Ta obrona aktywna kładzie nacisk na niemilitarne środki działania i wykorzystuje rosyjskie narzędzia w postaci – rozwijanej, od co najmniej XIV w. – strategii wojskowej maskowania działań (ros. маскировка) [210].

Ponadto, strona rosyjska wykorzystywała w przeszłości tzw. prywatne firmy wojskowe, które były istotnym elementem działań hybrydowych. Z uwagi na brak bezpośredniego powiązania z siłami zbrojnymi, najemnicy Ci posiadają dużą elastyczność prowadzenia akcji i mogli stosować m.in. metody terrorystyczne. Tacy kontraktorzy wspierali separatystów na Krymie i w Donbasie, a także ochraniali infrastrukturę energetyczną w Syrii (np. Grupa Wagnera czy RSB-Group[211] – realizująca kontrakty m.in. dla ONZ)[212]. Wszystko to były działania sprzyjające realizacji interesów Rosji.

Najemnicy Wagnera[213] pojawili się po raz pierwszy na Krymie w lutym 2014 r., gdzie działali ramię w ramię z regularnymi jednostkami armii rosyjskiej wspierając rozbrajanie Ukraińców i przejmowanie kontroli nad wyselekcjonowanymi obiektami mającymi znaczenie dla funkcjonowania władz lokalnych.

Zatrudniając „kontraktorów", jak trafnie zauważa F. Bryjka, Moskwa prowadziła w Donbasie wojnę przez pośredników (*war by proxy*). Po zajęciu Krymu kilkuset paramilitarnych żołnierzy, których zaczęto określać, jako „małe zielone ludziki" trafiło do regionu Donbas we wschodniej Ukrainie. Dzięki ich wsparciu, Rosji udało się zdestabilizować ukraińskie siły bezpieczeństwa w regionie. Zablokowano możliwość funkcjonowania instytucji samorządowych, przejmowano składy amunicji oraz kontrolę nad miastami. Żołnierze prywatnych firm wojskowych przeprowadzali ataki z ukrycia, dokonywali rozpoznania, zbierali informacje wywiadowcze i towarzyszyli znaczącym lokalnie politykom prorosyjskim[214].

---

[210] Chociaż, jak ocenili M. Boulègue i A. Polyakova, Rosja nie może sobie pozwolić na zastosowanie tej strategii w skali globalnej, to w skali regionalnej silne skoncentrowane konwencjonalnej siły militarnej bywa skuteczne. M. Boulègue A. Polyakova, *The Evolution of Russian Hybrid Warfare*…

[211] Zob. *Private Military Consulting Company RSB-Group* (Russian Security Systems) https://rsb-group.org/about [dostęp: 28.09.2021].

[212] F. Bryjka, *Rosyjscy „kontraktorzy" w służbie Kremla*, Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2019/08/ROSYJSCY-%E2%80%9EKONTRAKTORZY%E2%80%9D-W-S%C5%81U%C5%BBBIE-KREMLA-Warsaw-Institute.pdf [dostęp: 9.06.2021] , s. 2, 14.

[213] Przeciwko założycielowi grupy Dmitrijowi „Wagnerowi" Utkinowi Służba Bezpieczeństwa Ukrainy planowała wnieść oskarżenie do biura Prokuratora Generalnego Ukrainy.

[214] F. Bryjka, Rosyjscy „kontraktorzy" w służbie Kremla…

Działania hybrydowe polegały także na osłabianiu ukraińskich struktur bezpieczeństwa przez intensywne działania wywiadowcze Moskwy. Ważnym czynnikiem, który umożliwił Rosji błyskawiczną aneksję Krymu była głęboka infiltracja ukraińskich sił zbrojnych i struktur politycznych. W takich arcytrudnych i groźnych uwarunkowaniach – jak przypomina Matthew Fisher powołując się na raport opracowany dla armii USA (*U.S. Army's Foreign Military Studies Office*) – pojawia się istotne ryzyko w zakresie współpracy sojuszników z Ukrainą. Wiąże się ono, bowiem z wysokim prawdopodobieństwem przenikania wrażliwych informacji do obozu wroga[215].

W czasie prezydentury Janukowycza (2010-2014) nastąpiła szczególnie intensywna penetracja ukraińskich sił bezpieczeństwa (zwłaszcza Służby Bezpieczeństwa Ukrainy) przez wywiad Federacji Rosyjskiej. Wojsko, przedstawiciele ministerstwa spraw wewnętrznych, jak i Służby Bezpieczeństwa Ukrainy (SBU), byli rekrutowani lokalnie na – w większości prorosyjskim – Krymie, co okazało się fatalną pomyłką. W czasie wydarzeń na Krymie tysiące funkcjonariuszy Służby Bezpieczeństwa Ukrainy, policjantów i wojskowych zbiegło przechodząc na stronę rosyjskich sił okupacyjnych. Dla przykładu, pierwszy zastępca głównodowodzącego ukraińską marynarką wojenną Sergei Yeliseyev urodził się w Rosji, ukończył sowiecką szkolę marynarki wojennej w Kaliningradzie i służył w rosyjskiej flocie pacyficznej. W czasie kryzysu krymskiego zbiegł on do Rosji, gdzie otrzymał stanowisko zastępcy dowódcy floty bałtyckiej Federacji Rosyjskiej. Nie był to odosobniony przypadek. Donbas stał się później kolejnym regionem, gdzie zaobserwowano to zjawisko na szerszą skalę[216].

Warte odnotowania spojrzenie na zagrożenia hybrydowe ze strony Rosji prezentuje badacz tej problematyki Mark Galeotti. Strona rosyjska, w jego ocenie, prowadzi działania z użyciem agresywnej narracji politycznej, gospodarczej ekspansji, szpiegostwa[217] i dezinformacji. Świadczy to zdaniem tego badacza o woli prowadzenia przez władze

[215] M. Fisher, *Russian infiltration of Ukrainian military complicates Canadian training mission*, National Post, Apr 14, 2015 https://nationalpost.com/news/world/russian-infiltration-of-ukrainian-military-complicates-canadian-training-mission [dostęp: 27.09.2021]

[216] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea*…

[217] Prawo międzynarodowe nie wyraża się jasno w kwestii szpiegostwa cyfrowego. Zob. *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

w Moskwie globalnej rywalizacji (mimo słabości nie pozwalającej na otwartą konfrontację militarną z Zachodem) [218].

Ponadto, charakterystyczną cechą działań rosyjskich o naturze hybrydowej jest celowe zacieranie granic między działaniami agend państwowych, formacji paramilitarnych oraz użycie wprowadzających przeciwnika w błąd działań maskujących (*dupe*)[219]. Administracja W. Putina od wielu lat uważa, że jest w stanie niewypowiedzianej wojny z krajami zachodnimi, dlatego stosuje wszystkie dostępne jej instrumenty walki (w rozumieniu i retoryce Kremla – samoobrony). Zaliczają się do nich, w ocenie M. Galeottiego, narzędzia wykorzystujące zasoby społeczne takie jak szerzące dezinformację farmy internetowych najemników (troli), patriotyczni hackerzy, banki transnarodowe, ochotnicy rekrutowani wśród Kozaków i przedstawicieli półświatka przestępczego[220]. W kontekście zagrożeń hybrydowych zwłaszcza te ostatnie kategorie można określić, jako bardzo zbliżone w działaniach dezorganizujących państwo do aktywności terrorystycznej[221].

Przykład ingerencji Rosji w sytuację na Ukrainie w 2014 r. pokazuje też wagę czynnika mniejszości etnicznych lub narodowych dla bezpieczeństwa na współczesnym polu walki. Państwo jednolite w kontekście narodowym ma w opisanym zakresie istotną przewagę[222].

Rosyjskie interwencje militarne (w Syrii, Wenezueli, Libii) wykorzystały istniejącą wcześniej na tych terenach korzystną dla Kremla sytuację (brak stabilizacji i skutecznego nadzoru państwa), której Rosja bezpośrednio nie spowodowała. Ponadto, wraz z rosnącą potęgą konwencjonalną Rosja stała się z czasem znacznie bardziej skłonna do wykorzystywania twardej siły w zakresie środków hybrydowych[223].

Ponadto, bardzo ważnym wymiarem zagrożeń hybrydowych jest – proceder znany od tysiącleci – manipulacja informacjami, która bywa określana, jako wirus. Jednak

---

[218] M. Galeotti, *Russia's Hybrid War as a Byproduct of a Hybrid State,* War on the Rocks, December 6, 2016, https://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/ [dostęp: 27.09.2021].

[219] T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa…*, s. 36.

[221] Tamże.

[222] Nie wdając się przy tym w dywagacje na temat słuszności takiej koncepcji czy tzw. politycznej poprawności. T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa…*, s. 37.

[223] Mathieu Boulègue Alina Polyakova, The Evolution of Russian Hybrid Warfare, 29 stycznia 2021 r. https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/

współcześnie, jak wskazują redaktorzy wydanego w Londynie opracowania poświęconego konfliktom hybrydowym i wojnie informacyjnej[224], trzymając się zaprezentowanego wcześniej porównania, wirus ten może rozprzestrzeniać się o wiele efektywniej niż w przeszłości. Jest tak dlatego, ponieważ popularne już nawet w ubogich społeczeństwach technologie informatyczne pozwalają na rozpowszechnianie dezinformacji znacznie szybciej i szerzej, niż miało to miejsce kiedykolwiek wcześniej. Można stwierdzić, że *wirus dezinformacji* uderza obecnie z większą siłą odziaływania na masy ludzkie niż dawniej. W tym właśnie aspekcie O. Fridman, V. Kabernik i J. C. Pearce postrzegają nowy wymiar zagrożeń hybrydowych, które objawiły się, jako jeden z owoców tzw. rewolucji informacyjnej. Jej przyspieszenie jest odnotowywane zwłaszcza od dwóch dekad (szczególnie, jeśli chodzi o dostęp mas społecznych do globalnej sieci internetowej). Fakt, że coraz więcej ludzi jest narażonych na dezinformację jest źródłem przewagi podmiotów państwowych i niepaństwowych chcących użyć tego instrumentu odziaływania. Wynika to z masowego wykorzystania zwłaszcza przez młodsze pokolenia m.in. mediów społecznościowych, internetu, jako głównych źródeł wiedzy, informacji, ale także inspiracji do działania oraz miejsca skąd czerpią autorytety.

Źródeł skuteczności działań hybrydowych Rosji, M. Galeotti upatruje w hybrydowej naturze tego państwa, które charakteryzuje się zatarciem granic między tym, co państwowe a tym, co prywatne (są one nieokreślone). Istotne znaczenie ma także brak skutecznych mechanizmów kontroli systemu politycznego przez naród, co odróżnia Rosję od demokracji państw zachodnich. Autorytarny, w swej pierwotnej naturze, model rządów w Rosji, w ocenie tego byłego specjalnego doradcy brytyjskiego *Foreign Office* oraz profesora na New York University, przypomina włoski system faszystowskich rządów B. Mussoliniego, który zawierał się w haśle: „wszystko w państwie, nic poza państwem, nic przeciwko państwu". Włochy za rządów Mussoliniego, co warto przypomnieć, wysłały „oddziały hybrydowe" na pomoc gen. Franco w czasie wojny domowej w Hiszpanii w latach 30 XX w. Te zastępy, określane przez Galeottiego jako „małe ludziki w czarnych koszulach" ("little blackshirt men"), początkowo walczyły bez żadnych insygniów występując formalnie jako ochotnicy[225].

[224] O. Fridman, V. Kabernik, J. C. Pearce (red.), *Hybrid Conflicts And Information Warfare. New Labels, Old Politics, Londyn 2019.*

[225] M. Galeotti, *Russia's Hybrid War...*

Warto zauważyć, że najpotężniejsze państwa na świecie, w sensie gospodarczym, militarnym i politycznym, cechuje wysoka spójność, stabilność i wieloletnia strategia kształtowania interesów narodowych. Przykładem są tu m.in. Niemcy, które były w stanie rozpocząć projekt Gazociągu Północnego przez socjaldemokratów Gerharda Schrödera i ukończyć go za rządów chrześcijańsko-demokratycznej CDU. Ponadto, zostało to dokonane w sytuacji silnego, publicznie wyrażanego sprzeciwu międzynarodowego w tym czołowych partnerów gospodarczych i wojskowych z UE i NATO – np. Polski. Różnice nawet pomiędzy ugrupowaniami politycznymi deklarującymi publicznie skrajnie odmienne światopoglądy w najsilniejszych demokracjach (typu kraje G7) nie stoją, więc generalnie na przeszkodzie w realizacji długoterminowych interesów tych państw o znaczeniu strategicznym.

W Rosji, jak kontynuuje dalej swój wywód M. Galeotti, instytucje państwowe są traktowane, jako łup polityczny i źródło finansowania rozmaitych projektów nie zawsze związanych ze statutową formą działalności danej instytucji. Stanowią przy tym często rodzaj „folwarku" osoby desygnowanej tam do pełnienia funkcji kierowniczej. Trudno nie zgodzić się z tym twierdzeniem, które jednak jest charakterystyczne nie tylko dla Rosji, ale także szeregu innych krajów, gdzie podobne praktyki bywają po prostu lepiej zakamuflowane. Także rosyjska Cerkiew Prawosławna jest postrzegana na zachodzie jako ramię Kremla[226].

Rosja wykorzystała działalność gospodarczą rozciągając wpływy w całej Europie. Kreml wypracował także jeden z najlepszych mechanizmów tzw. hybrydowego biznesu ("hybrid business") polegającego na tworzeniu legalnych i nielegalnych przedsiębiorstw handlowych, które generują środki finansowe, ale jednocześnie mogą zostać wykorzystane do celów zgodnych z interesem państwa. Rosyjskie instytucje prywatne stanowią zasłonę dla

[226] Biorąc to pod uwagę, jak wskazuje brytyjski badacz, Rosja Putina jawi się w tym ujęciu jako struktura wykorzystująca tzw. biurokratyczny pluralizm pozwalający władzom centralnym kierować państwem na zasadzie „dziel i rządz" Świadczy o tym np. zaangażowanie się krajowej Federalnej Służby Bezpieczeństwa (FSB) w aktywność zagraniczną wzmagając konkurencję w panteonie rosyjskich służb specjalnych. [226] Nawiasem mówiąc, abstrahując od moralnie wątpliwej idei i etyki działania, ich skuteczność w ochronie reżimu należy ocenić bardzo wysoko (ponad 20 letnie sprawowanie władzy przez wybranego w 2000 r. po raz pierwszy na prezydenta W. Putina i jego współpracowników).

Jako cywilna służba specjalna, FSB wywalczyła sobie początkowo monopol w zakresie walki informacyjnej, co nastąpiło miejsce po wojnie w Gruzji (na mocy dekretu prezydenckiego z 2013 r.). Od tego czasu monopol ten, jak ocenia M. Galeotti, został naruszony w wyniku domniemanego zaangażowania się wywiadu wojskowego w działania na terenie Ukrainy. Potwierdza to wspomniane wcześniej przyzwolenie władz do konkurowania ze sobą wpływowych agencji rządowych, aby móc je łatwiej nadzorować z poziomu politycznego. Zob. M. Galeotti, *Russia's Hybrid War…*

personelu wywiadowczego, szerzą dezinformację oraz są źródłem finansowania ruchów politycznych i społecznych korzystnych z punktu widzenia interesów Moskwy. Dla przykładu, M. Galeotti przytacza informację, iż przeciwny integracji europejskiej Front Narodowy Marine Le Pen we Francji otrzymał 9 mln euro pożyczki z banku kontrolowanego przez osobę uważaną za stronnika W. Putina. Kampanie polityka czeskiej partii komunistycznej / socjaldemokratycznej Miloša Zemana miały być z kolei wspierane datkami szefa lokalnego oddziału rosyjskiej firmy naftowej Lukoil (darowizny te były rzekomo prywatne)[227].

Nie tylko działania zbrojne na Krymie, ale także walki w Syrii, jak zaznacza M. Galeotti, były wspierane najemnikami, którzy zostali zidentyfikowani, jako – walczący anonimowo – rosyjscy żołnierze. Ponadto, jeśli jest taka potrzeba, do walki hybrydowej angażuje się nawet członków przestępczości zorganizowanej[228]. Mimo faktu, że działalność Rosji w tym zakresie jest znacząca na świecie, warto odnotować, że środki hybrydowe przyciągają zainteresowanie także innych rządów, np. Chin.

Różne sfery życia społecznego, które na Zachodzie są generalnie rozdzielone (państwowa, prywatna, wojskowa i cywilna) w uwarunkowaniach rosyjskich przenikają się w znacznie większym stopniu. Dodatkowym czynnikiem jest aktywność różnych agencji, które często konkurują ze sobą. Stwarza to wyzwanie w zakresie skoordynowania spójnej strategii względem danego celu. M. Galeotti przywołuje przykład ataku hakerskiego z 2016 r. na serwery biura krajowego amerykańskiej Partii Demokratycznej, w którym przenikały się działania FSB i rosyjskiego wywiadu wojskowego (GRU) – w pewnych zakresach wydające się sprzeczne ze sobą. Taka sytuacja może przy tym stanowić dodatkową trudność w jej właściwym rozpoznaniu i zneutralizowaniu dla służb odpowiedzialnych za przeciwdziałanie takiej aktywności[229].

Przyzwolenie na szeroki mandat działania służb specjalnych z wykorzystaniem infrastruktury cywilnej, kontrolowanego i sterowanego biznesu oraz określonych kręgów społeczeństwa (np. hakerzy patrioci) także może – w ocenie M. Galeottiego – stanowić zagrożenie dla bezpieczeństwa wewnętrznego Rosji[230].

[227] Tamże.
[228] Tamże.
[229] Tamże.
[230] Tamże.

Ważna jest także sfera przedsiębiorczości. Działalność biznesowa stwarzająca pozory inicjatywy prywatnej służąca rosyjskim interesom może być realizowana w szeregu europejskich krajach UE i NATO. Jest ona jednak często finansowana, jak zauważa M. Galeotti z budżetu federalnego Rosji. Oznacza to, jego zdaniem, kwintesencję prowadzonej przez Rosję, jak to określa "wojny totalnej" polegającej na „braku prawnych, etycznych czy praktycznych ograniczeń zdolności państwa to otwartego lub skrytego wykorzystywania (z pozoru niezależnych – przyp. autora) instytucji do swoich celów[231]."

Skuteczność działań hybrydowych jest uzależniona m.in. od stopnia rozpracowania wywiadowczego danego państwa przez agresora. Roger McDermott – powołując się na źródła rosyjskie – ostrzegał przed „penetracją ukraińskich służb specjalnych przez agencje wywiadowcze Federacji Rosyjskiej (FSB, SVR i GRU)[232]." Ponadto, nie chodzi w tym przypadku tylko o zagrożenie działaniami wrogich Ukrainie służb, ale o przychylność względem Moskwy osób zatrudnionych w wielu krytycznych obszarach ukraińskiej administracji. Można domniemywać, jak stwierdza R. McDermott, że w prawie każdej ważniejszej jednostce wojskowej są osoby sympatyzujące z polityką Kremla[233]. Przez dziesięciolecia Ukraina[234] (podobnie, jak Białoruś) była niemalże częścią radzieckich struktur państwowych, chociaż pozostawała jedną z trzech republik związkowych ZSRR (obok Rosji i Białorusi) posiadających prawo głosu w ONZ. Po Krymie, Donbas jest regionem na Ukrainie z największym odsetkiem osób uważających się za Rosjan (prawie 40% w 2001 r.)[235].

Przykład konfliktu krymskiego w 2014 r. pokazuje skuteczność operacji hybrydowej, która umożliwiła włączenie w granice Rosji części Ukrainy. Wykorzystana w tym przypadku

---

[231] Tamże.

[232] W eseju pt.: "Brothers Disunited: Russia's Use of Military Power in Ukraine. M. Fisher, *Russian infiltration of Ukrainian military complicates Canadian training mission*, National Post, Apr 14, 2015 https://nationalpost.com/news/world/russian-infiltration-of-ukrainian-military-complicates-canadian-training-mission [dostęp: 27.09.2021].

[233] M. Fisher, *Russian infiltration of Ukrainian military complicates Canadian training mission*, National Post, Apr 14, 2015 https://nationalpost.com/news/world/russian-infiltration-of-ukrainian-military-complicates-canadian-training-mission [dostęp: 27.09.2021].

[234] Termin „ukraina" oznaczał przez stulecia jedynie rodzaj pogranicza terenów, będących pod kontrolą różnych państw nie mając charakteru oficjalnego. Początki kształtowania się tożsamości narodowej i określenia „Ukraińcy" miały miejsce w drugiej połowie XIX w. Ukraina uzyskała niepodległość (od ZSRR) dopiero w 1991 r.

[235] I. Oldberg, *The Long War in Donbas: Causes and Consequences,* The Swedish Institute of International Affairs, 2020 https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-report-no.-1-2020.pdf [dostęp: 27.09.2021].

strategia hybrydowa okazała się efektywna. Mimo krytyki ze strony państw zachodnich – głównie UE i NATO – polityka faktów dokonanych z użyciem sprawnie przeprowadzonej operacji zbrojnej oraz przy umiejętnym wyeksponowaniu rzekomego społecznego poparcia (prorosyjskiej) ludności na spornym terenie pokazała, że skuteczność działań dyplomatycznych jest wypadkową realnej siły politycznej, organizacyjnej i wojskowej danego państwa oraz jakości i głębi jego relacji sojuszniczych[236].

W świetle wyników przeprowadzonych badań, aneksja Krymu, w świetle obecnej wiedzy, przedstawia się, jako misternie zaplanowane przedsięwzięcie oparte o dobre rozpoznanie słabych stron Ukrainy i precyzyjne plany ewentualnościowe (*contingency plans*). Kombinacja rewolucji demokratycznej w Kijowie (przez stronę rosyjską określanej mianem „puczu") oraz czasowa destabilizacja sytuacji politycznej na Ukrainie stanowiły dogodny moment do uruchomienia przez Moskwę przygotowanych wcześniej planów, zasobów i mechanizmów działania[237]. Aneksja Krymu dostarcza także wskazówek na temat możliwości przeciwdziałania zagrożeniom hybrydowym, które powinny uwzględniać aspekt antyterrorystyczny (zapobieżenie destabilizacji aparatu państwowego) oraz przeciwdziałania dezinformacji[238].

Od czasu aneksji Krymu i walk we wschodniej Ukrainie część ekspertów zachodnich zaczęła mówić nawet o konieczności akceptacji scenariusza nieuchronności tzw. "finlandizacji" Ukrainy. Jednakże, w ocenie części zachodnich ekspertów, Rosja nie jest zainteresowania neutralną Ukrainą, ale jej (ponownym) włączeniem do swojej strefy wpływów[239]. Działania hybrydowe mogą stanowić narzędzie osiągniecia tego celu. Moskwa nie tylko nie potrzebuje silnej demokracji u swoich granic, ale także państwa stanowiącego zagrożenie z uwagi na dawanie swoistego „złego" przykładu w regionie oraz wśród rosyjskiej klasy średniej, której poziom życia odbiega od krajów, takich jak Polska. Podobny

[236] Ukraina po zakończeniu Zimnej Wojny i uzyskaniu państwowości otrzymała gwarancje nienaruszalności terytorium (dobrowolnie pozbywając się atutu broni nuklearnej, która stacjonowała na jej terenie).

[237] T. Kuzio, P. D'Anieri, *Annexation and Hybrid Warfare in Crimea...*, https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/ [dostęp: 27.08.2021]

[238] Przykład sztucznie wygenerowanego kryzysu z udziałem imigrantów „na granicy polsko-białoruskiej w 2021 r. i instrumentalne wykorzystanie mediów pokazuje skalę zagrożenia w postaci tym razem demograficznej broni hybrydowej (stworzenie wrażenia niestabilności politycznej, ryzyko zainicjowania starć zbrojnych i włączenie się do nich państw trzecich)." T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa...*, s. 39.

[239] Tamże, s. 37.

scenariusz może być przewidziany także dla państw bałtyckich oraz – czego nie można wykluczać – dla Polski. Na Zachodzie nie docenia się w wystarczający sposób wagi zagrożenia, jakim – w perspektywie Kremla – jest wizerunkowy sukces międzynarodowego uniezależnienia się oraz rozwoju gospodarczego Polski – nie tak dawno – kluczowego państwa bloku radzieckiego i drugiej armii Układu Warszawskiego[240].

Abstrahując od zmian ekip rządzących na Kremlu, warto odnotować długookresową konsekwencję polityki zagranicznej Rosji, której przywódcy od lat 90-tych XX w. dążyli do dominowania w Eurazji. Traktowano to, jako swoiste prawo Rosji. Elity rosyjskie oczekiwały uznania zasadności tych dążeń przez USA i inne kraje zachodnie. W tym ujęciu negatywnie należy oceniać potencjalne konsekwencje wynikające ze zgody USA na rosyjsko-niemiecki Gazociąg Północny (Nord Stream) 1 i 2, który doprowadził do poszerzenia swobody działania Rosji w regionie. Odtąd nie musiała ona liczyć się, bowiem ze znaczeniem Ukrainy, jako kraju tranzytowego. Miało to znaczenie nie tylko dla bezpieczeństwa energetycznego, ale także dla bezpieczeństwa narodowego Ukrainy i regionu[241]. Konsekwencje tego groźnego geopolitycznie projektu, pozornie ubranego w szaty przedsięwzięcia *stricte* biznesowego, objawiły się w 2022 r. w postaci agresji rosyjskiej na Ukrainę[242]. Zdywersyfikowanie szlaków eksportu gazu przez Rosje za pomocą Nord Stream 2 z pewnością ułatwiło decyzję o ataku na Ukrainę (podwodny rurociąg został ukończony jesienią 2021 r., tj. niewiele ponad kwartał przed rozpoczęciem agresji Kremla na obszary ukraińskie).

---

[240] T. Kijewski, *Zagrożenia hybrydowe, a bezpieczeństwo państwa…*, s. 38.

[241] Tamże.

[242] Od początku działań rosyjskich, strona atakująca doświadczała rozmaitych przeszkód i utrudnień, które z pewnością wpłynęły na fiasko pierwotnych planów zdobycia Kijowa w ciągu kilku dni i zakończenia – jak to określano – specjalnej operacji wojskowej. Warto odnotować, że w maju 2022 r. pojawiły się informacje o mających miejsce niemal codziennie w różnych miejscach w Rosji pożarach składów z bronią i amunicją, fabryk, a nawet samochodów pracowników służb specjalnych. Incydenty zbiegły się w czasie z wyjątkowo poważnymi pożarami syberyjskich lasów (ich gaszenie było utrudnione ze względu na udział rosyjskich służb w wojnie).

W kontekście rosyjskiej agresji na Ukrainie i neutralnym stanowiskiem strony serbskiej, w maju 2022 r. władze w Belgradzie stanęły przed wyzwaniem rosnącej liczby alarmów bombowych. Na przestrzeni kilku dni serbskie instytucje otrzymały łącznie kilkaset zgłoszeń dotyczących podłożenia ładunków wybuchowych Zgłoszenia dotyczyły budynków użyteczności publicznej (szkół, szpitali, galerii handlowych). *AirSerbia*, która – obok linii tureckich – była jedyną europejską linią lotniczą obsługującą regularne połączenia z Rosją, otrzymała ponad 20 tego typu zgłoszeń. Na początkowym etapie spowodowały one konieczność anulowania rejsów do Rosji.

Zgłoszenia, w ocenie strony serbskiej, były częścią operacji hybrydowej prowadzonej przez państwa zachodnie, która miała na celu zmuszenie Serbii do przyłączenia się do antyrosyjskich sankcji. Zgłoszenia, jak podawały lokalne media, pochodziły z co najmniej kilku państw europejskich, w tym z Polski.

Podejście Federacji Rosyjskiej do działań niekonwencjonalnych jest warte analizy w kontekście wypracowania metod przeciwdziałania zagrożeniom hybrydowym. Militarne i niemilitarne metody prowadzenia wojny hybrydowej zostały zdefiniowane przez generała Walerija Gierasimowa, który w 2013 r. – na rok przed aneksją Krymu – prezentował publicznie rosnące znaczenie działań politycznych (dyplomatycznych), ideologicznych, gospodarczych i innych. Razem, jak trafnie zauważają Olga i Sergiusz Wasiuta, stanowią one oręż walki hybrydowej, który jest uzupełniany bezwzględnie elementem informacyjnym na wszystkich etapach (także po zakończeniu konfliktu). Wojna informacyjna była przy tym bezwzględnie obowiązującym elementem rosyjskiej agresji na Ukrainie w 2014 r. na każdym etapie konfliktu, a także po jego zakończeniu[243].

Do militarnych środków prowadzenia wojny hybrydowej, O. i S. Wasiuta zaliczają:

- selektywne użycie sił specjalnych (np. działań komandosów przebranych za lokalny element marginesu i świata przestępczego, separatystów, załogi konwojów humanitarnych itp.);
- konwencjonalne działania zbrojne z udziałem żołnierzy zawodowych, ale bez identyfikujących ich przynależność dystynkcji;
- nieregularne działania zbrojne (dywersja, bandytyzm, powstania, akty terrorystyczne, prowokowanie protestów i zamieszek ulicznych, sabotaż, partyzantka i grupy paramilitarne atakujące regularne siły zbrojne, zastraszanie lokalnej ludności, terroryzujące siły zbrojne zamachy na funkcjonariuszy i kadrę dowódczą);
- zorganizowanie zbrojnych oddziałów najemników i separatystów na terenie ukraińskim (jako siły samozwańczych republik Donieckiej i Ługańskiej);
- barbarzyńskie metody (celowe ostrzeliwanie dzielnic mieszkalnych, użycie cywilów jako tzw. *żywych tarcz*, organizowanie pozycji bojowych w szkołach i szpitalach czy innych gęsto zaludnionych lokacjach cywilnych) [244].

[243] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie*. Arkana – Kraków 2017, s. 142-149.

[244] Tamże.

Podział tych środków ma wymiar jedynie teoretyczny. Różne sposoby prowadzenia wojny, co słusznie zauważają O. i S. Wasiuta, w praktyce – w różnych konfiguracjach – zawsze są obecne łącznie na współczesnym polu bitwy.

Do kategorii niemilitarnych metod prowadzenia wojennych działań hybrydowych O. i S. Wasiuta zaliczają m.in.:

- propagandę bazującą na wykorzystaniu wszystkich dostępnych kanałów komunikacji i sposobów oddziaływania na świadomość własnych obywateli i otoczenia międzynarodowego (przedstawianie zadaniowanych przez siebie prowokatorów / agentów, jako ludność cywilną zasadnie żądającą sprawiedliwości, a organy ścigania – jako prześladowców);
- instrumenty polityczno-społeczne polegające na tworzeniu na terenie ukraińskim lojalnych grup dbających o podstawy dla sztucznej opozycji politycznej. Najczęściej są to skonfliktowane z resztą społeczeństwa mniejszości / wspólnoty terytorialne, narodowe, religijne lub polityczne, które niejako hoduje się zapewniając im finansowanie i wsparcie kierunkowe. Tworzenie takiej grupy jest długie i kosztowne, dlatego wykorzystuje się często, jako bazę – już istniejące – tlące się lub zamrożone konflikty;
- generowanie wewnętrznych konfliktów i napięć za pomocą agentów wpływu. Utworzenie nowych albo wsparcie istniejących, radykalnych organizacji siejących terror, który destabilizuje cały kraj lub jest wymierzony w konkretną grupę społeczną, ale może być także dobrą kartą przetargową (agresor, oficjalnie lub kanałami poufnymi, żąda wtedy ustępstw od władz państwa napadniętego w zamian za zaprzestanie działań hybrydowych tego typu);
- inspirowanie incydentów (często z użyciem przemocy) pozwala na wykorzystanie ich potem do medialnej walki propagandowej. W sposób sztuczny tworzy się w ten sposób alternatywną, korzystną dla agresora rzeczywistość osłabiając jednocześnie zdolności zaatakowanego kraju do skutecznej obrony przez dezintegrację tkanki społecznej i skierowanie debaty publicznej na fałszywe tory;
- narzędzia ideologiczne polegające na osłabianiu pozycji i wartości reprezentowanych przez kraj objęty atakiem hybrydowym. Wykorzystane do tego mogą być specjalnie przygotowane ideologiczne i psychologiczne kampanie informacyjne, lub

inspirowanie uderzeń punktowych wyprowadzanych przez dane jednostki: prorosyjskich dziennikarzy / ekspertów itp. Przedstawianie agresora, jako kraju znajdującego się na wyższym poziomie rozwoju cywilizacyjnego niż kraj-ofiara ataku (często fałszywe lub dokonane w sposób przesadny). Jednocześnie kształtuje się lub wzmacnia nastroje prorosyjskie poprzez idee wspólnoty braterstwa (tzw. ruski mir). W tym przypadku, chodzi o deprecjonowanie ukraińskiego dziedzictwa historycznego i wartości kulturowych oraz zaprzeczanie istnieniu oddzielnego narodu ukraińskiego;

- instrumenty gospodarcze w postaci sankcji, embarga, sabotażu łańcuchów dostaw, wprowadzanie cel zaporowych lub innych blokad swobody gospodarczej państwa atakowanego (a czasem także – jego stronników);
- środki nacisku energetycznego i surowcowego. Mimo, że jest to kategoria mieszcząca się częściowo w sferze gospodarczej, strategiczne znaczenie nośników energii przemawia za wydzieleniem tej grupy środków odziaływania hybrydowego. Narzędzia te mogą polegać na szantażu energetycznym – grożeniu odcięciem dostaw gazu ziemnego, ropy naftowej czy dostaw innych niezbędnych do funkcjonowania współczesnego państwa surowców. Wykorzystuje się tu także działania wspomagające takie jak ataki hakerów, których dokonano na ukraińskie sieci energetyczne czy akty terrorystyczne na system transportowy (np. incydenty na sieć gazową w obwodach iwano-frankowskim i połtawskim;
- aktywność służb specjalnych (obsadzenie agenturą urzędów centralnych i władz lokalnych, związków zawodowych, mediów oraz przedsiębiorstw prywatnych – zwłaszcza dużych zakładów produkcyjnych mających znaczenie w czasie wojny);
- wykorzystanie nowych technologii informacyjnych zaprzęganych do ataków na dany kraj, jak również pozwalających budować / chronić pozytywny wizerunek agresora w kontekście ocen własnych obywateli oraz tzw. opinii międzynarodowej (dezinformacja, propaganda);
- cyberataki: ofensywne działania typu hybrydowego prowadzone bezpośrednio przez służby specjalne agresora lub – pośrednio – przez powiązane z nim grupy zadaniowe złożone z wysoko opłacanych hakerów i tzw. trolli internetowych. Celem jest paraliżowanie i destabilizowanie państwa napadniętego;

- działania dyplomatyczne z wykorzystaniem wielu różnorodnych forów międzynarodowych (budowanie politycznego lobby w organizacjach międzynarodowych w celu zyskania ich przychylności w przypadku przeniesienia sporu na arenę międzynarodową – unikniecie lub złagodzenie sankcji);
- izolację międzynarodową – osłabianie międzynarodowej pozycji kraju zaatakowanego, który staje się międzynarodowym wyrzutkiem. Proces ten może trwać wiele lat lub nawet dekad, zanim przygotuje się podatny grunt pod siłową zmianę danego przywódcy lub ekipy rządzącej państwem obranym za cel ataku[245].

Granica dzieląca występowanie zagrożeń hybrydowych i wojny hybrydowej jest cienka i przykład konfliktu na Ukrainie w 2014 r. pokazuje jak łatwo sytuacja może się dynamicznie zmieniać. Ofensywna polityka Rosji skutkująca aneksją Krymu, wsparcie grup separatystycznych na Ukrainie i groźba eskalacji w postaci pełnowymiarowego użycia siły militarnej, w ocenie S.-D. Bachmanna, pozostawiły w 2014 r. Zachód i NATO praktycznie bezradne w zakresie skutecznej odpowiedzi. Niechęć NATO do wyrażenia zgody na bardziej zdecydowaną odpowiedź na działania hybrydowe Rosji wynikała częściowo z uzależnienia wielu członków tej organizacji od dostaw rosyjskiego gazu. Poza kwestiami bezpieczeństwa energetycznego, wpływ na to miały także ograniczenia prawne mające swe źródło w artykule 5 NATO, który zezwala jedynie na użycie zbiorowej samoobrony w przypadku ataku wyłącznie na państwo członkowskie tego sojuszu (Ukraina takim krajem nie była) [246].

Ponowna aneksja Krymu przez Rosję w 2014 r., jak stwierdza S.-D. Bachmann, stała się faktem dokonanym i jest mało prawdopodobne, aby – przy utrzymaniu się aktualnej polityki zagranicznej Rosji – stan ten został zrewidowany w przyszłości. Ponadto, Ukraina już jest jego zdaniem krajem podzielonym z walkami toczącymi się wzdłuż jego linii etnicznych, co bardzo przypomina casus byłej Jugosławii w latach 90-tych XX w. Początek konfliktu na Ukrainie w 2014 r. może być, więc zwiastunem tego, co nadejdzie. Perspektywa takiej hybrydowej wojny domowej, zdaniem S.-D. Bachmanna, dla Kremla usunęła w 2014 r. konieczność dokonania tam otwartej rosyjskiej interwencji wojskowej. Zamiast tego, Rosja zaczęła wojnę przez pośrednika (war by proxy) używając do tego celu tajnych agentów i/lub

[245] O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji...*

[246] S.-D. Bachmann, *Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security*, Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, s. 77 – 98.

najemników. Jednocześnie, w czasie narastającej eskalacji sytuacji w Donbasie, prezydent Putin zacieśnił relację strategiczną z Chinami, z którymi w maju 2014 r. zawarł umowę gazową. Rozwój tej współpracy gospodarczej w zakresie kluczowych dla bezpieczeństwa energetycznego dostaw gazu może, zdaniem S.-D. Bachmana, zakłócić kluczowe dostawy energii do Europy[247].

Scenariusz działań na Krymie, jak dowodzi M. Wojnowski, został następnie powtórzony – z mniejszą skutecznością – we wschodnich obwodach państwa ukraińskiego. Istotnym novum w zakresie tego etapu konfliktu było zastosowanie nowoczesnej techniki w sferze walki informacyjnej i w konwencjonalnych działaniach zbrojnych. W ocenie tego autora: „Inwazja zbrojna na Krym stanowiła (…) podsumowanie poprzedzających ją przedsięwzięć. Uwzględniając specyfikę rosyjskiej kultury strategicznej i myśli wojskowej (…) należy podkreślić, że główną uwagę przywiązuje się w Rosji do działań prowadzonych w czasie poprzedzającym interwencję zbrojną. Przybierają one charakter niemilitarny i są uzależnione od wielu indywidualnych czynników decydujących o stanie danego państwa lub regionu. Próbując przewidzieć rosyjską logikę działania, należy przede wszystkim zwrócić uwagę na niedoskonałości i słabości własnej organizacji państwowej, specyfikę kulturową i etniczną kraju, stan elit przywódczych zarówno w wymiarze zbiorowym, jak i indywidualnym oraz na kwestie dotyczące mniejszości narodowych, tak wewnątrz państwa, jak i poza jego granicami. Pogłębionej analizy wymagają wszelkiego rodzaju negatywne tendencje i procesy zachodzące w państwie oraz ich źródła[248].”

Badacz usiłuje też trafnie przeanalizować możliwości odpowiedzi ze strony Polski na zagrożenia hybrydowe, co stanowi poważne wyzwanie dla zdolności i zasobów państwa polskiego w starciu ze znacznie silniejszym przeciwnikiem takim jak Rosja: „(…) rosyjskie rozumienie przyczyn, przebiegu oraz skutków konfliktów ma charakter geopolityczny, czyli przestrzenny. Oznacza to, że według Rosjan działania są prowadzone w przestrzeni geograficznej, ekonomicznej, informacyjno-cybernetycznej oraz informacyjno-psychologicznej danego państwa. Z punktu widzenia bezpieczeństwa Polski konieczne jest zatem stworzenie doktryny bezpieczeństwa informacyjnego RP, uwzględniającej rosyjską specyfikę działań. Stanowiłaby ona punkt odniesienia dla działalności legislacyjnej,

[247] Tamże.
[248] M. Wojnowski, *Mit „wojny hybrydowej”…*

precyzyjnie definiując zagrożenia i ich skutki. Państwo polskie nie dysponuje potencjałem materialnym, technologicznymi finansowym, aby przygotować symetryczną odpowiedź na rosyjskie formy oddziaływania informacyjnego. Pewną próbą udzielenia takiej odpowiedzi może być jednak prowadzenie szerokiej akcji informacyjnej i edukacyjnej w społeczeństwie oraz pogłębianie specjalistycznych studiów nad rosyjską myślą wojskową, strategią i historią rosyjskiej wojskowości, bez zamykania się tylko i wyłącznie w kręgu zachodniej sztuki wojennej[249].”

Analiza aktywności Federacji Rosyjskiej na Ukrainie wskazuje, jak zauważa A. Rogozińska, że do arsenału niemilitarnych zagrożeń należały głownie:

– działania służb specjalnych (budowa struktur wywiadowczych, pozyskiwanie informacji, sabotaż);

– presja ekonomiczna (embarga lub zawyżone opłaty celne – także wobec krajów, które udzielają wsparcia państwu objętemu działaniami hybrydowymi);

– działania w cyberprzestrzeni (zakłócenie funkcjonowania administracji i infrastruktury krytycznej atakowanego państwa);

– narzędzia dyplomatyczne (dążenie do zdyskredytowania państwa atakowanego, lobbing w organizacjach międzynarodowych) [250].

Wśród katalogu działań hybrydowych, które były stosowane przeciwko Ukrainie, wyłania się bardzo szeroki wachlarz środków, metod i narządzi, m.in. następujące:

– monopol rosyjski na środki masowego przekazu na Ukrainie (i w innych krajach postradzieckich), co umożliwiło stworzenie zamkniętej przestrzeni informacyjnej (znaczenie tego środka bazującego na prasie, telewizji i radiu słabnie w miarę upowszechniania się internetowych źródeł informacyjnych (trend ten widać w konflikcie rosyjsko-ukraińskim z 2022 r.);

– mocny, stronniczy przekaz rosyjski, ukazujący Ukrainę, jako państwo upadłe i pozbawione perspektyw geopolitycznej egzystencji;

[249] Tamże.
[250] A. Rogozińska, *Niemilitarne zagrożenia dla Ukrainy…*

– podważanie legalności nowych władz ukraińskich, które doszły do władzy w wyniku Euromajdanu (po odsunięciu od rządów prorosyjskiego ośrodka władzy wokół prezydenta Wiktora Janukowycza);

– zmasowana dezinformacja w prasie, radiu, telewizji i w Internecie (m.in. przypadek tzw. doktora z Odessy – sfabrykowanego przez siły prorosyjskie profilu lekarza Igora Rozowskiego relacjonującego bestialstwo Ukraińców, rozpuszczanie fałszywych pogłosek, że flagowy okręt ukraińskiej marynarki wojennej „Hetman Sahajdaczny" przeszedł na stronę rosyjską);

– propagowanie w mediach zdjęć poległych (ukraińskich) żołnierzy, cywilów oraz zniszczonego sprzętu wojskowego w celu zastraszenia i zniechęcenia obywateli do podejmowania służby wojskowej;

– wyolbrzymianie w przekazie medialnym napięć politycznych w obozie rządzącym w Kijowie (podważenie zaufania do nowych władz);

– tworzenie prorosyjskiego lobby na Zachodzie bazującego na stosunku do kwestii energii (oparcie w partiach eurosceptycznych, teza: za wszelkie problemy związane z przesyłem gazu ziemnego w Europie jest odpowiedzialna Ukraina, która dodatkowo kradnie surowiec);

– utwierdzenie w świadomości Rosjan mitu o Władimirze Putinie jako jednoczycielu „rosyjskich terenów historycznych";

– podzielenie Unii Europejskiej przez obalenie przeświadczenia o jej udanym projekcie integracyjnym;

– wydarzenia rozgrywające się w Kijowie od października 2013 r. do lutego 2014 roku przedstawiane były w rosyjskich mediach jako bezprawny bunt przeciwko legalnej władzy, którego inicjatorem była „trzecia siła" z zewnątrz;

– ukazanie rzekomego zdemoralizowania władz cywilnych i militarnych na Krymie oraz przekonanie światowej opinii publicznej do narracji rosyjskiej;

– udział żołnierzy rosyjskich w działaniach zbrojnych na Ukrainie przeprowadzany był pod przykrywką tworzenia ochotniczych sił separatystycznych;

– koncentracja oddziałów wojska rosyjskiego przerzucanych na Ukrainę nosiła nazwę ćwiczeń w obwodach nadgranicznych. Opublikowano treści na setkach stron i licznych portalach społecznościowych o pozornie niezależnym, obiektywnym i informacyjnym charakterze, w rzeczywistości jednak powiązanych i skutecznie realizujących działania dezinformacyjne;

– metodą w zakresie dezinformacji okazała się także plotka, uwiarygodniona oficjalnymi wiadomościami przekazywanymi przez rosyjskich polityków i wojskowych. Założonym celem przekazywania i upowszechniania tego typu informacji było wytworzenie poczucia strachu, tak podczas mobilizacji armii ukraińskiej, przebiegającej w atmosferze chaosu i nieufności, jak i podczas prowadzenia właściwych działań militarnych. Przyjęte założenia okazały się skuteczne, czego dowodem był chociażby odwrót wojsk ukraińskich pod Debalcewe, a straty wówczas poniesione uznano za „wynik paniki, której źródłem były rosyjskie media bombardujące żołnierzy informacjami o pełnym okrążeniu, co przerodziło kontrolowany odwrót w bezwładną ucieczkę";

– propagowanie negatywnych stereotypów dotyczących społeczeństwa i elit władzy na Ukrainie, tj. powszechna korupcja, nacjonalizm w zachodnich obwodach Ukrainy, rozdźwięki pomiędzy obozem władzy prezydenta i premiera;

– wzmożoną kampanię informacyjną, mającą na celu uwypuklenie podziałów mających miejsce w Unii Europejskiej i NATO w zakresie zasadności pomocy dla Kijowa oraz sankcji nałożonych wobec Moskwy. Wykorzystywano do tego zarówno kontakty personalne z zachodnimi politykami, zachęty natury ekonomicznej, jak i oddziaływanie medialne;

– w przestrzeni informacyjnej prezentowano rosyjską narrację, której głównym celem pozostawało poróżnienie opinii publicznej. Podstawowym założeniem takiego działania było kształtowanie obrazu Rosji, jako ofiary cynicznej gry zachodniego *establishmentu*, oskarżanego przy tej okazji o kreowanie fałszywego obrazu prezydenta Rosji oraz przyczyn i przebiegu konfliktu ukraińskiego;

– pomimo, że zgromadzony potencjał militarny dawał gwarancję całkowitej swobody operacyjnej stronie rosyjskiej posługiwała się ona całym zespołem zakamuflowanych działań, jak chociażby wykorzystanie konwojów humanitarnych, jako jednego z elementów dozbrajania sił separatystycznych, co potwierdza zaobserwowana zbieżność pomiędzy rosyjskimi konwojami humanitarnymi a intensywnością prowadzonych działań zbrojnych przez oddziały separatystów;

– budowa pozytywnego obrazu Rosji, priorytetowego znaczenia tego państwa dla stabilności i bezpieczeństwa systemu międzynarodowego, ale także osłabianie solidarności państw członkowskich NATO oraz Unii Europejskiej, stworzenie w społeczeństwie rosyjskim subiektywnego odczucia osamotnienia i zagrożenia ze strony państw zachodnich. Do działań o tym charakterze zaangażowani zostali także rosyjscy dyplomaci oraz współpracujące z nimi podmioty, do zadań których należało promowanie interesów Federacji Rosyjskiej poza granicami kraju;

– Rosjanie dysponowali dokładną wiedzą z zakresu stanu osobowego jednostek wojsk ukraińskich, także delegatur i placówek Służby Bezpieczeństwa Ukrainy oraz ukraińskiej infrastruktury krytycznej. Ponadto, służby rosyjskie prowadziły rozległy wywiad psychologiczny polegający na pozyskiwaniu, przetwarzaniu i analizowaniu informacji dotyczących poszczególnych grup społecznych, służb mundurowych i administracji na Ukrainie[251].

Rosyjska agresja na Ukrainę w 2014 r. cechowała się więc nie tylko tradycyjnym (kinetycznym) charakterem. Stosowane były w niej także narzędzia walki hybrydowej takie jak wojna informacyjna, w tym zwłaszcza dezinformacja. W trakcie miesięcy a nawet lat poprzedzających aneksję Krymu strona rosyjska sukcesywnie informowała o rzekomym skrajnym nacjonalizmie i postawach pronazistowskich na Ukrainie oraz fałszowała obraz rzeczywistości w szeregu innych kwestiach.

Federacja Rosyjska, jak można było wywnioskować z oficjalnych wypowiedzi jej przedstawicieli, nie uznawała Ukrainy za w pełni niepodległe państwo, które ma prawo do

[251] Tamże.

prowadzenia swojej polityki zagranicznej. Było ono natomiast postrzegane i przedstawiane przez Federację Rosyjską, jako kraj upadły, podzielony i skorumpowany, który znajduje się pod wpływami różnych grup oligarchicznych oraz Zachodu. Poza-konstytucyjna zmiana władzy na Ukrainie w 2014 r. jest stale postrzegana w Rosji, jako jedna z tzw. „kolorowych rewolucji" (inspirowanych – według propagandy rosyjskiej – przez Anglosasów). W tej logice, strona rosyjska przedstawiała swoje zaangażowanie na Krymie, jako przejaw samoobrony w celu zabezpieczenia interesów mieszkających tam Rosjan[252]. Jest to bardzo ważna wskazówka dla innych krajów będących celem ataków dezinformacyjnych ze strony Rosji (a także innych krajów, jak Chiny). Przykłady takich działań poprzedzających aneksję Krymu i wojnę w Donbasie (a także późniejsza inwazja na Ukrainę w 2022 r.) jasno pokazują skalę niebezpieczeństwa z pozornie niegroźnymi działaniami w sferze informacji publicznej.

W 2014 r. Ukraina, której siły zbrojne przez dekady pozostawały częścią armii radzieckiej, stosowała metody walki charakterystyczne dla radzieckiej szkoły wojskowej. W tamtym czasie, rozpoczęta już modernizacja ukraińskich sił zbrojnych w kierunku modelu zbliżonego do zachodniego, nie była jeszcze zaawansowana. Ułatwiło to władzom w Moskwie zorganizowanie skutecznej operacji ataku (m.in. hybrydowego) i przejęcie Krymu. W 2022 r. Siły zbrojne Ukrainy walczyły już w znacznie większym stopniu używając technik wzorowanych na zachodnich, co osłabiło skuteczność ataków Rosji[253]. Na Ukrainie, w wyniku wojny polaryzującej to dychotomiczne społeczeństwo (ukraińsko- i rosyjskojęzyczne), wzmocniły się także postawy patriotyczne. W 2014 r. cześć ludności ukraińskiej próbowała zatrzymywać własne wojska zmierzające by wyzwolić określone tereny. W 2022 r. takich sytuacji nie odnotowano na większą skalę[254].

---

[252] I. Oldberg, *The Long War in Donbas: Causes and Consequences*, The Swedish Institute of International Affairs, 2020 https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2020/ui-report-no.-1-2020.pdf [dostęp: 27.09.2021].

[253] Warto jednak zauważyć, że ogromne zniszczenia infrastruktury koniecznej dla funkcjonowania społeczeństwa na Ukrainie mogą zostać wykorzystane do sprowokowania emigracji tamtejszej ludności na stałe (np. do Polski i innych krajów zachodnich) i de facto „oczyszczenia" tych terenów pod zagospodarowanie przez agresora.

[254] Mając na uwadze, rosyjską agresję na Ukrainę w 2022 r., jeśli chodzi o sytuację prawnomiędzynarodową, Rosja popełniała tam okrucieństwa (*atrocity crimes*), ale nie stanowią one ludobójstwa. Nie ma to znaczenia dla ludzi uwikłanych w ten brutalny konflikt, ale politycy powinni być świadomi różnicy i odpowiednio dostosowywać swoją reakcję oraz wypowiedzi w przestrzeni publicznej. Wśród taktyk stosowanych przez Rosję na Ukrainie przywołuje się użycie amunicji kasetowej, rzekome ataki na korytarze humanitarne i niszczenie szpitali. Czyny te stanowią zbrodnie wojenne i zbrodnie przeciwko ludzkości, a nie ludobójstwo. Prokurator Generalny Międzynarodowego Trybunału Karnego wszczął dochodzenie przeciwko Federacji Rosyjskiej, ponieważ istniały uzasadnione podstawy, aby sądzić, że popełniono rzekome zbrodnie wojenne, jak i zbrodnie przeciwko ludzkości (ale nie wymienił on

2.4. Wnioski

Kategoria zagrożeń hybrydowych obejmuje szerokie spektrum operacji militarnych i niemilitarnych. Praktycznie są to wszystkie działania poza otwartą, wypowiedzianą wojną. Mogą to być tak różne grupy zagrożeń, jak np. ataki cybernetyczne i dezinformacyjne, presja gospodarcza, izolacja na arenie międzynarodowej czy wręcz wykorzystanie sił specjalnych i grup dywersyjnych do prowadzania operacji zbrojnych[255].

Poddane badaniom w studiach przypadku dwa konflikty zbrojne ukazują szeroki zakres narzędzi hybrydowych, które zostały zastosowane w konfrontacji między stronami. Elementy hybrydowe były widoczne w czasie wojny w Syrii od 2011 r., gdzie stosowano walkę informacyjną skoordynowaną z działaniami kinetycznymi. Syria stanowiła także źródło cennej wiedzy oraz poligon doświadczalny dla zaangażowanych w ten konflikt stron, m.in. – Rosji.

Federacja Rosyjska dostarczała antyzachodnio nastawionym władzom w Damaszku broń, amunicję oraz wsparcie dowódcze, a także żołnierzy i najemników. Doprowadzono nawet do stworzenia tymczasowej zagranicznej bazy wojskowej, która umożliwiała Federacji Rosyjskiej aktywne wsparcie reżimu w Damaszku. Wśród działań hybrydowych było także improwizowane, niezgodne z pierwotnym przeznaczeniem użycie sprzętu wojskowego. Stosowano m.in. nieprecyzyjne rakiety typu SCUD powodujące straty wśród ludności cywilnej oraz wykorzystywano ludzi, jako tzw. żywe tarcze.

---

ludobójstwa). Zbrodnie wojenne oznaczają poważne naruszenia Konwencji Genewskiej i inne poważne naruszenia praw i zwyczajów międzynarodowych konfliktów zbrojnych (ataki na obiekty chronione, jak np. obiekty wpisane na światową listę dziedzictwa ludzkości lub inne obiekty historyczne). Zbrodnie przeciwko ludzkości to z kolei akt – taki jak morderstwo, gwałt i tortury – popełniony w ramach szeroko zakrojonego lub systematycznego ataku skierowanego przeciwko jakiejkolwiek ludności cywilnej. W przypadku zbrodni przeciwko ludzkości niekonieczne jest istnienie konfliktu zbrojnego, ale warunkiem jest popełnienie ich przeciwko ludności cywilnej w ramach zmasowanych akcji. Ludobójstwo różni się od innych zbrodni międzynarodowych, ponieważ obejmuje zamiar zniszczenia" grupy ludzi ze względu na ich narodowość, pochodzenie etniczne, rasę lub religię. Warto jednak zauważyć, że problemem przy ustalaniu zbrodni ludobójstwa jest udowodnienie zamiaru sprawcy, aby wyniszczyć konkretną chronioną grupę ludzi w całości lub części. Chociaż okrucieństwa na Ukrainie są szokujące, według stanu na sierpień 2022 r. nie ma dowodów na to, że celem Rosjan jest unicestwienie Ukraińców (brak dowodów na plan zniszczenia Ukraińców jako grupy; Ukraińcy w Rosji i poza nią nie są celem ataków).

[255] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych,* OSW, 24.4.2020, https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 10.07.2022].

Elementem strategii wojny hybrydowej w Syrii było zastosowanie przez władze w Moskwie również tzw. środków aktywnych, co polegało na udzielaniu wsparcia sprzyjającym Rosji ugrupowaniom społeczno-politycznym oaz dezinformacji. Strona rosyjska starała się przedstawiać, jako obrońca światowego dziedzictwa kulturowego organizując koncert w mieście Palmyra (po odbiciu tego miejsca z rąk Państwa Islamskiego). Ważnym wymiarem działań była aktywność dyplomatyczna ze strony rosyjskiej dla prezydenta Assada, co utrudniało nałożenie sankcji oraz napiętnowanie polityki władz w Damaszku w ramach organizacji międzynarodowych. Wszystkie te działania były realizowane przy wydatnym wsparciu służb specjalnych Federacji Rosyjskiej.

Zaangażowanie rosyjskie w wojnie w Syrii zostało wykorzystane do udoskonalenia technik walki hybrydowej, które Moskwa skutecznie zaaplikowała następnie podczas ataku na Ukrainę w 2014 r. Działania hybrydowe stanowiły wówczas podstawowy oręż, który umożliwił Rosji szybkie zajęcie i aneksję Półwyspu Krymskiego. Taktyką Federacji Rosyjskiej było zacieranie granic między działaniami rządowymi, najemników i separatystycznych formacji paramilitarnych oraz użycie środków maskujących. Charakterystyczną cechą wydarzeń na Krymie były wspólne działania rosyjskich sił konwencjonalnych oraz nieregularnych. Do aktywności hybrydowych zaliczało się wykorzystanie sił prywatnych firm militarnych, których operacje uzupełniały działania nieoznakowanych oddziałów rosyjskich. Ich ścisła kooperacja z siłami regularnymi była cenna dla rozpoznania wywiadowczego sił obrońców. Strona rosyjska wykorzystała m.in. siły nieregularne (tzw. zielone ludziki), wsparcie prorosyjskiej ludności lokalnej oraz wojnę informacyjną, której celem było przedstawienie aneksji, jako usprawiedliwionej koniecznością ochrony mieszkańców tych – jak tłumaczono – rdzennie rosyjskich terenów. Agresja hybrydowa ze strony Federacji Rosyjskiej polegała także na działaniach wywiadowczych biorących za cel ukraińskie siły bezpieczeństwa. Głęboka infiltracja ukraińskich sił zbrojnych i struktur politycznych w regionie niewątpliwie ułatwiła aneksję Krymu.

Istotny wymiar miała wojna informacyjna. Strona rosyjska wykorzystywała agresywną narrację polityczną, szpiegostwo i dezinformację. Przy braku skutecznych kampanii informacyjnych ze strony Ukrainy w 2014 r., głównym dostarczycielem informacji dla lokalnych społeczności stały się media prorosyjskie, które Zachód oskarżał

o dezinformację i szerzenie kremlowskiej propagandy. Wsparcie znacznej części mieszkańców Krymu dla działań władz w Moskwie przy bierności reszty oraz kolaboracja elit przywódczych, w tym czołowych wojskowych i przedstawicieli służb mundurowych, umożliwiła bezkrwawe przejęcie tego strategicznie ważnego terytorium. Szybkość z jaką się to stało osłabiła skuteczną reakcję zarówno rządu ukraińskiego, jak i działania piętnujące Rosję na arenie międzynarodowej. Jednak co ważniejsze, kraj – mimo postępującego zbliżenia z Zachodem – nie był wówczas jeszcze przygotowany na obronę przed przeciwnikiem tak silnym jak Rosja. Diametralnie inna sytuacja miała miejsce podczas inwazji rosyjskiej na Ukrainę w 2022 r. Wówczas władze w Kijowie otrzymały kluczowe wsparcie wywiadowcze, wojskowe i dyplomatyczne bez którego, jak wskazuje część ekspertów, stolica zostałaby zajęta w krótkim czasie przez Rosjan, co złamałoby opór reszty kraju.

3. Rozwiązania stosowane w zakresie przeciwdziałania zagrożeniom hybrydowym

Obecnie funkcjonujące rozwiązania w zakresie przeciwdziałania zagrożeniom hybrydowym są odpowiedzią na wyzwania, które ujawniły się w Europie i na świecie, szczególnie od czasu wojny na Ukrainie w 2014 r. Zarówno Polska, jak i pozostałe kraje NATO oraz UE podjęły działania mające na celu zniwelowanie ryzyka wynikającego z zagrożeń hybrydowych. Metody doskonalenia sposobów przeciwdziałania zagrożeniom hybrydowym są praktykowane także w krajach pozaeuropejskich, z których scharakteryzowano Australię i Nową Zelandię.

3.1. Rozwiązania prawne i instytucjonalne w Polsce ukierunkowane na przeciwdziałanie zagrożeniom hybrydowym

Przeciwdziałanie zagrożeniom hybrydowym z perspektywy Polski uwzględnia krajowe mechanizmy służące bezpieczeństwu narodowemu oraz regulacje wynikające z naszego członkostwa w organizacjach międzynarodowych (NATO, UE). Przeciwdziałanie zagrożeniom hybrydowym w Polsce znajduje się w kompetencji szeregu instytucji, służb i formacji. Jeśli chodzi o rozwiązania systemowe w zakresie przeciwdziałania zagrożeniom hybrydowym (w tym dezinformacji) w Polsce, funkcjonują wyspecjalizowane komórki w ramach administracji. Przeciwdziałaniem zagrożeniom hybrydowym zajmują się także inne instytucje takie, jak Biuro Bezpieczeństwa Narodowego, Krajowa Rada Radiofonii i Telewizji. Powstają nowe ośrodki takie jak Akademickie Centrum Komunikacji Strategicznej przy Akademii Sztuki Wojennej. Rządowy Zespół Zarządzania Kryzysowego ds. zagrożeń hybrydowych odbywa regularne spotkania kończące się rekomendacjami dla decydentów. Pod egidą Rządowego Centrum Bezpieczeństwa działa Zespół Bezpieczeństwa Przestrzeni Informacyjnej, Rządowy Zespół Zarządzania Kryzysowego ds. zagrożeń hybrydowych, służby mundurowe oraz inne dedykowane komórki w ramach administracji:

a) Ministerstwo Spraw Zagranicznych – Referat ds. komunikacji strategicznej (StratCom MSZ);

b) Ministerstwo Obrony Narodowej – Wydział Strategii Komunikacyjnej i Medialnej;

c) Naukowa i Akademicka Sieć Komputerowa – Dział Przeciwdziałania Dezinformacji[256].

Działania hybrydowe są opisane w zaktualizowanym w 2020 r. Krajowym Planie Zarządzania Kryzysowego i pokazują jak Polska definiuje ten problem. Określono je w tym dokumencie, jako działania zmierzające do osiągnięcia celów politycznych i strategicznych. Są to więc działania wymierzone w cele długoterminowe, które przewidziano do osiągnięcia na lata, a nawet dekady. Kolejnym elementem charakteryzującym zagrożeń hybrydowych jest ich wielowymiarowy, skryty charakter ukierunkowany na utrudnienia identyfikacji przeciwnika i przypisanie odpowiedzialności za nie sprawcy.

Działania hybrydowe prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, często rozłożone w dłuższym okresie czasu. W tym ujęciu do zagrożeń hybrydowych można zaliczyć wiec nie tylko działania typu cyberataki (krótkoterminowe), ale także użycie instrumentów informacyjnych (np. rozciągnięte na lata lub dziesięciolecia kampanie propagandowe i dezinformacyjne – w tym generujące chaos / szum informacyjny uniemożlwiający właściwą ocenę sytuacji przez państwo atakowane. Chodzi m.in. o próby wpływu na politykę historyczną, szkolnictwo, naukę, aby dokonać zmiany w świadomości społecznej. Działania hybrydowe charakteryzują się także tendencją do wywierania nacisku i uzależniania atakowanego podmiotu w różnych wymiarach (np. gospodarka).

W Polsce, zagrożeniami hybrydowymi zajmuje się m.in. Zespól Roboczy przy Rządowym Zespole Zarządzania Kryzysowego[257]. Zespół, zgodnie z art. 8 i 9 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, to organ opiniotwórczo – doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Przewodniczącym Zespołu jest premier, członkami ministrowie: Obrony Narodowej spraw wewnętrznych / administracji publicznej Spraw Zagranicznych.

[256] *Dezinformacja jako główna oś kampanii hybrydowych,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

[257] Jego zadania znajdują się w trakcie reorganizacji w związku z projektem ustawy o ochronie ludności oraz o stanie klęski żywiołowej z 2022 r.

Sekretarzem Rządowego Zespołu Zarządzania Kryzysowego jest Dyrektor Rządowego Centrum Bezpieczeństwa[258].

Natomiast utworzony przy Rządowym Zespole Zarządzania Kryzysowego w 2018 r. Zespól Roboczy został wyposażony w kompetencje dotyczące zagrożeń hybrydowych w następujących podkategoriach: bieżące monitorowanie, identyfikacja, analiza, przygotowanie propozycji reagowania na zagrożenia hybrydowe, koordynacja działań organizacji rządowych, instytucji państwowych i służb w tym zakresie. Przez bieżące monitorowanie należy rozumieć systematyczną wymianę i analizę informacji na temat wewnętrznych i zewnętrznych zagrożeń dla bezpieczeństwa i integralności terytorium RP oraz ocenę ryzyka wystąpienia sytuacji kryzysowych wskutek działań hybrydowych.

Funkcję szefa zespołu roboczego Rządowego Zespołu Zarządzania Kryzysowego pełni Dyrektor Rządowego Centrum Bezpieczeństwa, a członkowie zespołu to przedstawiciele administracji / ministerstw oraz służb mundurowych oraz eksperci (specjaliści od cyberbezpieczeństwa, systemów finansowych – referują sprawę zależnie od tematu). Sekretarz jest wyznaczony przez Dyrektora Rządowego Centrum Bezpieczeństwa, a miejsce pracy zespołu to siedziba Rządowego Centrum Bezpieczeństwa. W czasie względnie spokojnej sytuacji w otoczeniu Polski (czas „P") zespól działa w innym rytmie, niż podczas występowania zagrożeń charakterystycznych dla czasu wojny („W"), które zintensyfikowały się zwłaszcza od czasu kryzysu imigranckiego w 2021 r. i po ataku Rosji na Ukrainę w 2022 r. W tym ostatnim przypadku, rekomendacje Zespołu są wysyłane częściej. Praca Zespołu Roboczego jest orgaznizowana w postaci regularnych spotkań jego członków oraz zaproszonych gości-ekspertów o profilu zbieżnym z poruszaną problematyką. Przedstawiane są oceny sytuacji oraz omawiane scenariusze kierunku wydarzeń. Jeśli zaistnieje nagła potrzeba spotkanie może zostać zwołane w trybie pilnym.

W RCB, przy udziale zespołu hybrydowego, wydawane są poradniki mające na celu przygotowanie i rozwój świadomości na temat przeciwdziałania zagrożeniom hybrydowym (kolejna edycja została opracowana w 2022 r. – pt. „Bądź gotów").

Powstaje także biuletyn „DisInfo Radar", który identyfikuje i ujawnia fałszywe linie rosyjskich narracji wymierzone zwłaszcza w postrzeganie uchodźców ukraińskich. Są oni, w ocenie źródeł Federacji Rosyjskiej, obciążeniem dla budżetu (zapewnianie im bezpłatnie

[258] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

opieki medycznej, żywności, mieszkań i edukacji) i ich masowe sprowadzanie przez rząd w Warszawie doprowadzi do destabilizacji sytuacji w Polsce (ubóstwo, masowe protesty). Co więcej, w optyce rosyjskiej polski rząd przyjmuje uchodźców, aby przypodobać się USA, a pozostałe państwa UE nie zamierzają ani ich finansować ani sprowadzać do siebie w znaczących liczbach. Wreszcie, polityka Polski wobec Ukrainy nieuchronnie sprowadza zagrożenie dla bezpieczeństwa międzynarodowego i prowokuje wybuch wojny, jak utrzymuje promowana przez Federację Rosyjską narracja.

Skuteczną odpowiedzią na zagrożenia hybrydowe jest wzmocnienie odporności oraz budowa zdolności do wczesnego rozpoznania i szybkiego wdrożenia działań minimalizujących negatywne skutki. W tym celu niezbędne jest zrozumienie mechanizmów powstawania tego typu zagrożeń, monitorowanie działań i interesów inicjatora zagrożeń hybrydowych, aby w konsekwencji ocenić ryzyka wystąpienia tych zagrożeń.

Jeśli chodzi o metody przeciwdziałania zagrożeniom hybrydowym w Krajowym Planie Zarządzania Kryzysowego jego autorzy przypisali najważniejszą rolę podmiotom bezpieczeństwa narodowego, w tym podmiotom, które są „odpowiedzialne za kierowanie tym bezpieczeństwem, stanowiące potencjał obronny i ochronny państwa. Z tego względu ważne jest przygotowanie administracji publicznej, służb, inspekcji, straży oraz sił zbrojnych do reagowania na zagrożenia hybrydowe, także poprzez nadanie im odpowiednich kompetencji oraz zapewnienie sił i środków w przypadku niespodziewanej eskalacji kryzysu. Wojskowe środki używane przez przeciwnika w ramach działań hybrydowych mogą bowiem kamuflować przygotowania do faktycznego użycia sił zbrojnych (np. niezapowiedziane ćwiczenia militarne, którym towarzyszy duża koncentracja sił zbrojnych)[259].”

Skuteczną odpowiedzią na zagrożenia spowodowane działaniami hybrydowymi, według twórców KPZK, jest „wzmocnienie odporności oraz budowa zdolności do wczesnego rozpoznania i szybkiego wdrożenia działań minimalizujących negatywne skutki, również jako element odstraszania skierowany do inicjatora (agresora) tych działań. W tym celu niezbędne jest zrozumienie mechanizmów powstawania tego typu zagrożeń, monitorowanie działań i interesów inicjatora tego typu działań, aby w konsekwencji ocenić ryzyka wystąpienia tych zagrożeń w warunkach normalnego funkcjonowania państwa,

[259] *Krajowy Plan Zarządzania Kryzysowego,* Rządowe Centrum Bezpieczeństwa, 2022, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego [dostęp:21.10.2022].

szczególnie w obszarze gospodarczego bezpieczeństwa państwa, obronności i świadczenia usług dla ludności. Takie komplementarne podejście do budowy systemu reagowania na działania hybrydowe pozwoli na szybkie i efektywne reagowanie ogniw militarnych oraz pozamilitarnych w sytuacji wystąpienia tego typu zagrożeń. Działania hybrydowe charakteryzują się tym, że mogą występować w poszczególnych obszarach (…) lub w kilku równocześnie. Do przeprowadzenia skutecznych działań hybrydowych, muszą być zagwarantowane odpowiednie warunki dla powodzenia realizacji zakładanych celów. Dotychczasowe doświadczenia wskazują, iż obszar społeczny oraz ekonomiczny i informacyjny są najbardziej podatne na działania hybrydowe. Potencjalny przeciwnik, prowadząc działania w danym obszarze lub obszarach, wybiera najbardziej podatne a najmniej odporne obszary[260].”

Jedną z cech działań hybrydowych, co odnotowano w omawianym dokumencie planistycznym, jest „ich niska przewidywalność oraz możliwość utajnienia prawdziwych intencji przez potencjalnego przeciwnika zwłaszcza w fazie przygotowawczej. (…) Do realizacji działań hybrydowych potencjalny agresor będzie używać różnych dostępnych przez siebie narzędzi: zdarzeń o charakterze terrorystycznym, organizacji przestępczych, cyberataku, dezinformacji, nielegalnej migracji ludności, blokady i dyskryminacji gospodarczej, spekulacji finansowych, incydentów granicznych, niezapowiedzianych ćwiczeń przy granicy państwa, naruszeń granicy państwowej, nieporozumień na tle kulturowym i religijnym, wywoływanie napięć na tle narodowościowym, zakłóceń systemu zaopatrzenia, celowego zarażania chorobami zakaźnymi ludzi, jak np. wąglik i rozpowszechnienia chorób zwierząt jak np.: afrykański pomór świń, wysoce zjadliwa grypa ptaków (HPAI) u drobiu itp. Skutki zagrożenia zarówno dla ludności, gospodarki, mienia, infrastruktury czy środowiska naturalnego będą zależały od rodzaju i skali zdarzeń. W zawiązku z tym należy się liczyć z możliwością paraliżu systemów finansowych (w tym bankowych), telekomunikacyjnych, teleinformatycznych, opieki zdrowotnej, zaopatrzenia w energię, paliwa, żywność i wodę, zakłócania funkcjonowania struktur państwa, jego rozwoju gospodarczego, bezpieczeństwa przemysłowego w obszarach strategicznych gospodarki, dezinformacją, aż po bezpośrednie zagrożenie dla zdrowia i życia ludności oraz integralności terytorialnej. W skrajnym przypadku działania hybrydowe mogą doprowadzić

[260] Tamże.

również do wystąpienia kryzysu polityczno-militarnego i przyczynić się do utraty suwerenności[261].”

Co istotne, w dokumencie planistycznym trafnie zauważono, że „efektywne zapobieganie, przeciwdziałanie i reagowanie na zagrożenia hybrydowe wymaga podjęcia przez instytucje państwa odpowiednich działań, m.in. w zakresie przygotowania struktur i narzędzi służących wykrywaniu i identyfikowaniu działań hybrydowych oraz przygotowaniu do obrony przed nimi[262].”

Istotnym wymiarem przeciwdziałania zagrożeniom hybrydowym jest działalność organizacji pozarządowych i mediów (tzw. fakt-checkers), które zajmują się w sposób profesjonalny demaskowaniem fałszywych przekazów (m.in. InfoOps, Centrum Badań nad Współczesnym Środowiskiem Bezpieczeństwa – infowarfare.pl, Demagog, Konkret24, AntyFake, CyberDefence24). Wyzwaniem w zakresie przeciwdziałania zagrożeniom hybrydowym w Polsce pozostaje skuteczna koordynacja wysiłków w tym zakresie, zwłaszcza w odniesieniu do dezinformacji. W innych krajach taka struktura jest usytuowana przy kancelarii premiera. Stworzenie takiego ciała było jedną z rekomendacji zwartej w Strategii Bezpieczeństwa Narodowego RP[263].

Przeciwdziałaniem dezinformacji w ramach Ministerstwa Spraw Zagranicznych zajmuje się Referat ds. Komunikacji Strategicznej (StratCom MSZ). Ta funkcjonująca w ramach Biura Rzecznika Prasowego komórka wyłoniła się w 2019 r. z Departamentu Wschodniego Ministerstwa Spraw Zagranicznych, gdzie była pierwotnie zlokalizowana. Pokazuje to ukierunkowanie priorytetów w zakresie przeciwdziałania dezinformacji, które w Polsce koncentrują się w ostatnich latach na kierunku wschodnim. Komórka ta zajmuje się monitoringiem i analizą inforsfery, proaktyw1ną komunikacją, budowaniem odporności poprzez szkolenia i współpracą międzynarodową. Na podstawie informacji tzw. białego wywiadu (źródeł otwartych – OSINT), materiałów opracowanych przez Europejską Służbę Działań Zewnętrznych oraz z wykorzystaniem informacji z placówek, przygotowywany jest biuletyn DisInfo Snapshot informujący o incydentach i wydarzeniach mających konotacje z dezinformacją. Wspólnie z partnerami zagranicznymi tworzone są wspólne publikacje takie

[261] Tamże.
[262] Tamże.
[263] *Dezinformacja jako główna oś kampanii hybrydowych…*

jak raport z 2022 r. poświęcony fałszowaniu narracji w kontekście bezpieczeństwa energetycznego[264].

StratCom Ministerstwa Spraw Zagranicznych pełni też rolę punktu kontaktowego Rapid Alert System, który działa w unijnej służbie dyplomatycznej Europejskiej Służbie Działań Zewnętrznych. Z ramienia administracji rządowej komórka ta bierze udział w pracach legislacyjnych UE ws. dezinformacji. Ważnym zadaniem jest współpraca z platformami społecznościowymi i portalami informacyjnymi (rola koordynacyjna).

Współpraca międzynarodowa dotyczy przede wszystkim konsultacji dwu- i wielostronnych (ze stroną brytyjską oraz amerykańską – GEC / Departament Stanu USA, a także – kraje bałtyckie, Finlandia) posiada też plan przeciwdziałania dezinformacji z Wielką Brytanią.

Od listopada 2021 r. funkcjonuje też plan przeciwdziałania dezinformacji w ramach państw Trójkąta Lubelskiego (Litwy, Ukrainy i Polski), którego zadania zostały przeformułowane w kontekście wojny na Ukrainie w 2022 r.

Jednym z najważniejszych filarów działań jest mobilizowanie sektora prywatnego do ograniczania dezinformacji. Istotna jest tu współpraca z platformami społecznościowymi, które stały się sygnatariuszami Kodeksu Postępowania. Wagę tego wymiaru przeciwdziałania zagrożeniom hybrydowym pokazują dotyczące także Polski wydarzenia. Mimo nagłośnienia w 2021 r. znaczenia sprawy sztucznie wytworzonego hybrydowego zagrożenia imigranckiego na wschodniej granicy NATO / UE, podjęcie skutecznych działań wymagało czasu. Dla przykładu, FaceBook dopiero w lutym 2022 r. usunął internetowe grupy społecznościowe użytkowników z irackiego Kurdystanu, które były miejscem zachęcania potencjalnych imigrantów do udawania się na Białoruś (zrzeszały one aż ponad 400 tys. osób). Tak długi czas reakcji (prawie rok) od eskalacji kryzysu) pokazuje jakim wyzwaniem pozostaje przeciwdziałanie zagrożeniom hybrydowym w tym kontekście. Na mocy unijnego planu, utworzono też system wczesnego ostrzegania przed działaniami dezinformacyjnymi – Rapid Alert System[265].

Cyberbezpieczeństwo staje się jednym z ważnych wymiarów aktywności Polski, co znalazło wyraz w organizacji m.in. międzynarodowej konferencji w Łodzi (20-21.10.2022

[264] Tamże.
[265] Tamże.

r.) poświęconej temu aspektowi przeciwdziałania zagrożeniom hybrydowym (w ramach przewodnictwa Polski w OBWE). W jej trakcie dyskutowano o kwestii podnoszenia świadomości dot. cyberzagrożeń, potrzeby edukacji, budowania odporności społecznej i roli sektora prywatnego, a także o znaczeniu środków budowy zaufania.

22 października 2019 r. Rada Ministrów przyjęła uchwałę w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, która zakłada systematyczne wzmacnianie i rozwój krajowego systemu cyberbezpieczeństwa. Dokument zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Przyjęcie Strategii wynika z Ustawy o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r.

Cyberbezpieczeństwo to nie tylko domena wyspecjalizowanych agencji oraz służb mundurowych, ale także dyplomacji. Ministerstwo Spraw Zagranicznych bierze udział w kształtowaniu procesów cyfrowych na poziomie regionalnym (OBWE), także – w ograniczonym zakresie – w globalnym (ONZ). W ramach UE, Polska pełni kluczową rolę w procesach uruchamianych w ramach Cyber Diplomacy Toolbox, czyli zestawie narzędzi politycznie skoordynowanej reakcji UE na cyber ataki.

Po agresji Rosji na Ukrainę, jak wynika z wypowiedzi przedstawicieli polskiego resortu spraw zagranicznych na poświęconej cyberbezpieczeństwu katowickiej konferencji Cybersec, Polska wzmocniła możliwości identyfikowania oraz przeciwdziałania rosyjskim cyberatakom.

Do środków przeciwdziałania zagrożeniom hybrydowym w wymiarze zagrożeń cybernetycznych włączono także resorty spraw zagranicznych. Cyberdyplomacja, jako oddzielny nurt, wykształciła się po roku 2015. Od tego czasu postanowiono powierzać kwestie cyber dyplomatom, których zadaniem było zwalczanie tego wymiaru zagrożeń hybrydowych za pomocą instrumentów służby zagranicznej. Mimo faktu pozostawania sfery cyfrowej w domenie prywatnej, współczesne priorytety bezpieczeństwa narodowego wymagają nadzoru nad nią służb i instytucji państwowych, co jest już realizowane.

Istnieje potrzeba, aby rozszerzyć postrzeganie wyzwań w dziedzinie cybernetycznej, budując zasoby cyberdyplomacji. Ze względu na wysoki poziom łączności transgranicznej w cyberświecie pojawiła się potrzeba nowego podejścia do kwestii cyberbezpieczeństwa, która musi uwzględniać międzynarodowy wymiar tego zjawiska. Dlatego zamiast skupiać się wyłącznie

na cyberobronie czy cyberwojnie, ważne jest również rozwijanie cyberdyplomacji. Niewiele rządów uwzględnia dyplomatyczny wymiar cyberbezpieczeństwa w swoich działaniach, co nie pozwala im wypracować strategii dyplomatycznych współmiernych do cyberzagrożeń. Działania określane jako cyberdyplomacja, dyplomacja cyfrowa" i e-dyplomacja nabierają znaczenia, jako nowe formy dyplomacji publicznej, które mają na celu dotarcie do odbiorców spoza sfery rządowej[266].

Rozwój nowoczesnych technologii stwarza nowe wyzwania dla stosunków międzynarodowych, co dostrzega także polski resort dyplomacji. Pojęcie „cyberdyplomacji", jak podkreślił szef służby zagranicznej Ministerstwa Spraw Zagranicznych Arkady Rzegocki, jest odpowiedzią na wyzwania związane z cyberbezpieczeństwem i polityką cyfrową państw. Prekursorem „cyberdyplomacji" były Stany Zjednoczone, ale obecnie UE także prowadzi wiele działań w tym zakresie. Ponadto, termin „cyberdyplomacja" – w ocenie przedstawiciela Ministerstwa Spraw Zagranicznych – wskazuje także na wykorzystanie narzędzi cyfrowych do promowania państwa, jego wizerunku, polityki itd. W tym ujęciu dla Polski wyzwaniem jest stawienie czoła dezinformacji. Największym wrogiem, jak ocenił A. Rzegocki, jest ignorancja i brak wiedzy o kraju. Zwiększanie w skuteczny sposób wiedzy o Polsce radykalnie zmniejszy możliwości wprowadzenia w błąd odbiorców fake newsów[267].

Ważnym aspektem przeciwdziałania zagrożeniom hybrydowym jest ochrona infrastruktury krytycznej państwa, którą – zgodnie z ustawą o zarządzaniu kryzysowym (2007) – są „obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla funkcjonowania państwa i zapewnienia ciągłości dostarczania usług służących zaspokajaniu niezbędnych potrzeb ludności[268]." Zasadność jej ochrony jest warunkiem skutecznego przeciwdziałania zagrożeniom hybrydowym w przypadku zagrożeń w postaci na przykład ataku hybrydowego

[266] *Cybersecurity & Cyber Diplomacy*, European Security Defence College 2022.

[267] Gen. bryg. Karol Molenda: „Nasza praca to nie działanie pojedynczych samotnych wilków", Cyberdefence24, 03.09.2021 https://cyberdefence24.pl/armia-i-sluzby/gen-bryg-karol-molenda-nasza-praca-to-nie-dzialanie-pojedynczych-samotnych-wilkow [dostęp: 12/10.2022].

[268] Ustawa definiuje też europejską infrastrukturę krytyczną, do której zalicza „obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w zakresie systemów zaopatrzenia w energię elektryczną, ropę naftową i gaz ziemny oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie". *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (Dz.U.2020.0.1856) https://lexlege.pl/ustawa-o-zarzadzaniu-kryzysowym/ [dostęp: 18.11.2022].

z użyciem niezidentyfikowanych dronów lub rakiet na cele typu elektrownie czy stacje uzdatniania wody. Ważkość tej kwestii pokazuje przykład wojny na Ukrainie, gdzie celowemu niszczeniu poddawana jest infrastruktura kluczowa dla działania państwa i zabezpieczająca funkcjonowanie społeczeństwa. Zapewnianie ciągłości funkcjonowania infrastruktury krytycznej jest jednym z priorytetów państwa w sytuacji kryzysowej. Infrastruktura krytyczna obejmuje m.in.. systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności i sieci teleinformatycznych (cyberbezpieczeństwo), finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe oraz substancji chemicznych, promieniotwórczych i niebezpiecznych[269].

Warto odnotować, że w lipcu 2015 r. BBN poinformowało, o rozpoczęciu prac nad polską Doktryną bezpieczeństwa informacyjnego. Nastąpiło to rok po aneksji Krymu przez Rosję. Stwierdzono, że jest to istotne w związku z eskalacją zagrożeń hybrydowych, w tym o charakterze informacyjnym (propaganda, dezinformacja czy psychologiczne zastraszanie ze strony obcych państw i aktorów niepaństwowych np. organizacji terrorystycznych). Planowano, jak czytamy w projekcie, „stworzenie struktur wewnątrz Sił Zbrojnych RP i rozwój ich zdolności w zakresie przeciwdziałania zagrożeniom hybrydowym (np. Centrum Operacji Komunikacyjnych) (…); powołanie zespołów funkcyjnych odpowiedzialnych za bieżące monitorowanie i odpowiednio szybkie reagowanie wobec powstających zagrożeń informacyjnych; rozwijanie zdolności służb specjalnych do prowadzenia w ramach wojen hybrydowych działań o charakterze informacyjnym, zarówno o charakterze ofensywnym, jak i defensywnym[270].” Rekomendacje i oceny zawarte w Doktrynie, która miała mieć charakter dokumentu wykonawczego do Strategii Bezpieczeństwa Narodowego RP, powinny – w ocenie BBN – stać się podstawą do koordynacji działań państwa, sektora prywatnego i obywateli wobec zagrożeń informacyjnych.

3.2. Przeciwdziałanie zagrożeniom hybrydowym w UE i NATO

W odniesieniu do polityki NATO i UE w ramach przeciwdziałania zagrożeniom hybrydowym są one reakcją na wydarzenia międzynarodowe związane z tą sferą

[269] Tamże.

[270] Zob. *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*, BBN, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 28.11.2022].

bezpieczeństwa. Można tu wymienić m.in. wojnę z terroryzmem oraz tzw. Państwem Islamskim, atak cybernetyczny na Estonię (2007 r.), okupacja Półwyspu Krymskiego przez Rosję (od 2014 r.), eksplozję w składzie amunicji w Czechach (2014 r.), przerwanie dostaw prądu – atak cybernetyczny na infrastrukturę krytyczną na Ukrainie (2015 r.), ingerencja w wybory w USA (2016 r.), otrucie Siergieja Skripala (uznane prze z Zachód za przypadek użycia broni chemicznej), proliferacja zagrożeń hybrydowych związana z pandemią COVID (2019 r.), incydent Solarwinds (2020 r.) oraz instrumentalizacja migracji na wschodniej granicy NATO (2021 r.).

Kwestie bezpieczeństwa legły u podstaw kształtowania się UE. Po okresie wojen światowych było to celowe działanie wygaszające konflikty i minimalizujące ryzyko ich ponownego wybuchu. W tym zakresie nie Unia nie ma przewagi nad wrogami w postaci silnych, unitarnie zarządzanych państw, jak Rosja czy Chiny. Fundusze w krajach unijnych przez dekady były kierowane na sfery poza obronne. Pod wpływem wydarzeń w Europie, zwłaszcza aneksji Krymu w 2014 r., zmieniły się priorytety leżących w tej części świata państw. W odniesieniu do struktur unijnych, opracowano wytyczne w postaci Kompasu Strategicznego, który jest wyrazem dążenia i wzrostu świadomości konieczności podjęcia dodatkowego wysiłku w zakresie obrony społeczeństw europejskich.

UE kładzie coraz większy nacisk na zagrożenia hybrydowe, zwłaszcza od czasu zajęcia Krymu przez Rosję. Od 2014 r. Bruksela przyjęła ponad 20 różnego typu dokumentów odnoszących się do tego zagadnienia. Dotyczyły one, jak wskazał Piotr Szymański, m.in.: „zwalczania broni masowego rażenia, bezpieczeństwa dostaw energii, bezpieczeństwa morskiego, ochrony danych, ochrony unijnych granic, przestrzeni kosmicznej czy zagranicznych inwestycji bezpośrednich. UE ma także własny program ochrony infrastruktury krytycznej oparty na Dyrektywie ws. rozpoznania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (2008)[271]. Jednak w ostatnich latach największe znaczenie w budowaniu unijnej odporności na zagrożenia hybrydowe zyskało wzmacnianie świadomości sytuacyjnej i cyberbezpieczeństwa oraz walka z dezinformacją. Podobnie jak w przypadku mechanizmów natowskich opartych na art. 5 Traktatu Waszyngtońskiego, UE zdecydowała

[271] P. Szymański, *NATO i Unia Europejska wobec zagrożeń hybrydowych,* OSW, 24.4.2020 https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych [dostęp: 10.07.2022].

w 2019 r., że – w reakcji na poważne zagrożenie natury hybrydowej – jej członkowie mają możliwość aktywowania unijnej klauzuli solidarności (art. 222 Traktatu o funkcjonowaniu UE)[272].

Rozwój zdolności przeciwdziałania zagrożeniom hybrydowym w UE następował szczególnie intensywnie od 2016 r. i przyniósł efekty w postaci m.in. identyfikacji obszarów ryzyka w państwach członkowskich, utworzenia centrów eksperckich (HFC w ramach INTCEN, HCoE w Helsinkach), komunikacji strategicznej (STRACOM), a także wzmocnienie odporności infrastruktury krytycznej. Wprowadzone wówczas wytyczne unijne (w postaci wspólnych ram *Joint Framework on Countering Hybrid Threats – a European Union response)* były kamieniem milowym przeciwdziałania zagrożeniom hybrydowym w UE.

Podejście Unii do zagrożeń hybrydowych zostało następnie rozwinięte w komunikacie *Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* z 2018 r.[273] *Strategia bezpieczeństwa UE* z 2020, która zawierała mechanizmy usprawniające przeciwdziałanie zagrożeniom hybrydowym, została następnie uzupełniona Kompasem Strategicznym w 2022 r. Doprowadził on do stworzenia zestawu nowych instrumentów unijnych do przeciwdziałania zagrożeniom hybrydowym (m.in. EU hybrid toolbox, nacisk na rozwój technologiczny, przeciwdziałanie dezinformacji w sytuacjach kryzysowych – COVID). Cztery główne obszary przeciwdziałania zagrożeniom hybrydowym to w ocenie EUEAS to: świadomość sytuacyjna, odporność, odpowiedź oraz współpraca.

Ważne dla przeciwdziałania zagrożeniom hybrydowym jest rozwinięcie świadomości ich występowania w całym społeczeństwie, nie tylko w instytucjach i służbach odpowiedzialnych za bezpieczeństwo i obronę. Każdy przedstawiciel sektora państwowego oraz prywatnego powinien być świadomy zagrożeń hybrydowych i aktorów państwowych ora pozapaństwowych, którzy mogą stanowić zagrożenie.

Wiedza sytuacyjna jest zatem podstawą wszelkich działań wobec zagrożeń hybrydowych. Biorąc pod uwagę naturę tych zagrożeń są to w większości działania ukryte z uwzględnieniem elementów oszustwa. Dlatego kluczowe dla wypracowania skutecznych

[272] Tamże.

[273] J. Balcewicz, *Strategia bezpieczeństwa UE 2020-2025,* 21 sierpnia 2020 https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/ [dostęp: 6.10.2022].

metod odpowiedzi jest działalność Hybrid Fusion Cell, która mieści się w instytucji wywiadu cywilnego UE (INTCEN) i korzysta z zasobów uwzględniających materiały wywiadów wojskowych (SIAC – ang. *Single Intelligence Analysis Capacity*). Przygotowuje ona raporty ad hoc dotyczące sytuacji kryzysowych w zależności od zainteresowania państw członkowskich oraz raporty roczne prezentujące trendy w zakresie zagrożeń hybrydowych. Materiały te są przygotowywane w oparciu o informacje wywiadowcze przekazane przez państwa członkowskie UE (Unia nie posiada własnych zdolności wywiadowczych). Hybrid Fusion Cell dokonuje ich agregacji i tworzy regularne, niejawne raporty analizujące tendencje w obszarze zagrożeń hybrydowych (Hybrid Trends Analysis).

Następnym filarem budowania skutecznego systemu przeciwdziałania zagrożeniom hybrydowym jest odporność (ang. resilience), rozumiana jako zdolność do przeciwdziałania atakom, a jeśli się wydarzą – do odzyskania po nich siły instytucji państwowych i społeczeństwa. Odporność rozumiana w tym ujęciu to zdolność nie tylko do wytrzymania i radzenia sobie z wyzwaniami bezpieczeństwa, ale także do przejścia danej zmiany / okresu przejściowego w przewidywalny lub kontrolowany sposób. Strategia odstraszania potencjalnych agresorów także ma znaczenie dla budowania odporności. Chodzi o stworzenie takiej sytuacji, że agresor jest zmuszony inwestować coraz więcej w przygotowanie skutecznego ataku. Intencją obrońcy jest w tym przypadku uczynienie potencjalnego ataku tak trudnym do wykonania jak to możliwe (tzw. „odstraszanie przez odmowę" – ang. *deterrence by denial*). Do chwili obecnej te działania nie przynoszą wymiernych korzyści, ponieważ stale notowany jest wzrost zagrożeń hybrydowych. Jednak strategia ta jest ukierunkowana na długoterminową zmianę w tym zakresie i zniwelowanie zagrożeń hybrydowych w przyszłości. Przedstawiciele państw zachodnich mają jednak świadomość, że „odstraszanie przez karę" (ang. *deterrence by punishment*) również musi być rozważane, jako jedna z opcji obrony przed zagrożeniami hybrydowymi. Wytyczne UE pokrywają się z NATO-wskimi w tym zakresie, ale maja szerszy charakter[274].

Trzecim wymiarem unijnego przeciwdziałania zagrożeniom hybrydowym jest odpowiedź na zagrożenie (ang. response). Zaliczają się do tej kategorii m.in. środki przeciwdziałania zagrożeniom cybernetycznym (*cyber diplomacy toolbox*, bezpieczeństwo

[274] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

zdrowia publicznego i żywnościowe (inicjatywa HERA – *Health Emergency Preparedness and Response*), misje zagraniczne w ramach Wspólnej Polityki Bezpieczeństwa i Obrony (CSDP).

Narzędzia w ramach czwartego filaru dotyczącego współpracy obejmują wzmocnienie kooperacji z krajami partnerskimi, prowadzenie badań zagrożeń hybrydowych w sąsiedztwie Unii a także międzynarodową kolaborację w sprawach ataków cybernetycznych. Unia stara się wzmocnić zdolności obronne krajów partnerskich, co ma pomóc poprawić także poziom bezpieczeństwa UE. Kooperacja UE jest rozwijana m.in. z państwami grupy G7 i NATO[275].

W 2016 r. utworzono unijną Komórkę ds. Syntezy Informacji o Zagrożeniach Hybrydowych, którą ulokowano w strukturze Centrum Analiz Wywiadowczych UE. Powierzono jej gromadzenie i analizę danych o zagrożeniach hybrydowych na terytorium UE i w jej sąsiedztwie. Uzupełnieniem tej struktury jest powołane w 2017 r. Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych w Helsinkach. Jest ono otwarte dla państw UE, ale także NATO międzynarodową platformę ułatwiającą działalność badawczo-szkoleniową[276].

Potrzebę unijnych działań wspierających państwa członkowskie w walce z zagrożeniami hybrydowymi pokazały ataki cybernetyczne z 2017 r. Incydent określany jako WannaCry zakłócił działalność szeregu kluczowych instytucji i firm w Europie (m.in. niemieckich kolei, firmy Renault oraz służby zdrowia w Wielkiej Brytanii). Celem drugiego cyberataku (NotPetya) była Ukraina, ale straty poniósł też duński potentat transportowy Mærsk[277].

Od czasu przyjęcia w 2016 r. dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych, w UE zobligowano kraje członkowskie do wprowadzenia wspólnych standardów cyberbezpieczeństwa (obowiązek raportowania cyberincydentów w kluczowych sektorach, wprowadzenie narodowych strategii bezpieczeństwa cybernetycznego, zespoły reagowania na incydenty oraz wymiana informacji w europejskiej sieci CERT)[278].

[275] Tamże.
[276] P. Szymański, op. cit.
[277] Tamże.
[278] Tamże.

Aktywność regulacyjną UE uzupełniają działania obliczone na „odstraszanie" w cyberprzestrzeni i wzmocnienie wojskowych zdolności w zakresie cyberobrony. Rekomendowane rozwiązania uzupełniono w późniejszych latach o możliwość nakładania sankcji na autorów cyberataków (zakaz wjazdu na teren UE, zamrożenie aktywów)[279].

UE wspiera też działalność badawczą w obszarze cyberbezpieczeństwa, którą realizuje Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA). Z kolei, rozwój współpracy z sektorem prywatnym, powierzono Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO).[280]

Złośliwa aktywność cybernetyczna jest odnotowywana przez służby odpowiedzialne za bezpieczeństwo w państwach członkowskich UE. Bezpieczeństwo cybernetyczne jest współdzieloną odpowiedzialnością UE (ang. *shared responsibility*). Takie podejście wymaga budowania wzajemnego zaufania wśród państwach członkowskich. System cyberbezpieczeństwa UE ma trzy główne zadania: ochronę obywateli, zabezpieczenie instytucji UE, struktur oraz koordynowanie sieci współpracy i wspieranie unijnych programów. Szkolenia w zakresie przeciwdziałania cybernetycznym zagrożeniom hybrydowym są zapewniane m.in. przez unijne centrum, które przeprowadza treningi i kursy dla przedstawicieli państw członkowskich.

Do narzędzi cyberdyplomacji UE należą m.in. sankcje. Unia zwiększyła w ostatnich latach swoje zdolności do reagowania na zagrożenia w cyberprzestrzeni w ten sposób. 30 lipca 2020 r. UE po raz pierwszy w historii zastosowała środki mające na celu zwalczanie cyberataków, które zagrażają jej państwom członkowskim, państwom trzecim lub organizacjom międzynarodowym. Sankcje polegały na zakazie wjazdu na terytorium UE, zamrożeniu środków finansowych, a także zakazie udostępniania sprawcom funduszy przez osoby i podmioty z UE. Objęto nimi osoby oraz podmioty na terenie Rosji, Chin i KRLD, które były zaangażowane m.in. w ataki na polską Komisję Nadzoru Finansowego, sieć energetyczną na Ukrainie i w próbę ataku na Organizację ds. Zakazu Broni Chemicznej. Ukierunkowane na te osoby i podmioty sankcje, jak poinformowano, miały funkcję odstraszającą i zniechęcającą, ale nie oznaczały przypisania odpowiedzialności państwu trzeciemu[281].

[279] Tamże.

[280] Tamże.

[281] *Unia Europejska po raz pierwszy stosuje sankcje związane z cyberatakami*, Biuro Rzecznika Prasowego, Ministerstwo Spraw Zagranicznych, 31.07.2020 https://www.gov.pl/web/dyplomacja/unia-europejska-po-raz-pierwszy-stosuje-sankcje-zwiazane-z-cyberatakami [dostęp: 12.10.2022].

W kontekście przeciwdziałania kolejnemu wymiarowi zagrożeń hybrydowych – dezinformacji, w Europejskiej Służbie Działań Zewnętrznych powołano w 2015 r. grupę zadaniową East Stratcom. Eksperci ci, zorganizowani rok po aneksji Krymu przez Rosję, odpowiadają za upublicznianie przykładów sprzyjającej Rosji a wrogiej interesom UE dezinformacji. Do życia powołano także unijną sieć podmiotów weryfikujących fakty (*fact-checking*) oraz mechanizm wczesnego ostrzegania przed dezinformacją – Rapid Alert System (blokowanie działań dezinformacyjnych o dużej skali)[282].

Mając na uwadze przeciwdziałanie propagandzie i dezinformacji na obszarze UE, Parlament Europejski zachęcił kraje członkowskie do opracowania skoordynowanych mechanizmów strategii komunikacyjnej. W związku z tym, KE zarekomendowała wielowymiarowe podejście opierające się na szeregu współzależnych działań, które dotyczą m.in.:

a) wypracowania narzędzi umożliwiających użytkownikom i dziennikarzom radzenie sobie z dezinformacją;

b) promowania umiejętności weryfikowania informacji w celu przeciwdziałania dezinformacji (tzw. fact-checking – uzupełniony wsparciem dla użytkowników w poruszaniu się sprawnym w środowisku mediów cyfrowych);

c) zwiększenia transparentności wiadomości online (udostępnianie danych o systemach, które umożliwiają ich obieg w sieci);

d) ochrony różnorodności i trwałości europejskiego ekosystemu mediów informacyjnych oraz promowanie badań naukowych na temat wpływu dezinformacji w Europie[283].

Ważnym aspektem przeciwdziałania zagrożeniom hybrydowym jest budowa instytucji specjalizujących się w tym obszarze ryzyka. W 2016 r., dwa lata po aneksji Krymu, UE i NATO uznały przeciwdziałanie zagrożeniom hybrydowym za priorytetowy obszar pogłębiania współpracy. We wspólnej deklaracji opisane organizacje wskazały na konieczność powołania instytucji do spraw przeciwdziałania zagrożeniom hybrydowym oraz

[282] P. Szymański, op. cit.

[283] *European Commission. A Multi-Dimensional Approach to Disinformation. Report of the Independent High Level Group on Fake News and Online Disinformation*, Luxembourg 2018, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1 [dostęp: 23.11.2022].

zaapelowały do państw członkowskich o udzielenie wsparcia takiej inicjatywie. Oficjalnie Hybrid CoE powołano 11 kwietnia 2017 r. z chwilą podpisania przez 9 państw porozumienia (MoU). Centrum w Helsinkach to organizacja międzynarodowa utworzona na zasadach prawa fińskiego o autonomicznym statusie. Nie jest to agenda NATO ani UE, ale organizacje te są członkami Hybrid CoE. Odróżnia to tę instytucję od innych Centrów Doskonałości, które funkcjonują przeważnie w ramach NATO (m.in. centra do spraw: komunikacji strategicznej w Rydze, cyberbezpieczeństwa w Tallinie, energii w Wilnie)[284].

Centrum Hybrid CoE zostało zainicjowane przez 9 państw UE/NATO: USA, Wielką Brytanię, Francję, Niemcy, Litwę, Łotwę, Estonię, Finlandię i Polskę) i zainaugurowało działalność w październiku 2017 r. Łącznie, aktywne w ramach centrum jest ponad 30 państw uczestniczących i liczba ta rośnie. Roczny budżet centrum, które zatrudnia ok. 40 osób, wynosi ok. 3,6 miliona euro z czego połowę pokrywa państwo gospodarz – Finlandia, natomiast drugą połowę stanowią kontrybucje państw uczestniczących. Jako typowa organizacja siecio-centryczna Hybrid CoE zleca często opracowania podmiotom zewnętrznym. W radzie Zarządzającej Centrum, która spotyka się kilka razy w roku, każde państwo uczestniczące posiada swojego przedstawiciela (z ramienia Polski – Ministerstwo Spraw Zagranicznych). Skład zespołu Hybrid CoE, który tworzą nie tylko reprezentanci administracji rządowej, wojskowi, ale także naukowcy i eksperci zewnętrzni, odzwierciedla złożoność tematyki przeciwdziałania zagrożeniom hybrydowym.

Wśród kwestii znajdujących się w sferze zainteresowania centrum znajdują się takie wymiary przeciwdziałania zagrożeniom hybrydowym jak ochrona procesów demokratycznych i wyborów (wzmocnienie zdolności państw do monitorowania, wykrywania i odpowiedź na obcą ingerencję), odstraszanie (ćwiczenia, studia przypadków współpracy UE-NATO), budowa odporności administracji sektora prywatnego i społeczeństwa obywatelskiego, kwestie instrumentalizacji migracji (interpretacja praw człowieka jest wykorzystywana przez agresorów i uniemożliwia Europie skuteczną ochronę granic) oraz analizy (regionalne, porównawcze adwersarzy). Głównym obiektem badań Centrum są wielowymiarowe zagrożenia hybrydowe ze strony Rosji i Chin[285].

[284] *What is Hybrid CoE?,* The European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland, 2022 https://www.hybridcoe.fi/who-what-and-how/ [dostęp: 25.10.2022].

[285] Tamże.

Sieciocentryczność w przypadku Hybrid CoE[286] oznacza, łączenie różnych danych w jeden system. Jest budowana baza danych. Organizując warsztaty, zajęcia i ćwiczenia zaprasza się ekspertów, którzy tworzą sieć kontaktów służących wsparciem w przeciwdziałaniu zróżnicowanym zagrożeniom hybrydowym. Hybrid CoE nie może wspierać bezpośrednio krajów spoza organizacji, ale pośrednio może służyć takimi działaniami (np. wspierając USA realizujące projekty wsparcia Ukrainie). Z podobnych centrów funkcjonujących poza UE i NATO działa ono w Singapurze.

Hybrid CoE we współpracy z Komisją Europejską (JRC) opracowało model koncepcyjny zagrożeń hybrydowych (ang. *The Landscape of Hybrid Threats*). W tym modelu koncepcyjnym znajduje się opis domen, narzędzi, celów oraz faz działania w kampanii hybrydowej. Aktorzy podejmujący działania hybrydowe (państwowi i niepaństwowi) wykorzystują różnorodne narzędzia w celu wpływania na procesy w określonych domenach. Model koncepcyjny zawiera 13 takich domen (m.in. infrastruktura, gospodarka kultura, wywiad, dyplomacja, informacja). W modelu tym należy analizować zagrożenia w danej domenie w łączności z ich możliwym wpływem na stan bezpieczeństwa państwa w pozostałych domenach. Agresor ma zwykle możliwość swobodnej zmiany rodzaju działalności eskalując sytuację (od uzyskania wpływu aż do hybrydowych działań wojennych z dominującymi aktywnościami kinetycznymi). Wszystkie te działania mają wpływ na proces decyzyjny atakowanego podmiotu, czyli zwykle współczesnego państwa[287]. Sytuacja na Ukrainie, która ewoluuje szczególnie szybko od 2014 r., według modelu koncepcyjnego Hybrid CoE jest oceniana jako wojna hybrydowa, gdzie przeważają działania kinetyczne.

Do najważniejszych działań UE wobec zagrożeń hybrydowych należała odpowiedź na aktywność dezinformacyjną Rosji po zajęciu Krymu w 2014 r. W czasie wydarzeń poprzedzających aneksję Krymu, władze rosyjskie utrzymywały, że nie są zaangażowane, a inicjatorem działań separatystycznych jest ludność lokalna chcąca przyłączenia do Rosji. W odpowiedzi na rozwój wypadków, w Unii został powołany Wydział Komunikacji Strategicznej, a w jego ramach grupa zadaniowa do zwalczania dezinformacji (East Stratcom Task Force), której kierownictwo powierzono w 2021 r. Polce Martynie Bildziukiewicz. Pod

[286] Centrum ds. cyber-zagrożeń w Estonii wnika bardzo głęboko w kwestie techniczne natomiast Hybrid CoE analizuje bada wpływ i współzależności domen.

[287] *What is Hybrid CoE?...*

jej nadzorem realizowany jest m.in. projekt EUvsDisinfo (https://twitter.com/EUvsDisinfo), który ma na celu przeciwdziałanie dezinformacji w mediach społecznościowych. Strona EUvsDisinfo na Twitterze dociera z przekazem do ponad 70 tys. odbiorców, w tym wielu decydentów i polityków państw europejskich.

W 2016 r. UE wypracowała pierwsze całościowe podejście do zagrożeń hybrydowych, które zawierało 20 różnych aktywności. Zostały one wprowadzone w życie. Do najbardziej znaczących można zaliczyć utworzenie Hybrid Fusion Cell – komórki zajmującej się analizą informacji o zagrożeniach hybrydowych. Miało także miejsce wydanie podręcznika o zagrożeniach hybrydowych (Hybrid Playbook), który jest protokołem operacyjnym dla instytucji UE, który określa rolę poszczególnych agend i jednostek organizacyjnych w zakresie przeciwdziałania zagrożeniom hybrydowym (zagrożenia hybrydowe są w nim potraktowane, jako element zarządzania kryzysowego). Badanie zagrożeń hybrydowych (Hybrid Risk Surwey) to z kolei przegląd sytuacji na terenie poszczególnych krajów UE, aby stwierdzić na ile są one przygotowane do radzenia sobie z zagrożeniami hybrydowymi. W Polsce odbyło się to już dwukrotnie (ostatnio w 2021 r.) i zaangażowanych było w opracowanie takiego raportu kilkanaście urzędów centralnych.

W 2018 r. KE przyjęła Plan działań przeciwko dezinformacji (Action Plan Against Disinformation), przed którym postawiono zadania w czterech głównych obszarach:

- filar I: poprawa wykrywania, analizowania i ujawniania dezinformacji (East StratCom Task Force, Western Balkans Task Force, Task Force South, EU Hybrid Fusion Cell);
- filar II: ściślejsza współpraca i wspólna reakcja na dezinformację (Rapid Alert System, tj. system wczesnego ostrzegania ws. działań dezinformacyjnych);
- filar III: mobilizowanie sektora prywatnego (kooperacja z platformami społecznościowymi – sygnatariuszami Kodeksu Postępowania);
- filar IV: zwiększanie odporności społecznej (Europejskie Obserwatorium Mediów Cyfrowych)[288].

[288] *Dezinformacja jako główna oś kampanii hybrydowych,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

Państwa członkowskie kierują pracami UE w obszarze zagrożeń hybrydowych na poziomie roboczym w ramach działającej od 2019 r. horyzontalnej grupy roboczej ds. wzmacniania odporności i przeciwdziałania zagrożeniom hybrydowym (HWP ERCHT – Finlandia). Wyłoniła się ona z funkcjonującej w 2017 r. grupy przyjaciół prezydencji estońskiej ds. Zagrożeń Hybrydowych, co pokazuje mechanizm formowania się takich celowych forów w UE. W tym przypadku zainteresowanie przeciwdziałania zagrożeniom hybrydowym wykazywały państwa członkowskie wschodniej flanki będące w sytuacji zagrożenia ze strony Rosji, które reaktywowało się od aneksji Krymu w 2014 r. W ramach Rady UE pracami HWP kieruje prezydencja.

Wyrazem woli politycznej państw UE w obszarze zagrożeń hybrydowych są konkluzje Rady UE, których w latach 2015-21 było kilkanaście. W konkluzjach z lat 2019 i 2020, uzgodniona przez ministrów spraw zagranicznych treść konkluzji kładła nacisk na konieczność budowania świadomości sytuacyjnej i wzmocnienia odporności, ale także rozpoczęto coraz bardziej akcentowanie potrzeby aktywnego reagowania na ataki hybrydowe (np. podnoszenie kosztów działań agresora).

Wypracowanych zostało także szereg innych narzędzi unijnych służących przeciwdziałaniu zagrożeniom hybrydowym w tym dezinformacji. Chodzi o dobrowolny kodeks postepowania dla platform internetowych, do którego przystąpiły Facebook, Google, Twitter, Microsoft, Mozilla i TokTok. Wprowadzono plan działań przeciwko dezinformacji, który przyczynił się m.in. do utworzenia mechanizmu szybkiego reagowania pozwalającego na koordynację działań państw członkowskich (Rapid Alert System). Nowa strategii bezpieczeństwa UE (wewnętrznego) z 2020 r. uwzględniła zagrożenia hybrydowe na wszystkich etapach działań oraz w unijnej legislacji.

Unijny system prawny w zakresie cyberbezpieczeństwa tworzy Strategia bezpieczeństwa UE, Strategia Cyberbezpieczeństwa z 2013 r. oraz szereg innych regulacji prawnych (Dyrektywa o cyberbezpieczeństwie NIS z 2016 r., rozporządzenie o cyberbezpieczeństwie z 2019 r., Budapeszteńska Konwencja o Cyberprzestępczości, ramy polityki UE w zakresie cyberobrony, konkluzje z 2015 r. w sprawie cyberdyplomacji oraz wspólny komunikat z 2017 r. w sprawie odporności, odstraszania i obrony).

W odniesieniu do zagrożeń sfery cyber w UE stworzono narzędzie określane jako cyber toolbox. Zaliczają się do niego różne metody działania Unii takie jak dialog, demarche

(apel do konkretnego państwa, które podejrzewamy o wrogie działania), a nawet zbiorowe działania mające cechy samoobrony. Cyber Diplomacy Toolbox to także mechanizm reagowania na cybernetyczne zagrożenia hybrydowe bazujący na koordynacji decyzji i uzgodnienia reżimu sankcyjnego. Po raz pierwszy wprowadził on tzw. cybersankcje, które można zastosować na skutek zagrożeń hybrydowych (zostały one już zastosowane).

Dostawcy usług bezpieczeństwa, z uwagi na ich kluczowe znaczenie w zakresie zapewniania bezpieczeństwa, powinni być wybierani spośród firm unijnych. Może to być niemożliwe jednak w odniesieniu do wszystkich zakresów usług. W takich przypadkach UE powinna wprowadzić programy stymulujące rozwój zdolności unijnych przedsiębiorstw w tej domenie. Istotne są też szkolenia przedstawicieli sektora prywatnego z naciskiem na biznes, ale konieczne jest tu wyważenie zaangażowania i obciążania tym obowiązkiem firm. Organizacje mające na celu przeciwdziałanie zagrożeniom hybrydowym nie mogą pozostawać w bezruchu, być statyczne stosując stale te same metody działania, kontroli i zabezpieczeń. Niezbędne jest zachowanie czujności na trendy i nowe luki, które muszą podlegać ciągłemu zabezpieczaniu[289].

W celu skutecznego przeciwdziałania zagrożeniom hybrydowym utworzono inicjatywę EU-HYBNET[290], która ma na celu wyjście z działaniami poza sektor rządowy stosując zasadę kompleksowego angażowania różnych części społeczeństwa (ang. *whole of socjety*). Tworzone są sieci instytucji / organizacji zajmujących się problematyką zagrożeń hybrydowych oraz promowane kontakty między praktykami a środowiskiem nauki i biznesu. Projekt jest ukierunkowany także na poszukiwanie nowych rozwiązań, w tym technologicznych, wspierających przeciwdziałanie zagrożeniom hybrydowym. EU-HYBNET składa się z partnerów z kilkunastu państw członkowskich UE i krajów stowarzyszonych, w tym Niemiec, Francji, Estonii, Finlandii, Norwegii, Włoch i Polski. Pozostali uczestnicy inicjatywy reprezentują przemysł, małe i średnie przedsiębiorstwa, środowiska akademickie i inne organizacje. EU-HYBNET Zakłada on współpracę z sektorem akademickim, pozarządowym oraz prywatnym w zakresie propagowania wiedzy o zagrożeniach hybrydowych.

[289] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

[290] EU-HYBNET 2022 https://euhybnet.eu/about/partners/ [dostęp: 2.09.2022].

W ramach działań na rzecz przeciwdziałania zagrożeniom hybrydowym w UE stale rozwijane jest prawodawstwo. W przygotowaniu jest szereg inicjatyw legislacyjnych, z których warto wymienić m.in. wzmocnienie unijnego Kodeksu postepowania w zakresie zwalczania dezinformacji. Jest on przewidziany dla największych platform internetowych tak, aby skutecznie skłaniać je do podejmowania szybszych działań w obliczu dużej dynamiki pojawiania się dezinformacji w ich zasobach. Duże znaczenie może mieć także projekt unijnego prawa w sprawie jednolitego rynku usług cyfrowych (ang. *Digital Services Act*), które – jako rozporządzenie – będzie stosowane bezpośrednio dlatego może mieć istotne znaczenie dla kształtowania bezpiecznej przestrzeni informacyjnej i cyfrowej. Ochrona wyborów do Parlamentu Europejskiego (najbliższe w 2024 r.) jest z kolei istotą implementacji Europejskiego planu działania na rzecz demokracji. Przewidziano w nim m.in. jawność reklamy politycznej. Ważne są też dwa projekty dyrektyw w sprawie ochrony infrastruktury krytycznej, które mają szansę na finalizację i wdrożenie do polskiego porządku prawnego w nadchodzących latach. Chodzi w nich o poszerzenie zakresu ochrony tej infrastruktury na zasadzie objęcia ochroną całych sieci infrastrukturalnych (ich funkcjonowania, usług, dostaw), a nie tylko obiektów infrastruktury krytycznej.

Warto też odnotować projekt Rozporządzenia w sprawie przeciwdziałania przymusowi gospodarczemu, który został zaproponowany jako reakcja na wymierzone w Litwę wrogie działania hybrydowe ze strony Chin. Pekin represjami gospodarczymi starał się wymusić decyzje polityczne w postaci korekty litewskiej polityki zagranicznej tak, aby ponownie przychylnie traktowała ona pogłębianie chińskiego zaangażowania w Europie.

Inicjatywa EU Hybrid Toolbox ma na celu koordynację i uproszczenie nie mechanizmu decyzyjnego i instrumentów reagowania na zagrożenia hybrydowe. W kontekście prac nad Kompasem Strategicznym, Polska przystąpiła w 2021 r. do dokumentu w sprawie utworzenia tego rozwiązania (typu *non-paper*). EU Hybrid Toolbox został ostatecznie wpisany do przejętego w 2022 r. Kompasu Strategicznego UE – dokumentu zawierającego kierunki działań Unii w obszarze bezpieczeństwa międzynarodowego. Ma on obejmować zarówno już istniejące, jak i nowe narzędzia w ramach skoordynowanej odpowiedzi na kampanie hybrydowe. Zaliczyć można do nich środki prewencyjne, kooperacyjne, stabilizacyjne i restrykcyjne. Postanowiono ustanowić unijne zespoły szybkiego reagowania na zagrożenia hybrydowe (ang. *EU Hybrid Response*

Teams). Zdecydowano też o podniesieniu świadomości sytuacyjnej poprzez wzmocnienie Hybrid Fusion Cell oraz zauważono konieczność poszukiwania możliwości poprawy współpracy z NATO.

Informacyjny wymiar przeciwdziałania zagrożeniom hybrydowym funkcjonuje w UE, jako element struktury wywiadowczej EU INTCEN. Służy ona za punkt kontaktowy grupujący unijne zasoby wywiadu cywilnego[291]. Ponadto, znajdujące się głębiej w strukturach centrum analityczne SIAC (Signal Intelligence Analysis Capacity) nie tylko dostarcza informacji dla decydentów UE, ale także wysyła raporty do państw członkowskich. Ich tematyka wynika z bieżących priorytetów (ang. *assesments driven by priority*). Świadomość sytuacyjna (situational awareness) jest bardzo istotna dla działania sił unijnych, zwłaszcza operujących za granicą w czasie misji Wspólnej Polityki Bezpieczeństwa i Obrony[292]. W ramach INTCEN działa unijna komórka (ang. *hybrid fusion cell*), która zajmuje się monitorowaniem zagrożeń hybrydowych mających wpływ na bezpieczeństwo UE, jak kwestie migracji, skutki, ale też tzw. globalnego ocieplenia klimatu.

Centrum Satelitarne UE (SATCEN) jest małą, zdecentralizowaną instytucją wykorzystującą dane z satelitów państw członkowskich UE i wspierającą wywiadowczo (geospacial intelligence) służbę zagraniczną UE, unijne operacje / misje zagraniczne (w ramach Wspólnej Polityki Bezpieczeństwa i Obrony) oraz państwa członkowskie. Centrum Satelitarne UE wykorzystuje głównie satelity komercyjne (niemieckie, francuskie i włoskie), które zwykle są własnością firm z ponad 50% udziałem państwa. UE posiada swoje satelity (Copernicus), ale – z powodu ograniczeń rozdzielczości – nie nadają się one do działań wywiadowczych. Kwatera główna centrum znajduje się w hiszpańskim Torrejon de Ardoz i działa bez przerwy (24/7). Zajmuje się m.in. kwestiami konfliktów regionalnych, migracji, proliferacji broni masowego rażenia (WMD), czyli sfer, które pośrednio mogą generować zagrożenia natury hybrydowej. Zatrudnia ok. 150 osób (100 członków stałych, 40 pracowników czasowych oraz grupę przedstawicieli delegowanych do Centrum Satelitarnego UE (seconded national experts – SNEs)[293].

[291] Wywiad wojskowy działa natomiast w ramach odrębnej struktury również zajmując się hybrydowym wymiarem współczesnego pola walki.

[292] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

[293] Tamże.

Podejście UE do zagrożeń hybrydowych opiera się na rozwiązaniach instytucjonalnych wypracowanych od 2016 r., takich jak: Wspólne Ramy Przeciwdziałania Zagrożeniom Hybrydowym, mechanizm reagowania na ataki cybernetyczne (*EU Cyber Diplomacy Toolbox*), działalność Horyzontalnej Grupy ds. Odporności i Zagrożeń Hybrydowych (HWP ERCHT), a także Wydziału Komunikacji Strategicznej Europejskiej Służby Działań Zewnętrznych (*EU Stratcom*).

Określając metody postępowania w zakresie przeciwdziałania nowym zagrożeniom, jak trafnie zauważyła Beata Jagiełło, UE wychodziła z założenia, iż działania w tym zakresie powinny mieć charakter długofalowy oraz tworzyć spójny plan operacyjny. Dużą wagę należy przy tym przywiązać do koordynacji współpracy z partnerami Unii. Koncepcja przeciwdziałania nowym zagrożeniom, a więc także tym hybrydowym, zakłada wykorzystanie nie tylko działań bezpośrednich ale także tych mieszczących się w kategorii tzw. miękkiego bezpieczeństwa (ang. *soft security*)[294].

Komunikacja strategiczna jest kluczowa dla przeciwdziałania zagrożeniom hybrydowym w wymiarze dezinformacji. Główna aktywność instytucji UE w zakresie przeciwdziałania zagrożeniom hybrydowym jest ukierunkowana na przeciwdziałanie dezinformacji. Bardzo ważną jednostką UE do spraw przeciwdziałania dezinformacji jest East StratCom Task Force, który powstał w 2015 r. Utworzono ją rok po aneksji Krymu przez Federację Rosyjską i ukierunkowano na przeciwdziałanie dezinformacji w info-sferze rosyjskiej oraz wspieranie niezależnych dziennikarzy. Służy temu działalność *EU Stratcom.* Kluczową rolę w walce z dezinformacją ze strony Rosji odgrywa zespół *EU Stratcom East* prowadzący projekt zwalczania dezinformacji w mediach społecznościowych (*EUvsDisinfo)*[295]. Wymiana informacji o kampaniach dezinformacyjnych między państwami członkowskimi jest prowadzona w ramach tzw. systemu wczesnego ostrzegania (*Rapid Alert System*, RAS – uczestniczy w nim Ministerstwo Spraw Zagranicznych.

Wzrost wrogiej aktywności dezinformacyjnej w ostatnich latach przekłada się na rosnące zainteresowanie państw UE zapobieganiem rozprzestrzenianiem się fałszywych narracji, Rozmieszczenie struktur zajmujących się komunikacją strategiczną (StratCom) jest

[294] Zob. B. Jagiełło, *Unia Europejska wobec wyzwań dla bezpieczeństwa europejskiego i jego zagrożeń,* Bezpieczeństwo międzynarodowe. Teoria i praktyka. M. Grącik, K. Żukrowska (red.), 2006, s. 266-267.

[295] W maju 2021 r. szefową *Stratcom East* została Polka (Martyna Bildziukiewicz).

zróżnicowane w państwach członkowskich UE. Wśród modeli można wyróżnić m.in. powołanie centralnej jednostki ds. komunikacji strategicznej, nadanie jej międzyresortowego charakteru (rozlokowanie komórek ds. komunikacji strategicznej w kilku resortach), umiejscowienie koordynacyjnej roli tej służby w Ministerstwie Spraw Zagranicznych lub w biurze premiera lub brak wyspecjalizowanych jednostek zajmujących się dezinformacją (spełnianie tego zadania przez inne instytucje).

Dobrym przykładem odpowiedzialnego podejścia do przeciwdziałania dezinformacji są Niemcy, które posiadają rozbudowane zdolności w tym wymiarze w ramach pełniącego rolę wiodącą resortu spraw zagranicznych, jak i pozostałych ministerstw. Poza Ministerstwem Spraw Zagranicznych, jednostki zajmujące się walką z dezinformacją zlokalizowano aż w 10 ministerstwach oraz instytucjach federalnych. Jest to potwierdzeniem wagi, jaką rząd w Berlinie przykłada do tego wymiaru przeciwdziałania zagrożeniom hybrydowym. Podobnie duży nacisk na przeciwdziałanie dezinformacji kładzie Francja, w której przy premierze powołano dedykowaną agencję zajmującą się komunikacją strategiczną i przeznaczono do niej ponad 50 ekspertów.

Na forum UE podejmowane były inicjatywy legislacyjne i regulacyjne, które mają ułatwić zwalczanie dezinformacji. Służyła temu implementacja Europejskiego planu działania na rzecz demokracji z 2020 r.(*European Democracy Action Plan*, EDAP)[296].

W 2020 r. przyjęto Europejski Plan Działania na rzecz Demokracji (EDAP), którego jednym z głównych założeń jest aktualizacja i wzmocnienie Kodeksu Praktyk dla platform społecznościowych w następujących wymiarach:

a) efektywne oznaczanie postów;
b) sprawniejsza demonetyzacja;
c) większa transparentność reklamy politycznej;
d) udostępnienie danych dla fact-checkerów[297].

W Unii przygotowywane jest wdrożenie dwóch ważnych aktów prawnych mających na celu przeciwdziałania zagrożeniom hybrydowym w wymiarze dezinformacyjnym. Chodzi o Akt o usługach cyfrowych (DSA) oraz Akt o rynkach cyfrowych (DMA). Mają one

[296] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*
[297] *Dezinformacja jako główna oś kampanii hybrydowych…*

dokonać głębokich zmian regulacji świata online uchylając dyrektywę o handlu elektronicznym z 2000 r. Przez ponad dwie dekady w świecie elektronicznym dokonały się znaczące zmiany wymagające reakcji. Nowe przepisy nakładają bardzo restrykcyjne obowiązki na platformy społecznościowe, a zwłaszcza te o kluczowym znaczeniu (tzw. „Strażnicy dostępu" – ang. „Gatekeepers")[298].

Akt o usługach cyfrowych przewiduje mechanizm sygnalizowania przez użytkowników fałszywych treści, a w przypadku platform – mechanizm współpracy z „zaufanymi podmiotami sygnalizującymi. Wprowadza się także ułatwienia w dostępie analityków do danych przechowywanych przez główne platformy, aby umożliwić im analizę działalności w kontekście przeciwdziałania dezinformacji

Co istotne w kontekście usprawniania systemu przeciwdziałania zagrożeniom hybrydowym w UE, raport Europejskiego Trybunału Obrachunkowego stwierdził, że dotychczasowe działania UE okazały się niewystarczające. W UE brakuje m.in. mechanizmów koordynacji współpracy państw członkowskich, działań na rzecz podniesienia odporności społecznej, czy narzędzi pozwalających na skuteczne wpływanie na postępowanie platform internetowych.

W tym kontekście, w celu poprawy unijnych zdolności przeciwdziałania zagrożeniom hybrydowym, w czerwcu 2021 r. Europejska Służba Działań Zewnętrznych zainicjowała dyskusję na temat zastąpienia terminu dezinformacji bardziej kompleksowym pojęciem „zewnętrznej manipulacji i ingerencji informacyjnej" (*foreign infromation manipulation and intereference*, FIMI). Jest to punkt wyjścia do wzmocnienia mechanizmu reagowania UE na wrogie działania w przestrzeni informacyjnej określanego jako *FIMI Toolbox*.

Instytucje UE pracowały w ostatnich latach nad wdrożeniem unijnej strategii wzmacniania cyberbezpieczeństwa z 2020 r. (*The EU's Cybersecurity Strategy for the Digital Decade*), składającej się z inicjatyw regulacyjnych, inwestycyjnych i politycznych. Trwały także przygotowania do powołania wspólnej jednostki ds. cyberbezpieczeństwa (Joint Cyber Unit, JCU)[299].

Prowadzone były także prace nad wzmocnieniem unijnego Kodeksu postępowania w zakresie przeciwdziałania dezinformacji dla platform internetowych. W maju 2021 r. KE

[298] Tamże.
[299] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

opublikowała wytyczne w sprawie poszerzenia zakresu odpowiedzialności platform i nadania ustanowionym w kodeksie normom bardziej wiążącego charakteru (stosowanie kodeksu było do tej pory dobrowolne). 16 czerwca 2022 r., jak podała KE UE, zaostrzono kodeks postępowania w zakresie zwalczania dezinformacji. Wprowadzono szerokie i precyzyjne zobowiązania branży do walki z dezinformacją. Wśród 34 sygnatariuszy znalazły się największe platformy internetowe (m.in. Meta, Google, Twitter, TikTok i Microsoft)[300].

Ponadto, KE prowadziła prace dotyczące wyznaczenia wskaźników odporności UE, wzorowanych na podobnych rozwiązaniach NATO (*resilience baselines*), obejmujących np. dostawy podstawowych usług, zaopatrzenie w podstawowe produkty. UE przygotowywała także nowe akty prawne, które mogą podnieść odporność infrastruktury UE. Trwały też prace nad projektem Rozporządzenia w sprawie jednolitego rynku usług cyfrowych (*Digital Services Act*), który będzie regulować działalność przedsiębiorstw cyfrowych, w tym największych platform społecznościowych i potencjalnie zawierać narzędzia służące zwalczaniu dezinformacji[301].

UE monitorowała w minionych latach rozwój zagrożeń hybrydowych wobec państw członkowskich, instytucji, czy unijnych misji zagranicznych. W 2021 r. KE przygotowała raport podsumowujący wyniki drugiego badania gotowości i odporności UE na zagrożenia hybrydowe (*Hybrid Risk Survey*), w którym potwierdziła wzrost zagrożeń hybrydowych wobec UE, przewidując dalsze utrzymanie się tego trendu. W ramach Unii od 2019 r. działa także Horyzontalna Grupa ds. Odporności i Zagrożeń Hybrydowych (HWP ERCHT). Jej pracami kieruje zawsze aktualna prezydencja UE[302].

Jednym z instrumentów tzw. miękkiej siły w zakresie przeciwdziałania zagrożeniom hybrydowym jest wydawanie wspólnych oświadczeń potępiających wrogie działania danego kraju. 10 maja 2022 r. UE opublikowała w imieniu 27 państw członkowskich deklarację potępiającą Rosję za cyberataki prowadzone przeciwko Ukrainie. Podobne oświadczenia wydali przedstawiciele władz Wielkiej Brytanii, Kanady oraz Australii. Bezpośrednią przyczyną wydania deklaracji był cyberatak na satelitarną sieć KA-SAT przeprowadzony

[300] *Zwalczanie dezinformacji w odniesieniu do koronawirusa*, strona internetowa Komisji Europejskiej 16 czerwca 2022 r.
https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_pl [dostep: 18.10.2022].

[301] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

[302] Tamże.

24 lutego 2022 r. (na godzinę przed rozpoczęciem rosyjskiej operacji wojskowej na Ukrainie. W wyniku cyberoperacji ucierpiały ukraińskie siły zbrojne i instytucje sektora publicznego. Skutki ataku Federacji Rosyjskiej dotknęły także kilka państw UE. 11 maja 2022 r. szef unijnej dyplomacji Josep Borrell poinformował, że to Rosja stała za masowym cyberatakiem, który pozbawił dostępu do Internetu tysiące Ukraińców.

Działania UE w zakresie przeciwdziałania zagrożeniom hybrydowym są także ukierunkowywane na wpływanie na kształtowanie bezpieczeństwa i stabilności w sąsiedztwie Unii. Do instrumentów wpływu UE na państwa trzecie należy handel oraz siła transformacyjna w postaci usprawnienia systemu sprawiedliwości, z naciskiem na zwalczanie korupcji. Dotyczy to m.in. przeciwdziałaniu masowych migracji lub wzrostu ekstremizmu. W ostatnich latach zainteresowanie w tym zakresie wiązało się ze wzrostem zagrożeń hybrydowych na wschodzie Europy oraz w różnych krajach afrykańskich. Jako przykład działań w tym kierunku warto odnotować, że UE wysłała siły FRONTEXU do Mołdawii – kraju wschodniego sąsiedztwa Unii.

Działania hybrydowe w Afryce, według autorów – opracowanego dla UE – raportu o implikacjach tego zjawiska obejmują m.in. wsparcie używających przemocy podmiotów niepaństwowych, wykorzystanie prywatnych firm wojskowych, atakowanie infrastruktury krytycznej i ingerencję z zagranicy w wybory celem przeforsowania korzystnej dla siebie władzy. Często te narzędzia są używane jednocześnie lub w różnych kombinacjach[303].

Unia starała się wpływać na stabilizację sytuacji politycznej w Afryce celem zminimalizowania ryzyka generowania na tym kontynencie zagrożeń hybrydowych, takich jak chociażby niekontrolowane migracje czy baza dla wymierzonej w państwa europejskie działalności terrorystycznej. Unijne misje wspólnej polityki bezpieczeństwa i obrony (WPBiO), za pomocą których UE postanowiła realizować te cele, są coraz częściej atakowane przez podmioty państwowe i niepaństwowe prowadzące operacje hybrydowe. Dokonuje się to w ramach szerszych prób podważenia wiarygodności i interesów UE w państwach afrykańskich. Misje WPBiO stają się celami ataków, ale – co podkreślają G., Faleg i N. Kovalčíková – są także częścią rozwiązania i ważnym instrumentem UE. Misje służą więc jako wskaźnik do oceny, w jakim stopniu UE stała się bezpośrednim celem i jak

[303] G., Faleg, N. Kovalčíková, *Rising Hybrid Threats in Africa. Challenges and implications for the EU*, 3 March 2022 https://www.iss.europa.eu/content/rising-hybrid-threats-africa [dostęp 13.4.2022].

szeroko mogą być dotknięte europejskie interesy bezpieczeństwa takimi zagrożeniami. Przewódcy UE dostrzegają potrzebę wzmożonych wysiłków i inicjatyw mających na celu ochronę unijnej obecności w Afryce przed szkodliwymi skutkami zagrożeń hybrydowych. Dzięki rozmieszczeniu tych misji kraje Unii przyczyniają się do przeciwdziałania zagrożeniom hybrydowym i budowaniu odporności[304].

Jednak, w obecnych uwarunkowaniach cywilne misje zagraniczne UE stają się obiektem ataków hybrydowych, w tym cybernetycznych i dezinformacyjnych. Unijna misja monitorująca na Ukrainie została zbombardowana (siedziba w Mariupolu) przez Rosję w 2022 r., co może być odczytane także symbolicznie, – jako pokaz siły i intencji Kremla dającego sygnał o swoim sprzeciwie wobec zaangażowania krajów europejskich na Ukrainie. Dlatego rozwój zdolności przeciwdziałania tego typu zagrożeniom w UE powinien być kontynuowany. Chodzi tu także o ewentualne przyszłe misje unijne na Ukrainie oraz w państwach Partnerstwa Wschodniego.

Także poszczególne kraje członkowskie UE prowadziły działania na rzecz zwalczania zagrożeń hybrydowych. W Danii w 2017 r. został utworzony Międzyresortowy Zespół Zadaniowy ds. Przeciwdziałania Dezinformacji, który odpowiada za monitorowanie dezinformacji, doradzanie partiom politycznym i koordynację działań. Struktura pierwotnie została powołana, aby przeciwdziałać ingerencji w kampanię wyborczą przed wyborami, ale prowadzi działalność również w okresie pomiędzy wyborami. Składa się on z ministrów: sprawiedliwości (rola koordynatora), spraw zagranicznych, obrony oraz służby wywiadu policyjnego (PET) i służby wywiadu wojskowego (FE). Przedstawiciele resortów spotykają się na szczeblu roboczym regularnie co kwartał, a także częściej – ad hoc w celu omówienia konkretnych spraw. W ramach zespołu, duńskie ministerstwo spraw zagranicznych odpowiada za współpracę międzynarodową w zakresie zwalczania dezinformacji, reprezentuje kraj w zespołach roboczych przy NATO i UE (np. w ramach Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats). W fińskim resorcie spraw zagranicznych w 2014 r. utworzono stanowisko cyberambasadora, do obowiązków którego zaliczono wzmocnienie działań dyplomatycznych w sferze zagrożeń cybernetycznych. Ponadto, w 2018 r. zdecydowano o utworzeniu kolejnego stanowiska mającego zapewnić wzmocnienie działań w zakresie zwalczania zagrożeń hybrydowych –

[304] Tamże.

ambasadora ds. hybrydowych. Został nim Mikko Kinnunen, kierujący wcześniej w resorcie wydziałem polityki bezpieczeństwa i zarządzania kryzysowego.

Aktywność Polski na forum UE utrzymywała się w ostatnich latach na wysokim poziomie. Polska popierała działania na rzecz przeciwstawienia się przez UE atakom hybrydowym. Opowiadała się m.in. za wypracowaniem mechanizmów przypisania autorstwa ataków (atrybucji) oraz wyciągania konsekwencji wobec sprawców (sankcje). Ponadto, Polska wspierała inicjatywy regulacyjne mające przyczynić się do zwiększenia odporności UE na zagrożenia hybrydowe – zwłaszcza te we wschodnim sąsiedztwie UE (m.in. kwestia instrumentalizacja migracji). W dniach 25-26 kwietnia 2019 r. w Warszawie odbyło się pierwsze spotkanie ekspertów ds. zagrożeń hybrydowych NATO, które było współorganizowane przez Ministerstwo Spraw Zagranicznych i Rządowe Centrum Bezpieczeństwa. Wzięli w nim udział przedstawiciele państw sojuszniczych, Sekretariatu Międzynarodowego NATO oraz helsińskiego Centrum Doskonalenia ds. Zagrożeń Hybrydowych.

Kwestiom przeciwdziałania zagrożeniom hybrydowym poświęca się coraz więcej uwagi także w ramach NATO. W ostatnich latach Sojusz Północnoatlantycki wzmacniał zdolności w zakresie reagowania na zagrożenia hybrydowe, opierając się na przyjętej w 2015 r. strategii NATO w sprawie przeciwdziałania zagrożeniom hybrydowym. Bazowała ona na 3 filarach: gotowości, odstraszaniu i obronie. W 2016 r. szczyt NATO w Warszawie podkreślił konieczność zacieśnienia współpracy Sojuszu Północnoatlantyckiego z Unią w celu zapewnienia lepszej odpowiedzi na te zagrożenia. W lipcu 2018 r., podczas Szczytu w Brukseli, podjęto decyzję o powołaniu zespołów przeciwdziałania zagrożeniom hybrydowym, które miały zapewnić wsparcie dla państwa goszczącego taki zespół w przygotowaniu i reagowaniu na zagrożenia hybrydowe. W przypadku ataku hybrydowego Rada Północnoatlantycka może uruchomić art. 5 Traktatu Waszyngtońskiego, tak jak w przypadku ataku zbrojnego, co potwierdzili przywódcy państw NATO podczas szczytu w 2021 r.

Odporność jest często wymieniana przez ekspertów, jako istotna metoda przeciwdziałania skutkom ataków hybrydowych. W ramach NATO prawnym filarem budowania odporności jest art. 3 Traktatu Waszyngtońskiego. Artykuł 3 tego traktatu mówi o tym, że dla „skuteczniejszego osiągnięcia celów niniejszego Traktatu Strony, każda

z osobna i wszystkie razem, przez stałą i skuteczną samopomoc i pomoc wzajemną będą utrzymywały i rozwijały swoją indywidualną i zbiorową zdolność do odparcia zbrojnej napaści[305].” Kładzie on nacisk na rozwój indywidualnych zdolności obronnych członków sojuszu. Poszczególne państwa NATO są przez to zobowiązane wzmacniać swój system bezpieczeństwa, który służy także przeciwdziałaniu zagrożeniom hybrydowym. Kraje nie mogą więc być bierne w tym zakresie licząc wyłączanie na wsparcie pozostałych sojuszników, ale są zobowiązane do zadbania o swoje bezpieczeństwo w pierwszej kolejności. Wymaga to stałego monitorowania stanu swoich sił zbrojnych, ich wzmacnianie i zapewnienie, że są one gotowe do odparcia agresji. Ponadto, ważną rolę ma budowanie odporności społeczeństwa na zagrożenia, jego zdolności obronnych oraz usprawnianie współpracy cywilno-wojskowej[306]. Kwestie związane z pandemią COVID-19 wpłynęły na postrzeganie problematyki odporności społecznej w Sojuszu. Od 2016 r. państwa członkowskie raportują do Paktu na ile są odporne w poszczególnych dziedzinach i czy mają gdzieś luki, które wymagają wypełnienia.

Szczyt NATO w Warszawie w 2016 r. zapoczątkował debatę o odporności. W Deklaracji Szefów Państw i Rządów dot. wzmacniania odporności zawarto 7 wytycznych na rzecz odporności:

1. gwarantowana ciągłość rządów i podstawowych usług rządowych;
2. odporne dostawy energii;
3. zdolność do skutecznego radzenia sobie z niekontrolowanym przepływem osób;
4. odporne zasoby żywności i wody;
5. zdolność do radzenia sobie z ofiarami na skalę masową;
6. odporne cywilne systemy łączności;
7. odporne systemy transportu cywilnego[307].

[305] *Traktat Północnoatlantycki,* Biuro Bezpieczeństwa Narodowego https://www.bbn.gov.pl/download/1/15754/TraktatPolnocnoatlantycki.pdf [dostęp: 9.09.2022].

[306] *Wzmacnianie odporności, jako kluczowa metoda przeciwdziałania zagrożeniom hybrydowym – odporność w NATO, UE i lessons learned z wybranych państw,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

[307] Tamże.

Szczyt NATO w Brukseli 2021 r. był kolejnym krokiem w stronę wzmacniania sojuszniczej odporności za zagrożenia, w tym hybrydowe. Najważniejszym novum było ustanowienie Komitetu ds. Odporności oraz Wysokich Przedstawicieli ds. Odporności. Podniesiono tym samym rangę tego zagadnienia w państwach sojuszniczych. Te kroki zostały podjęte w odpowiedzi na wyzwania stwarzane przez pandemię. Inicjatywie zwiększania odporności społecznej, z którą wyszła Polska, poświecono dużo uwagi podczas szczytu. Uznano, że społeczeństwo musi pełnić rolę spoiwa zaprezentowanych wcześniej 7. wytycznych na rzecz odporności[308].

Podejście do odporności w UE różni się od tego w NATO, gdzie jest to proces linearny. Natomiast w UE, z uwagi na kompleksowością i złożoność struktur unijnych, trudniej jednoznacznie wskazać kto odpowiada za kwestie promowania i wzmacniania odporności.

W UE występuje dwutorowe podejście do kwestii odporności: wymiar wewnętrzny (bezpieczeństwo państw UE) oraz zewnętrzny (pomoc rozwojowa i humanitarna dla regionów mających znaczenie dla bezpieczeństwa unijnego). Jeśli chodzi o wewnętrzny wymiar odporności w UE, w sprawozdaniu Komisji Europejskiej (KE) dot. Prognozy Strategicznej w 2020 r. stwierdzono, że *odporność nie jest tylko zdolnością do stawienia czoła wyzwaniom i radzenia sobie z nimi, ale także do „przechodzenia przez zmiany w sposób zrównoważony, sprawiedliwy i demokratyczny”.* Państwa UE badają swoją odporność za pomocą mierników, które różnią się jednak od tych natowskich. Chodzi o *cztery powiązane ze sobą wymiary – społeczno-gospodarczy, geopolityczny, ekologiczny i cyfrowy. Państwa członkowie analizując swoją odporność mogą aplikować w KE o granty na rzecz tych w celu poprawy sytuacji w tych krajach w tych czterech domenach*[309].

Jesienią 2021 wydano Konkluzje Rady UE w sprawie zwiększenia gotowości, zdolności do reagowania i odporności na przyszłe kryzysy, co wynikało z zagrożeń generowanych przez COVID-19 i migrację. Państwa zachodnie wyciągnęły wnioski z pandemii i dostrzegły potrzebę wzmacniania społeczeństw i struktur państwowych. Przyczyniły się do tego inspirowane przez siły wrogie Zachodowi kampanie dezinformacyjne rozbijace jedność krajów UE i NATO. W wielu krajach, także w Polsce,

[308] Tamże.
[309] Tamże.

miały miejsce przypadki paniki i wykupywania artykułów na zapas. Brak świadomości, że panika nie służy wzmocnieniu bezpieczeństwa, paraliżował dostawy części produktów spożywczych i innych[310].

Natomiast, jeśli chodzi o odporność w UE w wymiarze zewnętrznym, początkowo miała ona aspekt humanitarny i rozwojowy. Odporność definiowano w tym ujęciu, jako „zdolność jednostki, gospodarstwa domowego, społeczności, kraju lub regionu do radzenia sobie i szybkiej odbudowy po stresach i wstrząsach, takich jak przemoc, konflikty, susze i inne klęski żywiołowe bez narażania długoterminowego rozwoju. Aspekt ten został wzbogacony o kwestie bezpieczeństwa". Globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej w 2016 r. określiła, że odporność to „zdolność państw i społeczeństw do reformowania się, a tym samym przeciwstawiania się wewnętrznym i zewnętrznym kryzysom oraz odbudowa po nich – jest korzystna dla nas i dla krajów w naszych sąsiednich regionach, gdyż zapoczątkowuje trwały wzrost gospodarczy i prężne społeczeństwa". UE monitoruje stan odporności wewnątrz, ale ma świadomość tego, że zewnętrzne otoczenie międzynarodowe Unii wpływa na stan bezpieczeństwa jej państw członkowskich. Unia zidentyfikowała Wschód i Południe jako jeden z priorytetów swojej strategii budowania odporności państw i społeczeństwa[311].

Kolejnym dokumentem traktującym o wymiarze zewnętrznym unijnej odporności jest, przyjęty w marcu 2022 r., Strategiczny kompas na rzecz bezpieczeństwa i obrony, w którym zaznaczono już przewartościowania sytuacji wynikające z wojny na Ukrainie. Stwierdzono w nim, iż w związku z tym, że „środowisko bezpieczeństwa staje się coraz bardziej wrogie, musimy poczynić ogromny krok naprzód i zwiększyć naszą zdolność i chęć do działania, wzmocnić naszą odporność, a także zapewnić solidarność i wzajemną pomoc". Odporność UE powiązana została w tym dokumencie ze zwalczaniem zagrożeń hybrydowych (cyberbezpieczeństwo, ochrona IK, zwalczanie dezinformacji). Trend w zakresie unijnego podejścia do odporności wskazuje na odchodzenie od jej „miękkiego" charakteru (wsparcie gospodarcze, humanitarne) na rzecz akcentowania wymiaru „twardego" bezpieczeństwa. Wynikało to nie tylko z wojny na Ukrainie, ale też z efektów pandemii[312].

[310] Tamże.
[311] Tamże.
[312] Tamże.

Odporność ma także wymiar regionalny z uwzględnieniem krajów w sąsiedztwie RP. W odpowiedzi krajów, takich jak Szwecja czy Litwa, Polska mogłaby podjąć wzmożone działania w zakresie zwiększenia stopnia swojej odporności. Władze szwedzkie w latach 50-tych XX wieku przygotowały materiał informacyjny w postaci broszury dla społeczeństwa na czas kryzysu lub wojny („If crisis or war comes"), który podlegał aktualizacjom. W sąsiedztwie Polski, podobne materiały są wydawane także przez inne kraje, m.in. Estonię i Łotwę[313].

Agencja Swedish Civil Contingencies Agency jest odpowiedzialna za regularne przygotowanie szkoleń oraz kampanii informacyjnych dla ludności, sektora prywatnego, pozarządowego oraz administracji, które mają zwiększać świadomość wszelkich zagrożeń, w tym hybrydowych. Są one opracowywane nie tylko po szwedzku, ale i po angielsku. Przykładem innego kraju aktywnie przeciwdziałającemu zagrożeniom jest Litwa, gdzie charakterystyczną cechą jest oddolny charakter tego typu działań[314].

Dla przykładu, walka z dezinformacją stała się tam domeną działań luźno powiązanych ze sobą osób (na zasadzie grupy Anonymous) określanych jako „Elfy przeciwko Trollom", który został ukierunkowany na przeciwdziałanie aktywności szerzących rosyjską narrację tzw. trolli. Storna litewska przyznaje, że wielkość tego kraju wymusza kompleksowe podejście do zagrożeń hybrydowych uwzgledniające zagazowanie zwykłych ludzi („whole of socjety"). Te osoby („Elfy") funkcjonują w sposób anonimowy na Litwie. Polska także podejmuje kroki w zakresie budowania tego typu zdolności. Jest to skomplikowany proces, który wymaga dużego zaufania po stronie różnych partnerów (rząd – organizacje pozarządowe – biznes)[315].

Na szczególną uwagę zasługuje także model fiński, w którym funkcjonuje koncepcja całościowego bezpieczeństwa, w której łączy się wymiar militarny i pozamilitarny oraz nacisk na stałą gotowość do reagowania na sytuacje kryzysowe. Finowie są przygotowaniu na czas pokoju, kryzysu i wojny (czas P,K i W) w 7 następujących obszarach do zabezpieczenia: przywództwo, aktywność międzynarodowa, zdolności obronne, bezpieczeństwo wewnętrzne, bezpieczeństwo dostaw, prawidłowe funkcjonowanie społeczeństwa i usług publicznych oraz odporność psychologiczna. Prowadzone są tam

[313] Tamże.
[314] Tamże.
[315] Tamże.

bardzo kompleksowe szkolenia, w których biorą udział zarówno eksperci rządowi i ze służb mundurowych, ale także politycy ze wszystkich stron sceny politycznej oraz dziennikarze. Interakcje przedstawicieli różnych grup zawodowych podczas tego typu ćwiczeń są bezcenne w zakresie budowania zaufania, kanałów kontaktu oraz pogłębionej kooperacji. Programy szkoleń dla społeczeństwa obejmują m.in. kurs przetrwania w niesprzyjających warunkach (np. konieczność spędzenia 72 godzin w lesie). Przykład fiński jest wyjątkowy także ze względu na znaczny procent społeczeństwa deklarującego wsparcie w sytuacji kryzysowej[316].

Wśród niedostatków aktywności UE w obszarze zagrożeń hybrydowych w ostatnich latach należy przede wszystkim odnotować brak wdrożenia nowych aktów prawnych służących wzmocnieniu odporności państw członkowskich i instytucji UE, czy ograniczeniu swobody („szarej strefy") działania aktorów hybrydowych. Ponadto, mimo deklarowanej przez UE woli współpracy z NATO ws. zwalczania zagrożeń hybrydowych, w praktyce kontakty obu instytucji były ograniczone[317].

W UE istnieją różnice zdań w zakresie podejścia do przeciwdziałania zagrożeniom hybrydowym na kontynencie afrykańskim. Część państw członkowskich uzależnia swoje zaangażowanie od przychylności lokalnych władz. Jeśli władze afrykańskie współpracują jednak z prorosyjskimi organizacjami paramilitarnymi i prywatnymi firmami wojskowymi, jak Grupą Wagnera to takiej kooperacji być nie może. Ale sytuacja ta stanowi wyzwanie strategiczne dla UE, która może zostać zmuszona do wycofywania się z kluczowych regionów w Afryce a może i w innych częściach świata, które maja znaczenie w kontekście przeciwdziałania zagrożeniom hybrydowym. Powiązana z władzami na Kremlu Grupa Wagner, przez swoją aktywność m.in. w Centralnej Republice Afrykańskiej, doprowadziła do zablokowania misji UE w Mali. Skuteczność NATO i UE, co zauważył Piotr Szymański, ograniczają obecnie niedostateczne środki finansowe na przeciwdziałanie zagrożeniom hybrydowym oraz brak woli państw członkowskich do zwiększenia wymiany informacji wrażliwych, dotyczących np. ochrony infrastruktury krytycznej czy cyberbezpieczeństwa[318].

Reagując na zagrożenia hybrydowe UE koncentrowała się dotychczas na budowaniu odporności. Rozpoczęcie prac nad *EU Hybrid Toolbox* daje szansę stworzenia wspólnych

[316] Tamże.
[317] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*
[318] P. Szymański, op. cit.

narzędzi odpowiedzi na ataki hybrydowe, których dotkliwość może przyczynić się do powstrzymania części szkodliwych działań[319]. Nie należy jednak przeceniać przyszłej roli *EU Hybrid Toolbox*. Mimo nieustannych ataków cybernetycznych, w ramach istniejącego już mechanizmu przeciwdziałania zagrożeniom w cyberprzestrzeni, UE jedynie sporadycznie wytacza najcięższe działa, czyli stosuje sankcje (w lipcu i w październiku 2020 r. - w pierwszym przypadku po atakach na Organizację ds. Zakazu Broni Chemicznej (ang. *Organisation for the Prohibition of Chemical Weapons*, OPCW) OPCW, a w drugim w odpowiedzi na ataki rosyjskich hakerów w 2015 r. na niemiecki Bundestag)[320].

Jeśli chodzi o współpracę NATO i UE w ramach przeciwdziałania zagrożeniom hybrydowym istnieje potencjał do jej zacieśnienia, jednak obecnie największy poziom kooperacji ma miejsce albo w ramach państw NATO albo UE (wspólne ćwiczenia mają ograniczony charakter). W ostatnich latach stopniowo wzrastało zaangażowanie NATO i Unii Europejskiej w zwalczanie zagrożeń hybrydowych ze strony państw i aktorów niepaństwowych. Jednak organizacje te powinny poświęcać problematyce zagrożeń hybrydowych jeszcze większą uwagę.

Treści dezinformacyjne wokół inwazji Rosji na Ukrainie, w ocenie władz wielu państw zachodnich, powielane były głównie przez skrajnie prawicowe grupy, ekstremistyczne środowiska antyrządowe oraz grupy opowiadające się za obywatelską swobodą stosowania sczepień. W kontekście potrzeby zachowania wolności słowa, wypowiedzi m.in. osób publicznych powinny być generalnie traktowane jako opinie, a nie jako dezinformacja. Granica jest tu jednak dość płynna i ocena danego przypadku może nastręczać rozbieżności interpretacyjnych. Podstawą do oceny działania danego medium (np. w odniesieniu do sytuacji na Ukrainie powinny być rzetelnie zweryfikowane fakty, co jednak jest utrudnione w warunkach kryzysowych lub wojennych.

Strategia Bezpieczeństwa Narodowego RP, ogłoszona w maju 2020 r., zawiera konkretne odniesienia do kwestii odporności państwa na zagrożenia. Pojawia się tu postulat tworzenia – opartego na wysiłku całego narodu – systemu obrony powszechnej oraz budowanie zrozumienia dla rozwoju odporności i zdolności obronnych Polski. Nawiązuje ona do konieczności zwiększenia odporności na zagrożenia w zakresie 7 wytycznych na

[319] Tamże.
[320] Tamże.

rzecz odporności NATO. Ujęto w niej potrzebę przeciwdziałania zagrożeniom hybrydowym oraz wyzwania związane z systemem edukacji – również w zakresie bezpieczeństwa informacyjnego. Za istotne uznano, aby budować system obrony powszechnej w pełni wykorzystujący potencjał instytucji państwowych i samorządowych, podmiotów systemu edukacji i szkolnictwa wyższego, społeczności lokalnych, podmiotów gospodarczych, organizacji pozarządowych oraz obywateli, który będzie stanowił kompleksową odporność państwa na zagrożenia niemilitarne i militarne[321]. Wydarzenia za wschodnia granicą Polski (wojna na Ukrainie) skłaniają do przyspieszenia prac wdrażających zaprezentowane wcześniej rozwiązania.

Działania Sojuszu Północnoatlantyckiego skoncentrowały się w ostatnich latach na zabezpieczeniu przed militarnymi zagrożeniami hybrydowymi (poprawiono zdolności wywiadowcze i szybkość Sił Odpowiedzi NATO – VJTF) oraz pozamilitarnymi (przede wszystkim cyberbezpieczeństwo i przeciwdziałanie dezinformacji). Ważna była deklaracja szczytu NATO w Warszawie w 2016 r., w której stwierdzono, że Pakt jest gotowy udzielić wsparcia zaatakowanemu państwu członkowskiemu na każdym etapie kampanii hybrydowej, a Rada Północnoatlantycka może uruchomić art. 5 traktatu waszyngtońskiego[322].

W kontekście problematyki przeciwdziałania zagrożeniom hybrydowym warto przytoczyć spostrzeżenia ekspertów NATO Michaela Rühle i Clare Roberts, w ocenie których, zwalczanie zagrożeń hybrydowych jest „długoterminowym wyzwaniem strategicznym dla NATO i jego państw członkowskich. Wymaga odejścia od deliberatywnych i sekwencyjnych procesów planowania i podejmowania decyzji, typowych dla natowskich operacji reagowania kryzysowego w erze postzimnowojennej, w kierunku bardziej dynamicznego podejścia. W jego ramach nieustannie aktualizowana świadomość sytuacyjna inspiruje debatę polityczną, wypracowywanie opcji, podejmowanie decyzji i kontrolę polityczną. Aby robić to możliwie efektywnie NATO traktuje każdego hybrydowego gracza jako indywidualny podmiot posługujący się unikalną motywacją strategiczną. Bardziej ukierunkowane podejście podnosi zdolność NATO do ograniczania skuteczności kampanii hybrydowych poprzez wpływanie na analizę kosztów i korzyści dokonywaną przez potencjalnego hybrydowego przeciwnika, a także po to, by

[321] Tamże.
[322] P. Szymański, op. cit.

lepiej zwalczać „szarą strefę" pojawiającą się w tym, co stało się współczesnym teatrem operacyjnym[323]."

Jeśli chodzi o podejście NATO w zakresie reagowania na incydenty hybrydowe, obejmuje ono przede wszystkim monitorowanie i analizę zagrożeń, wymianę informacji wywiadowczych oraz zapewnianie wspólnej świadomości sytuacyjnej. Istotne w tym kontekście było stworzenie wydziału ds. analiz zagadnień hybrydowych, który powstał w 2017 r. w Kwaterze Głównej NATO (w ramach Połączonego Pionu Wywiadu i Bezpieczeństwa – Joint Intelligence and Security Division, JISD). Jego zadaniem jest analiza m.in. militarnych i niemilitarnych zagrożeń hybrydowych w transatlantyckiej strefie bezpieczeństwa[324]. NATO dysponuje też Zespołami Przeciwdziałania Zagrożeniom Hybrydowym (ang. Counter Hybrid Support Team, CHST). Eksperci wchodzący w skład tych zespołów, utworzonych w 2018 r., udzielają doraźnego wsparcia (doradztwo) władzom państw, w którym ma miejsce kryzys hybrydowy. Po raz pierwszy mechanizm ten wykorzystała Czarnogóra w 2019 r. w celu zwalczania zagrożeń hybrydowych ze strony Rosji (przed wyborami parlamentarnymi w 2020 r.). Wynikało to z oskarżeń Czarnogóry pod adresem Rosji i Serbii o próbę zorganizowania w tym kraju zamachu stanu w 2016 r. Misja zespołu, wspieranego przez specjalistów amerykańskich, skoncentrowały się na podniesieniu poziomu cyberbezpieczeństwa i zasugerowaniu zmian w ustawodawstwie[325].

O tym, że NATO traktuje zagrożenia informatyczne jako coraz ważniejsze zagadnienie, świadczy w ocenie P. Szymańskiego, uznanie cyberprzestrzeni za jedną z domen operacyjnych (analogicznie do lądowej, morskiej i powietrznej), co miało miejsce na szczycie w Warszawie w 2016 r. Przywołał on także stwierdzenie z deklaracji Sojuszu ze szczytu w Newport w 2014 r. o tym, że atak cybernetyczny może skutkować uruchomieniem art. 5.[326].

W ostatnich latach największe inwestycje w cyberbezpieczeństwo wśród europejskich sojuszników, jak odnotował analityk OSW, realizują Wielka Brytania (1,9

[323] M. Rühle, C. Roberts, *Zwiększanie zasobności środków NATO do zwalczania zagrożeń hybrydowych*, Przegląd NATO 19 marca 2021 https://www.nato.int/docu/review/pl/articles/2021/03/19/zwiekszanie-zasobnosci-srodkow-nato-do-zwalczania-zagrozen-hybrydowych/index.html [dostęp: 6.10.2022].

[324] P. Szymański, op. cit.

[325] Tamże.

[326] Tamże.

miliarda GBP w latach 2016–2021) i Francja (1,6 miliarda EURO w latach 2019–2025). Państwa członkowskie rozwijają też narodowe zdolności ofensywne w cyberprzestrzeni (dziewięć krajów zadeklarowało gotowość ich udostępnienia na potrzeby NATO)[327]. Utworzone w 2008 r. natowskie Centrum Doskonałości Obrony przed Cyberatakami w Tallinnie (NATO CCD COE) jest organizatorem głównych corocznych ćwiczeń Locked Shields[328].

Za ochronę sieci teleinformatycznych Paktu odpowiada Zespół Reagowania na Incydenty Komputerowe (działający w ramach NATO Computer Incident Response Capability, NCIRC[329]), który liczy około 200 ekspertów. NCIRC ma też zdolność wsparcia krajów członkowskich poprzez wysłanie zespołów szybkiego reagowania cybernetycznego, które w ciągu 24 godzin mogą udzielić pomocy w zakresie ochrony sieci[330].

W NATO działa także Centrum Operacji w Cyberprzestrzeni, które odpowiada za „budowanie świadomości sytuacyjnej Sojuszu dotyczącej zagrożeń cybernetycznych, koordynację aktywności państw członkowskich w cyberprzestrzeni, a także zabezpieczenie natowskich operacji i misji[331].”

Różnice w podejściu krajów członkowskich NATO są jednym ze słabych punktów systemu przeciwdziałania zagrożeniom hybrydowym. Państwa Sojuszu, które zainwestowały najwięcej w cyberbezpieczeństwo, niechętnie dzielą się technologiami z partnerami oszczędzającymi w przeszłości na tym obszarze. Wyzwaniem jest też trudność w rekrutacji odpowiednich specjalistów, która wynika z konkurencji z sektorem prywatnym[332].

Celem nadążenia za wyzwaniami postępu technologicznego, za ważną w NATO uznaje się współpracę z sektorem prywatnym, która jest realizowana jest m.in. przez platformę Malware Information Sharing Platform (dostęp do informacji dla firm na temat złośliwego oprogramowania). Dodatkowo, działa także program współpracy natowskiej Agencji Komunikacji i Informacji (NCIA) z podmiotami z sektora cyberbezpieczeństwa[333].

---

[327] Tamże.
[328] Tamże.
[329] NATO Communication and Information Agency – Cyber Security Service Line https://www.ncirc.nato.int/Home/About [dostęp: 11.08.2022].
[330] P. Szymański, op. cit.
[331] Tamże.
[332] Tamże.
[333] Tamże.

Istotnym elementem strategii przeciwdziałania zagrożeniom hybrydowym w NATO są ćwiczenia. Scenariusze hybrydowe uwzględnia się w corocznych ćwiczeniach zarządzania kryzysowego CMX (sztabowo-dowódczych). Ponadto, zdolność reagowania na zagrożenia hybrydowe jest sprawdzana podczas ćwiczeń poligonowych (m.in. NATO Trident Juncture, Brilliant/Noble Jump), w trakcie których doskonalone są metody ochrony infrastruktury krytycznej oraz zwalczania uzbrojonych grup sabotażowo-dywersyjnych[334].

Odnosząc się do przeciwdziałania zagrożeniom hybrydowym w NATO trzeba zaznaczyć, że Sojusz jest organizacją wojskową / obronną i kluczowe jest uznanie przez NATO, że będzie reagować na zagrożenia hybrydowe oraz wspierać swoich członków w tym zakresie. Zostało to ujęte w Strategii NATO w sprawie przeciwdziałania zagrożeniom hybrydowym, która została przyjęta w 2015 r. (rok po aneksji Krymu przez Rosję). Organizacja obwieściła wówczas, że wyraża wolę osiągniecia gotowości do przeciwdziałania wszelkim zagrożeniom hybrydowym, jakie mogą się pojawić oraz odstraszać tego typu ataki (prezentując zdolność do podejmowania decyzji politycznych, a gdy zaistnieje potrzeba obrony przed zagrożeniami hybrydowymi – udzielania szybkiej odpowiedzi militarnej. W przypadku, gdy odstraszanie natowskie zawiedzie, organizacja zapewniła, że podejmie się obrony wobec ataku hybrydowego, czyli zastosowany zostanie wówczas art. 5 Traktatu Waszyngtońskiego mówiący o przyjściu z pomocą państwu napadniętemu. Zostało to potwierdzone na szczytach NATO w Warszawie w 2016 r. oraz – ponownie – w Brukseli w 2021 r.[335] W przyjętej w Madrycie 29 czerwca 2022 r. koncepcji strategicznej Sojuszu Północnoatlantyckiego stwierdzono, iż przeciwnicy tej organizacji „inwestują w zaawansowane, bojowe zdolności konwencjonalne, nuklearne i rakietowe, ale także uciekają się do taktyk hybrydowych, zarówno bezpośrednio oraz za pomocą pośredników (proxies). Prowadzą wrogie działania w cyberprzestrzeni i kosmosie, realizują kampanie dezinformacyjne, instrumentalizują migracje, manipulują dostawami energii i stosują presję gospodarczą[336]".

[334] Tamże.

[335] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

[336] *NATO 2022 Strategic Concept*, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [dostęp: 22.07.2022].

Główna odpowiedzialność w zakresie przeciwdziałania zagrożeniom hybrydowym leży jednak po stronie państw członkowskich NATO, które w ostatecznym rozrachunku odpowiadają za swoje bezpieczeństwo. Względem państw członkowskich, NATO i UE odgrywają rolę subsydiarną zapewniając wsparcie w obszarach, które rządy zidentyfikują, jako wymagające wzmocnienia. Chodzi o budowanie wspólnej świadomości sytuacyjnej w zakresie zwalczania zagrożeń hybrydowych. Służy temu wymiana doświadczeń i poszerzanie wiedzy na ten temat realizowana za pomocą warsztatów i ćwiczeń z różnymi scenariuszami ataku hybrydowego lub ich serii. Ponadto, rolą NATO i UE jest wyznaczanie wspólnych standardów w zakresie zwalczania agresji hybrydowych. Ma to wzmocnić słabe ogniwa na poziomie narodowym, które wpływają na bezpieczeństwo europejskie i transatlantyckie[337].

Federacja Rosyjska, która odegrała kluczową rolę zarówno w przedstawionej wojnie w Syrii w 2011 r., jak i podczas konfliktu o Krym i Donbas w 2014 r., stała się w ostatnich latach ponownie najważniejszym rywalem NATO w Europie. Nastąpił, więc powrót do sytuacji z czasów Zimnej Wojny, jednak ze znacznie bardziej znaczącą rolą wspierających stronę rosyjską Chin. W wyżej wymienionym dokumencie koncepcyjnym Paktu Północnoatlantyckiego Rosję określa się jako największe i bezpośrednie zagrożenie dla bezpieczeństwa sojuszników oraz dla pokoju i stabilności w obszarze euroatlantyckim. Moskwa, w ocenie NATO, dąży do ustanowienia sfer wpływów i bezpośredniej kontroli poprzez stosowanie siły w relacjach międzynarodowych (przymusu), działalność wywrotową, agresję oraz aneksję. Ponadto, wykorzystuje środki konwencjonalne, cybernetyczne i hybrydowe przeciwko krajom uznanym za wrogie, w tym NATO[338].

Hybrydowym zagrożeniem NATO określa także Chińską Republikę Ludową, która stosuje szeroką gamę narzędzi politycznych, gospodarczych i wojskowych w celu zwiększenia swojego globalnego zasięgu. Polityka władz w Pekinie pozostaje jednocześnie niejasna w kwestii strategii, intencji i celu rozbudowy zdolności wojskowych. Wrogie hybrydowe i cybernetyczne operacje ChRL i ich konfrontacyjna retoryka szkodzą bezpieczeństwu Sojuszu. ChRL stara się ponadto kontrolować kluczowe sektory technologiczne i przemysłowe, surowce strategiczne i łańcuchy dostaw. Chiny wykorzystują

[337] Tamże.
[338] Tamże.

także swoją ekonomiczną przewagę do tworzenia strategicznych zależności i dalszego wzmacniania wpływów. Autorzy natowskiej koncepcji wskazują na pogłębianie strategicznego partnerstwa między Chińską Republiką Ludową a Federacją Rosyjską oraz ich wzajemnie wzmacniające się próby podkopania korzystnego dla świata zachodniego obecnego ładu międzynarodowego[339].

Chińskie podejście do działań hybrydowych zostało wyrażone m.in. w opublikowanej w 1999 r. książce emerytowanych pułkowników Armii Ludowo Wyzwoleńczej pt. „Nieograniczona wojna" (ang. Unrestricted Warfare), w której opisane są cywilne narzędzia walki takie jak wojna ekonomiczna, ataki terrorystyczne i cybernetyczne dezinformacja w Internecie oraz wykorzystanie instytucji pozarządowych do wpływu na politykę zagraniczną USA. Jest to rozwinięcie i zaktualizowanie, jak zauważa Michał Bogusz, niemieckiej koncepcji „wojny totalnej" z czasów I wojny światowej przewidującej m.in. ataki na cywilne statki. Ponadto, opracowanie to porusza tematykę strategii i konfliktu opisaną już w innych dobrze znanych na świecie książkach, takich jak „O wojnie" Clausewitza (1832 r.), „Ksiażę" Machiavellego (1513 r.), czy „Sztuka wojny" Sun Tzu z V w. p.n.e.[340].

Rozwiązań w zakresie przeciwdziałania zagrożeniom hybrydowym dostarcza obowiązująca koncepcja strategiczna NATO z 2022 r., która wskazuje na potrzebę inwestycji w zdolności do odstraszania i obrony przed staniem się celem taktyki politycznej zakładającej użycie siły, presji ekonomicznej, w tym – energetycznej, działań informacyjnych i innej hybrydowej taktyki stosowanej przez państwa i podmioty niepaństwowe. Istotnym nowym elementem pokazującym na wzrastające znaczenie zagrożeń hybrydowych jest stwierdzenie, iż operacje hybrydowe mogą osiągnąć skalę charakterystyczną dla ataku zbrojnego, co może zmusić Radę Północnoatlantycką do powołania się na artykuł 5 Traktatu Waszyngtońskiego[341].

Za ważny element przeciwdziałania wyzwaniom hybrydowym NATO uznaje wsparcie krajów partnerskich z innych struktur, takich jak Unia Europejska. Celem jest

[339] Tamże.

[340] Chodzi o książkę Qiao Liang i Wang Xiangsui. Zob. M. Bogusz, *Unrestricted Warfare*, portal Za Wielkim Murem: Chiny i Azja, https://zawielkimmurem.net/2018/10/28/qiao-liang-wang-xiangsui-unrestricted-warfare/ [dostęp: 28.11.2022].

[341] *NATO 2022 Strategic Concept…*

maksymalizacja synergii wynikająca z obustronnie korzystnej współpracy. Sojusz Północnoatlantycki postrzega UE za swojego niezbędnego partnera z uwagi na podzielanie tych samych wartości. NATO i UE odgrywać przy tym mogą uzupełniające się role we wspieraniu międzynarodowego pokoju i bezpieczeństwa. Odpowiedzią na zagrożenia nowego typu, w tym o hybrydowej naturze[342], jest więc wzmocnienie strategicznego partnerstwa NATO-UE, intensyfikacja konsultacji politycznych i zwiększenie współpracy w tym obszarze[343].

Dla rozwoju strategicznego partnerstwa między NATO a UE, jak wynika z koncepcji przyjętej w Madrycie, niezbędne jest jak najpełniejsze zaangażowanie państw spoza Unii w wysiłki obronne UE. NATO, w którym wiodącą rolę odgrywają USA, podkreśla konieczność wzmocnienia europejskich zdolności obrony, jednak tak, aby cechowały się one komplementarnością i interoperacyjnością z Sojuszem. Chodzi o wspieranie obustronnie korzystnych inicjatyw i unikanie niepotrzebnego dublowania działań, co ma być kluczem do zwiększenia bezpieczeństwa obszaru euroatlantyckiego, także w aspekcie przeciwdziałania zagrożeniom hybrydowym[344].

Podobnie jak w UE, podstawą działania w NATO w zakresie przeciwdziałania zagrożeniom hybrydowym jest świadomość sytuacyjna – wiedza o tym co się dzieje i wymaga reakcji. Za zbieranie i analizę informacji odpowiada od 2017 r. Komórka ds. Hybrydowych (ang. *Hybrid Analysis Branch*), która działa w kwaterze głównej NATO w ramach pionu wywiadowczego (ang. *Joint Intelligence and Security Division*).

Gotowość (zdolność) NATO do przeciwdziałania zagrożeniom hybrydowym jest uzyskiwana także poprzez szkolenia, ćwiczenia i ekspertyzę z obszaru obrony cywilnej czy ochrony infrastruktury krytycznej. Podstawowym instrumentem są tu przeprowadzane co dwa lata ćwiczenia CMX (ang. *Crisis Management Exercise*), które zawierają wątki hybrydowe.

Sojusz rozwija własne zdolności w zakresie przeciwdziałania zagrożeniom hybrydowym, zwłaszcza w zakresie komunikacji strategicznej (przeciwdziałanie

[342] W tej współpracy strategicznej chodzi także o przeciwdziałanie zagrożeniom cybernetycznym, wzrost mobilności wojskowej i odporności, powstające i destrukcyjne technologie (ang. Emerging and Disruptive Technologies, EDT), a także kwestie takie, jak uwzględnienie wpływu zmian klimatycznych na bezpieczeństwo czy agendy dotyczącej kobiet, pokoju i bezpieczeństwa.

[343] *NATO 2022 Strategic Concept…*

[344] Tamże.

dezinformacji, rzecznik, Public Diplomacy Division) i cyberbezpieczeństwa. Wspierają w tym sojusz dwa centra doskonałości: działające od 2008 r. w Estonii Centrum Doskonałości Cyberobrony NATO (ang. *NATO Cooperative Cyber Defence Centre of Excellence)* oraz zlokalizowane w 2014 r. na Łotwie Centrum Doskonałości Komunikacji Strategicznej NATO (ang. *NATO Strategic Communications Centre of Excellence*).

18 maja 2022 r. miało miejsce pierwsze spotkanie koordynatorów NATO ds. cybernetyki, którego tematem było strategiczne otoczenie po inwazji Rosji na Ukrainę i jego implikacje dla krajobrazu cyberzagrożeń. Dokonano również przeglądu postępów w dziedzinie cyberobrony, w tym wysiłków na rzecz zwiększenia odporności na zagrożenia w tej sferze (resilience to cyber threats). Uczestnicy zgodzili się, że istnieje pilna potrzeba zintensyfikowania podejścia do cyberobrony, a zbiorowy wysiłek oznacza również współpracę z sektorem prywatnym. Podkreślono, że cyberzagrożenia dla bezpieczeństwa Sojuszu są złożone, destrukcyjne, przymusowe i stają się coraz częstsze[345]. Zagrożenia hybrydowe w tym cyberbezpieczeństwo znalazły odzwierciedlenie w Koncepcji Strategicznej NATO przyjętej w Madrycie w 2022 r.

Istotnym elementem polityki NATO jest też przyjęcie w 2016 r. wskaźników bazowych dot. odporności, które określają jak organizacja i jej państwa członkowskie mają funkcjonować w przypadku kryzysu / zagrożenia. Chodzi tu głownie o zdefiniowanie usług, które muszą być zapewnione i dotyczą m.in. ciągłości działania infrastruktury krytycznej, transportu oraz zaopatrzenia.

Działania Sojuszu Północnoatlantyckiego w obszarze bezpieczeństwa cybernetycznego wspiera Centrum Doskonalenia Obrony Cybernetycznej NATO (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE) w Tallinnie. Powołane w 2008 r. centrum posiada status międzynarodowej organizacji wojskowej oraz akredytację NATO. Do zadań CCDCOE należy wspieranie poszczególnych państw członkowskich i partnerów NATO w zakresie rozwoju zdolności obronnych w obszarze bezpieczeństwa cybernetycznego[346]. Przeciwdziałanie zagrożeniom hybrydowym w tym wymiarze skupiało

[345] *First meeting of NATO national cyber coordinators*, NATO 18 May 2022, https://www.nato.int/cps/en/natohq/news_195493.htm [dostęp: 9.08.2022).

[346] Jest to dokonywane przez edukację, badania i rozwój oraz konsultacje. Centrum skupia 38 państw – 29 członków NATO (poza Macedonią Północną) oraz 9 państw partnerskich Sojuszu (Austria, Finlandia, Korea Południowa, Szwecja, Szwajcaria, Irlandia, Japonia, Ukraina i Nowa Zelandia).

się w ostatnich latach m.in. na śledzeniu botów, fałszywych kont czy nieautentycznych zachowań w mediach społecznościowych.

Sojusz Północnoatlantycki rozwija też ścisłą współpracę z partnerami w zakresie zagrożeń hybrydowych, w szczególności Finlandią, Szwecją, UE oraz Ukrainą. Płaszczyzną kooperacji była w ostatnich latach wymiana informacji oraz wzajemne wspieranie się zwłaszcza w przeciwdziałaniu cyberatakom. Jeśli chodzi o współpracę z Ukrainą działa Platforma NATO-Ukraina do spraw przeciwdziałania zagrożeniom hybrydowym, której pierwsze spotkanie odbyło się w 2017 r. w Warszawie. Polska była jednym z inicjatorów tego projektu mającego na celu wymianę informacji i doświadczeń w zakresie przeciwdziałania zagrożeniom hybrydowym z państwem niebędącym członkiem NATO. Platforma jest ukierunkowana na budowanie mechanizmu strategicznej oraz eksperckiej współpracy Paktu i Ukrainy w sprawach dotyczących zwalczania zagrożeń hybrydowych, m.in. poprzez organizowanie seminariów, wizyt studyjnych i eksperckich, sesji szkoleniowych, działalność badawczą. Utworzenie Platformy było jednym z głównych elementów Kompleksowego Pakietu Pomocowego dla Ukrainy (the Comprehensive Assistance Package CAP for Ukraine) z 2016 r. Platforma funkcjonuje na podstawie Karty o Szczególnym Partnerstwie NATO-Ukraina z 1997 r. (ang. *Charter on a Distinctive Partnership between NATO and Ukraine of 9 July 1997*).

Zespoły szybkiego reagowania w sprawie zagrożeń hybrydowych, które są dopiero planowane przez UE, w NATO funkcjonują od 2018 r. Podczas szczytu NATO w Brukseli w 2018 r. zdecydowano o możliwości powoływania – na wniosek zagrożonego członka Sojuszu – misji eksperckich Zespołów Przeciwdziałania Zagrożeniom Hybrydowym W listopadzie 2019 r. tego rodzaju zespół został po raz pierwszy wysłany do Czarnogóry, a w 2021 r. – na Litwę. Działanie to charakteryzuje się szybkim tempem proceduralnym. W przypadku Litwy, poczuła się ona zagrożona hybrydową aktywnością Białorusi eskalującej sztucznie wytworzony konflikt graniczny z użyciem migrantów. Wniosek został złożony w sierpniu 2021 r., a już na początku września tego samego roku zespól został rozmieszczony na terenie litewskim.

Instrumentarium NATO do spraw przeciwdziałania zagrożeniom hybrydowym jest skromniejsze niż w UE z uwagi na koncentrację tego wojskowego sojuszu na obronie przed zagrożeniami konwencjonalnymi. Natomiast świadomość o nowych zagrożeniach rośnie i są

podejmowane próby częściowego przekierowania zasobów sojuszniczych na zwalczanie zagrożeń hybrydowych. Jest kilka forów, gdzie takie prace koncepcyjne są prowadzone. Jednym z nich jest Komitet zastępców stałych przedstawicieli (DPRC, prace nad Non-military instruments of power), który porusza się w wymiarze politycznym NATO, instrumentów ekonomicznych i dyplomacji publicznej. Jest to miejsce gdzie NATO najczęściej dyskutuje o zagrożeniach hybrydowych.

UE współpracuje z NATO w 74 obszarach. Jednym z nich jest sfera zagrożeń hybrydowych. Współpraca ta odbywa się w zakresie wymiany informacji oraz doraźnych projektów i inicjatyw. Wyrazem tej kooperacji są m.in. wspólne deklaracje (z roku 2016 i 2018). Zawarto w nich propozycje działań, z których wiele odnosi się do zagrożeń hybrydowych, odporności, bezpieczeństwa cybernetycznego i komunikacji strategicznej. Efektem tych deklaracji są m.in. Ćwiczenia PACE (ang. *Parallel and Coordinated Exercise*), polegające na realizacji możliwych odpowiedzi na scenariusze zagrożeń hybrydowych (obie organizacje przeprowadzają je oddzielnie ale według ujednoliconych wytycznych). Innym efektem tej współpracy jest powołanie Europejskiego Centrum Doskonalenia w dziedzinie zwalczania zagrożeń hybrydowych z siedzibą w Helsinkach – Hybrid CoE. Zarówno UE, jak i NATO korzystają z zasobów tego centrum.

Podsumowując, zarówno UE, jak i NATO korzystają ze swoich zasobów, aby przeciwdziałać zagrożeniom hybrydowym wymierzonym w państwa członkowskie. Cześć inicjatyw została już wdrożona, a kolejne są w fazie planowania. Ta polityka i instrumenty są tworzone w reakcji na zagrożenia/wydarzenia. Jednocześnie, świadomość skali wyzwań powodowanych przez zagrożenia hybrydowe systematycznie rośnie. Państwa członkowskie skupione w obu organizacjach agregują dane wywiadowcze, dzięki czemu wiedzą coraz więcej o zagrożeniach hybrydowych i mogą skuteczniej im przeciwdziałać. Jednak wobec ciągłej i szybkiej ewolucji zagrożeń hybrydowych następuje ewolucja reagowania na nie ze strony zaprezentowanych wcześniej organizacji. Przeciwdziałanie zagrożeniom hybrydowym wymaga dalszych prac koncepcyjnych, zmian instytucjonalnych, legislacyjnych, zacieśnienia współpracy instytucji i państw członkowskich.

NATO i UE postrzegają zagrożenia hybrydowe w podobny sposób, kładąc nacisk na ich specjalny charakter wynikający ze połączenia skoordynowanych działań militarnych i niemilitarnych realizowanych bezpośrednio lub za pomocą aktorów państwowych

(z państw trzecich) i niepaństwowych. Wyzwania stwarzane przez działania hybrydowe wynikają m.in. z ich wielowymiarowości, utajnienia (trudność wykrycia i atrybucji odpowiedzialności) oraz destrukcyjnej siły względem funkcjonowania aparatu państwowego oraz społeczeństwa (zahamowanie procesów decyzyjnych, zakłócanie dostaw energii czy usług finansowych, paraliżowanie łączności – w tym satelitarnej GPS, uderzenia w słabe punkty, czynnik dezorientujący, podważanie zaufania społecznego do instytucji rządowych, pogłębianie podziałów społecznych np. na tle politycznym lub narodowościowym)[347]. Trzeba odnotować także operacje kinetyczne, w postaci możliwości użycia nieoznakowanych żołnierzy do opanowania danego terytorium lub zniszczenia istotnego obiektu (np. elektrowni, instalacji infrastruktury krytycznej), korumpowanie lub fizyczna eliminacja (zabójstwa) niewygodnych polityków, dziennikarzy i decydentów, wywołanie kryzysu politycznego w innych państwach lub organizacja zamachów stanu[348].

Unijne i natowskie przedsięwzięcia i współpraca dotycząca przeciwdziałania zagrożeniom hybrydowym nie ograniczają się tylko do sfery teoretycznej czy biurokratycznej, ale mają wymiar realnych działań i ich efektów obu organizacji. Jednym z nich jest komunikacja strategiczna. Współpracujący z ekspertami natowskimi unijny Wydział Komunikacji Strategicznej UE (StratCom) aktywnie zwalcza dezinformację. Kolejnym stosowanym narzędziem przeciwdziałającym zagrożeniom hybrydowym (głownie cyberatakom) są sankcje, które mają zniechęcać agresorów (prym wiedze tu przede wszystkim UE). Analizy wywiadowcze UE i NATO, które polegają na zbieraniu informacji od państw członkowskich i budowaniu szerszego obrazu zagrożeń hybrydowych niż ten, którym dysponują poszczególni członkowie. Istotne znaczenie mają także narzędzia do samooceny (unijny kwestionariusz zagrożeń hybrydowych) oraz wypracowane przez NATO wskaźniki odporności, które pomagają zlokalizować słabe punkty w systemie bezpieczeństwa. Zespoły szybkiego reagowania NATO umożliwiają faktyczną reakcję na zagrożenie hybrydowe względem kraju członkowskiego. Na drodze do utworzenia podobnych zespołów jest także UE.

Z uwagi na obserwowany w ostatnich latach w Europie wzrost znaczenia kwestii przeciwdziałania zagrożeniom hybrydowym w postaci dezinformacji, jednostki do spraw

[347] P. Szymański, op. cit.
[348] Tamże.

komunikacji strategicznej (StratCom) są rozwijane w większości państw UE. Tempo tych działań jest jednak różne. Skuteczne przeciwdziałanie zagrożeniom hybrydowym w omawianym obszarze wymaga przeznaczenia znacznych nakładów na specjalistów oraz wzmocnienie kompetencji struktur w jakich oni funkcjonują. W jednych z najbardziej znaczących gospodarczo i politycznie krajach UE (Niemcy, Francja, Hiszpania), ze względu na dużą wagę, jaką w rozwiązaniach krajowych nadano kwestiom przeciwdziałania dezinformacji, jednostki StratCom są usytuowane w kancelarii prezesa rady ministrów. Brak podobnego rozwiązania w Polsce, w postaci centralnej struktury koordynującej w ramach administracji, obniża skuteczność działań w zakresie skoordynowanego przeciwdziałania fałszywym narracjom. Utworzenie stałej komórki do spraw komunikacji strategicznej w KPRM o kompetencjach koordynujących oraz wzmocnienie istniejących struktur i zespołów zajmując się przeciwdziałaniem dezinformacji (m.in. w Ministerstwie Spraw Zagranicznych) usprawniłoby przeciwdziałanie zagrożeniom hybrydowym.

Doświadczenia Szwecji i Finlandii, które proaktywnie podejmują działania na rzecz przeciwdziałania zagrożeniom hybrydowym i szerzej rozumianego przygotowania społeczeństwa do zagrożenia bezpieczeństwa (regularne przygotowanie kampanii informacyjnych i szkoleń przez władze szwedzkie, fińska koncepcja całościowego bezpieczeństwa), powinny zostać wykorzystane przez Polskę. Strona polska wykorzystuje już cześć z tych rozwiązań. Większa regularność oraz planowanie niewątpliwie przyczyniłyby się do poprawy poziomu bezpieczeństwa w zakresie przeciwdziałania zagrożeniom hybrydowym. W 2022 r. z Rządowe Centrum Bezpieczeństwa wydało broszurę "Bądź gotowy - poradnik na czas kryzysu i wojny", w którym w wyjaśniono, jak przygotować się do funkcjonowania/działania w sytuacji kryzysowej oraz co zrobić, by uniknąć zagrożenia i jak się zachować podczas jego wystąpienia. Mankamentem był w tym przypadku czas tej publikacji, który nastąpił już po rozpoczęciu operacji / agresji rosyjskiej na Ukrainie. Taki poradnik powinien być uzupełniony kampanią informacyjną, która zachęca polskie społeczeństwo (złącza w gronie rodziny) do omawiania możliwości reagowania na zagrożenia i wypracowywania na swój prywatny użytek rekomendowanych metod działania[349].

[349] *Wzmacnianie odporności, jako kluczowa metoda przeciwdziałania zagrożeniom hybrydowym – odporność w NATO, UE i lessons learned z wybranych państw,* prezentacja w ramach seminarium online pt.

Nowe zagrożenia wynikają także z reorganizacji życia społecznego i zawodowego, które dokonano w wyniku pandemii. Dostęp coraz większych rzesz pracowników do większej ilości systemów informacji stanowi jeden z takich obszarów ryzyka. Pandemia COVID-19 wiązała się z transformacją stylu pracy w kierunku zwiększonego wykorzystania narzędzi cyfrowych. Przyspieszyło to transformację w zakresie cyfryzacji w postaci przejścia na pracę zdalną wielu zakładów i instytucji. Wzrosło tym samym znaczenie cybernetycznego wymiary zagrożeń hybrydowych, co wynikało ze wzrostu incydentów oraz wrogich ataków na państwa członkowskie. Istniejące problemy/incydenty związane z cyberbezpieczeństwem ulegną pogłębieniu w miarę obserwowanego coraz intensywniejszego stymulowania zmian społecznych sprzyjających digitalizacji praktycznie wszystkich dziedzin życia. Poziom zaawansowania cyberprzestępców jest według ekspertów wyższy niż państwowych służb odpowiedzialnych za bezpieczeństwo. Innowacje i konieczność przewidywania kolejnego kroku wroga (w przypadku cyber – hakerów) należą do wyzwań w zakresie przeciwdziałania zagrożeniom hybrydowym. Aby im sprostać firmy powinny zapewnić stosowane protokołów bezpieczeństwa wśród swoich załóg oraz w kontaktach z partnerami handlowymi[350].

W sektorach o kluczowym znaczeniu jak bankowość zabezpieczenie systemu pod kątem cyberzagrozeń ma szczególne znaczenie. UE w dużym stopniu opiera się na systemie cyfrowym dla wzajemnej wymiany gospodarczej, dlatego niektórzy eksperci wskazują, że rozwiązania prawne i standardy wzmacniające unijne bezpieczeństwo cybernetyczne powinny być obowiązkowo wprowadzane przez państwa członkowskie. Jak wskazuje cześć ekspertów UE potrzebuje wspólnej jednostki ds. cyberbezpieczeństwa. Ponadto, przyjmuje się holistyczne podejście w zakresie czterech głównych obszarów cyberbezpieczeństwa (ang. *cyber domains*): relacje zewnętrzne, cyberobrona, cyberprzestępczość i bezpieczeństwo sieciowe (ang. *Network Information Security*).

Wyzwanie w postaci braku pełnego zaufania pomiędzy państwami członkowskimi UE stwarza problem systemowy. Nawet zarządzane autorytarnie kraje mają ograniczoną swobodę decyzyjną w kwestiach bezpieczeństwa. Na pewno jednak jest ten proces szybszy niż w UE. Procesy decyzyjne w UE powinny zostać usprawnione, przyspieszone. Unia stoi przed

*Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

[350] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

wyzwaniem wypracowania szybszej ścieżki decyzyjnej, ale powinno się to zapewnić przy zachowaniu kompetencji państw narodowych w dziedzinie bezpieczeństwa.

Pomimo faktu opuszczenia przez Wielką Brytanie struktur UE, kraj ten przez dziesięciolecia uczestniczył w wypracowywaniu unijnych polityk, dlatego warto przywołać jego doświadczenia w zakresie przeciwdziałania zagrożeniom hybrydowym – dezinformacji. Ponadto, Wielka Brytania odznacza się długoterminowym (i – jak pokazuje historia – skutecznym) planowaniem umacnianiem swojego bezpieczeństwa, co także przemawia na korzyść analizy rozwiązań wprowadzanych przez władze w Londynie.

Na długo przed incydentem związanym z próbą otrucia Siergieja Skripala w 2018 r., w Wielkiej Brytanii wzrastała świadomość braku spójnej, narodowej strategii przeciwdziałania zagrożeniom hybrydowym, a zwłaszcza dezinformacji. Stwierdzono, że to nie tylko problem polityczny czy komunikacyjny. Konieczne było całościowe podeście i wypracowanie strategii ogólnokrajowej oraz zidentyfikowanie luk instytucjolano-prawnych (w celu m.in. umożliwienia skazywania osób szerzących dezinformację). W tym kontekście, pojawia się problem z interpretacją i zakresem treści, które dany rząd uznaje za dezinformację (sprawa wolności wypowiedzi i rzetelności przekazu publicznego). Poprawa systemu musi następować wraz ze wzrostem i ewolucją zagrożenia.

Walkę z dezinformacją rozpoczęto z konsekwencją na wszystkich kanałach informacyjnych: cyfrowych i analogowych. Zauważono, że niektóre media rozpowszechniające dezinformację robiły to nieświadomie. W przypadku części osobowości internetowych mających znaczące grono odbiorców, eksperci brytyjscy stwierdzili, że wierzą oni w prawdziwość określonych narracji i rozpowszechniają je w dobrej wierze. Stwarzało to duże zagrożenie z uwagi na znaczącą siłę oddziaływania kanałów internetowych prowadzonych przez te osoby. Niektóre przypadki dezinformacji postanowiono tylko monitorować, inne – niosące większe niebezpieczeństwo – aktywnie zwalczać. Za główny cel obrano walkę z narracjami sprzyjającymi Rosji i Chinom, ale także Iranowi[351].

Ponadto, zaniepokojone faktem upubliczniania różnych ocen na temat koronawirusów, władze brytyjskie powołały w 2020 r. specjalną komórkę, która miała przeciwdziałać dezinformacji w Internecie na ten temat. Ten zespół szybkiego reagowania,

[351] Prezentacja o przeciwdziałaniu dezinformacji w Wielkiej Brytanii w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

składający się z przedstawicieli rządu i sektora prywatnego, współpracował z firmami technologicznymi, aby zidentyfikować i zablokować „fałszywe narracje" w mediach społecznościowych. Zespół współpracował ze specjalistami od dezinformacji z tzw. społeczeństwa obywatelskiego (m.in. rozmaite fundacje) i środowisk akademickich wykrywając do 70 incydentów tygodniowo. Był to przykład działania ukierunkowanego na zwalczanie dezinformacji przez władze brytyjskie w ramach Departamentu Cyfryzacji, Kultury, Mediów i Sportu[352].

Ponadto, brytyjski rząd powołał Jednostkę ds. Komunikacji Bezpieczeństwa Narodowego (National Security Communications Unit), której zadaniem jest zwalczanie dezinformacji rozpowszechnianej przez podmioty państwowe i inne. Do decyzji tej przyczyniło się wykrycie przypadków ingerencji w referendum w sprawie Brexitu latem 2016 r., o które władze w Londynie oskarżyły Rosję. Był on częściowo wzorowany na utworzonym w 1948 r. w celu przeciwdziałania sowieckiej propagandzie Departamencie Badań nad Informacją brytyjskiego resortu spraw zagranicznych[353].

Podejście brytyjskie uwzględnia analizę trendów społecznych, które nasilają efekty dezinformacji. Przy priorytetyzacji uwzględnia się wpływ na odbiorców w przypadku braku podjęcia skutecznych środków zaradczych (marginalny, średni lub znaczący). Ważnym działaniem agencji przeciwdziałających dezinformacji pozostaje nie tylko wskazywanie fałszywych narracji, ale wskazanie pożądanego z punktu widzenia bezpieczeństwa narodowego obrazu rzeczywistości. W ten sposób zastępuje się przekaz uznany za dezinformację właściwym, odpowiadającym celom władz w Londynie[354].

3.3. Zarys metod zwalczania zagrożeń hybrydowych w Izraelu, Australii i Nowej Zelandii

W świetle wyników przeprowadzonych badań należy stwierdzić, że metody zwalczania zagrożeń hybrydowych stosowane przez niektóre państwa, w tym Izrael, Australię i Nową Zelandię, dostarczają cennych wskazówek w zakresie kształtowania polskiego systemu bezpieczeństwa narodowego w tym zakresie.

[352] Tamże.
[353] Tamże.
[354] Tamże.

Izrael jest przykładem kraju, który od dekad zmaga się nie tylko ze znaczącymi konfliktami zbrojnymi (wojnami), ale także z zagrożeniami hybrydowymi. Te ostatnie, choć często występują w postaci zamachów terrorystycznych, są w wielu przypadkach efektami działań hybrydowych wymierzonych w Izrael. Organizacje muzułmańskich bojowników otrzymują bowiem wsparcie od podmiotów państwowych. Państwa, z którymi strona izraelska ma napięte relacje, są oskarżane przez rząd w Tel Awiwie o wspieranie działalności organizacji terrorystycznych. Wśród czterech głównych zagrożeń dla swojego bezpieczeństwa Izrael definiuje Iran[355], palestyński terroryzm oraz działalność dwóch organizacji parapaństwowych uznawanych za terrorystyczne: Hamas (rządzi w Strefie Gazy od 2007 r.)[356] i – wspierany przez stronę irańską – Hezbollah.

W swojej historii Izrael regularnie stawał w obliczu poważnych zagrożeń – także hybrydowych – a jego ludność narażona była na ryzyko zamachów terrorystycznych, ostrzałów rakietowych i innych form ataków. Cechą charakterystyczną, która z tego wynika, jest wysoka świadomość zagrożeń wśród obywateli, ponieważ społeczeństwo żyje w poczuciu stałego niebezpieczeństwa (wzmacnianego pamięcią o zagładzie Żydów w czasie drugiej wojny światowej. Tym tłumaczyć można centralne miejsce i podporządkowanie wielu sfer życia sprawom bezpieczeństwa narodowego, ogromne zaufanie społeczne do armii, akceptacja powszechnej służby wojskowej, a także szczególne obostrzenia w przestrzeni publicznej[357]. Sama niepodległość Izraela była, od jego powstania, zagrożona przez wrogie nastawienie sąsiednich krajów arabskich, które dążyły do jego zniszczenia. W czasie wojny Jom Kippur w 1973 r. wojska egipskie i syryjskie przypuściły atak z zaskoczenia. Ryzyko porażki Izraela zostało odsunięte, ale było wówczas bardzo

[355] Izrael okresowo zapowiada możliwość prewencyjnego uderzenia na Iran w związku z rozwojem programu atomowego w tym kraju. Taki krok, może doprowadzić do wybuchu kolejnej wojny na Bliskim Wschodzie, której rozwój trudno przewidzieć dla samego Izraela. Największy przeciwnik polityczny dla strony izraelskiej, Iran, dysponuje znacznie większą populacją oraz terytorium niż Izrael. Iran ma największą armię na Bliskim Wschodzie, liczącą prawie 1 milion żołnierzy (534 tys. wojsk regularnych oraz 400 tys. rezerwy) wspieranych przemysłem obronnym (m.in. drony wykorzystane przez Rosję na Ukrainie w 2022 r.) rozbudowywanymi zdolnościami nuklearnymi. *Izrael czy Iran? Kto dysponuje większą siłą militarną?,* Rzeczpospolita 07.06.2018, https://www.rp.pl/konflikty-zbrojne/art9762901-izrael-czy-iran-kto-dysponuje-wieksza-sila-militarna [dostęp:7.12.2022].

[356] Hamas odmawia uznania Izraela i opowiada się za jego zniszczeniem, a Izrael postrzega Hamas jako organizację terrorystyczną, którą należy rozbroić.

[357] M. Matusiak, *Paradoksy izraelskiej polityki. Krótki kurs*, Ośrodek Studiów Wschodnich im. Marka Karpia, 2022-09-27, https://www.osw.waw.pl/sites/default/files/PW_87_Paradoksy%20izraelskiej%20polityki_net_0.pdf [dostęp: 13.12.2022], s. 19-20.

poważne. Władze izraelskie były świadome konieczności posiadania znacznie silniejszych sił zbrojnych, niż mogłyby na to wskazywać rozmiary tego państwa. Chodziło nie tylko o ich liczebność, ale przede wszystkim siłę ognia, wyszkolenie oraz uzupełnienie w postaci wydatnego wsparcia sojuszniczego ze strony tradycyjnie przychylnych Izraelowi Stanów Zjednoczonych, Wielkiej Brytanii i innych znaczących globalnie państw (często z aktywnym udziałem diaspory żydowskiej w tych krajach). Ważnym elementem walki z hybrydowymi przeciwnikami były także zdolności wywiadowcze i sił specjalnych, które często stosowano łącznie w różnego rodzaju operacjach w kraju i za granicami.

Specyfika izraelskiej polityki, jak wykazały wyniki badań, w dużym stopniu miała wpływ na bezpieczeństwo tego kraju. Izrael to, państwo rozwinięte, dostatnie, wpływowe na arenie międzynarodowej i silne militarnie. Zarazem jednak tamtejsze życie polityczne sprawia wrażenie, jak dowodzi Marek Matusiak, jakby stale znajdowało się w kryzysie albo o krok od niego. Normą są przedterminowe wybory, rozdrobnione parlamenty, krótkotrwałe koalicje, efemeryczne ugrupowania, natłok liderów, skandale kryminalne oraz prowizoryczne rozwiązania prawne – a wszystko to w warunkach niemal ciągłej kampanii wyborczej przynoszącej wciąż nowe impulsy do zmian[358].”

Spójność narodowa oraz umiejętność politycznego współdziałania w zakresie realizacji celów w polityce zagranicznej i bezpieczeństwa jest tym co wyróżnia współczesne państwo żydowskie. Cechy te, jak wykazały wyniki badań, są czynnikami generującymi skuteczne podejście władz w Tel Awiwie do przeciwdziałania zagrożeniom hybrydowym oraz innym zagrożeniom dla bezpieczeństwa narodowego. Zagrożenie zewnętrzne oraz silna tożsamość narodowa, jak dowodzi Marek Matusiak, sprawiają, że – w Izraelu, „pomimo ogromnej mozaikowości światopoglądowej, bardzo ostrych sporów oraz nietrwałości rządów – w wielu newralgicznych dziedzinach istnieje duży potencjał do kreatywnego konsensusu. Dotyczy to zwłaszcza kwestii bezpieczeństwa oraz głównych założeń polityki zagranicznej, gospodarczej czy historycznej, ale również zagadnienia etnicznie żydowskiego charakteru Izraela[359].” Konsensus ten, pomimo wielu trudności w polityce wewnętrznej, pozwala zabezpieczyć długoterminowe interesy Izraela, w tym w zakresie bezpieczeństwa narodowego.

[358] Tamże, s. 7.
[359] Tamże.

Na zdolność Izraela do zjednoczenia się ponad podziałami w obliczu stałego zagrożenia zwrócił uwagę m.in. premier Ja'ir Lapid, w ocenie którego „głęboką prawdą na temat Izraela jest to, że w odniesieniu do spraw naprawdę ważnych – wierzymy w to samo[360]." Takie podejście, po części wynika z efektu jednoczącego społeczeństwo, który wynika z zagrożenia arabskiego. Ważną rolę należy jednak przypisać przede wszystkim instytucjom odpowiedzialnym za bezpieczeństwo, które skutecznie wypełniają misję przeciwdziałania obcym wywiadom tradycyjnie starającym się dzielić narody krajów obranych za cel. Jak kontynuował autor, „na utrzymanie tej minimalnej spójności – szczególnie w zakresie polityki zagranicznej i bezpieczeństwa – wpływa wiele czynników, m.in. silna tożsamość narodowa i głęboko przeżywana wspólnota losu, w tym zjednoczenie w poczuciu zagrożenia. Z pewnością sprzyjają jej także powszechna służba wojskowa oraz tradycyjna obecność w elitach władzy wielu byłych oficerów. Owa spójność jest również pokłosiem imperatywu propaństwowości (hebr. mamlachtijut), który przenikał izraelską politykę w pierwszych dekadach po uzyskaniu niepodległości i nakazywał podporządkowanie partykularnych interesów potrzebom państwa[361]."

Izraelskie zdolności obronne rozwijano w sposób systemowy od powstania struktur tego państwa. Tworzenie Sił Obronnych Izraela (hebr. CaHaL – Cwa Hagana L-Israel) w bardzo szybkim tempie w czasie wojny o niepodległość w 1948 r. było możliwe, ponieważ proces ten oparto na już istniejących nacjonalistycznych, żydowskich organizacjach paramilitarnych (m.in. Hagany, Legionu Żydowskiego), których bojownicy wspierali w przeszłości m.in. armie państw zachodnich[362].

Siły zbrojne Izraela, które rozpoczęto formować zaledwie dwa tygodnie po ogłoszeniu przez to państwo niepodległości, były budowane z uwzględnieniem potrzeb obronnych wynikających z bardzo zaognionej sytuacji w regionie. Armie wrogo nastawionych do władz w Tel Awiwie sąsiadów znacząco przewyższały Izrael liczebnie. Dlatego, podstawowym elementem doktryny obronnej stało się założenie, że Izrael nie mógł przegrać ani jednej wojny. Uznano, że cel ten można było osiągnąć jedynie poprzez

[360] Tamże, s. 18.

[361] Tamże.

[362] Większość z nich, podobnie jak inne ruchy narodowowyzwoleńcze – w tym – polskie, stosowała w przeszłości metody terrorystyczne w celu wywalczenia sobie niepodległego państwa. *Siły obronne Izraela*, Konflikty.pl 19.11.2006 https://www.konflikty.pl/technika-wojskowa/na-ladzie/sily-obronne-izraela/ [dostęp:7.12.2022].

zagwarantowanie zdolności do szybkiej mobilizacji przytłaczającej siły ognia, co umożliwi uzyskanie przewagi, zepchnięcie wroga (lub kilku wrogów) i prowadzenie wojny na jego/ich terytorium[363].

Od czasu ogłoszenia niepodległości Izrael toczył wojny, w których poległo kilkanaście tysięcy tamtejszych żołnierzy. Oprócz tego państwo to przeprowadziło liczne operacje zbrojne na obszarze Strefy Gazy oraz doświadczyło dwóch powstań palestyńskich (intifady). Wśród przeciwników Izraela były m.in.: Egipt, Syria, Jordania, Irak, Organizacja Wyzwolenia Palestyny, Hezbollah i Hamas. Islamska Republika Iranu, jak odnotowuje M. Matusiak, przez dziesięciolecia prowadziła z Izraelem wojnę zastępczą otwarcie dążąc do jego fizycznego unicestwienia za pomocą wspieranych przez siebie państw i organizacji[364].

Izraelskie siły zbrojne, mimo że nie są tak liczne jak irańskie (największy wróg Izraela), a tym bardziej – połączonych państw arabskich w regionie, dysponowały bardziej zaawansowanym sprzętem. Wyższe było też morale żołnierzy. Izraelczycy mieli świadomość, że porażka wojenna może oznaczać kres ich państwowości. Izrael, w celu wyrównania swoich szans z przeciwnikami z państw arabskich, dążył przez lata do wytworzenia potencjału wojskowego porównywalnego do połączonych armii Egiptu, Syrii i Jordanii[365]. Wydatki na obronność Izraela wynosiły ponad 5% PKB tego kraju. Izrael, co ujawniły prace badawcze, posiadał znaczący przemysł zbrojeniowy zapewniający uzbrojenie na potrzeby wewnętrzne oraz eksport broni na rynki zagraniczne. Kraj otrzymywał ponadto wysoką pomoc wojskową ze Stanów Zjednoczonych. W zakresie bezpieczeństwa i obrony Izrael ściśle współpracował ze Stanami Zjednoczonymi, co przejawiało się m.in. wspólnymi ćwiczeniami wojskowymi, wymianą informacji wywiadowczych oraz kooperacją w badaniach i rozwoju nowych rodzajów broni[366].

Jak wykazały wyniki badań,, w kontekście potrzeb obronnych Izraela, jego siły zbrojne składały się ze stosunkowo niewielkiej liczby żołnierzy w czynnej służbie. Mniej więcej dwie trzecie z nich stanowili poborowi. Co więcej, utrzymanie dobrze wyszkolonych sił

[363] *Israel Defense Forces, Encyclopedia* Britannica, 20 Oct. 2022, https://www.britannica.com/topic/Israel-Defense-Forces [dostęp: 14.12.2022].
[364] M. Matusiak, op. cit., s. 18.
[365] Ł. Pacholski, A. Rokosz, *Siły zbrojne Izraela*, Defence 24, 17.11.2012 https://defence24.pl/sily-zbrojne/sily-zbrojne-izraela [dostęp:7.12.2022].
[366] Tamże.

rezerwy stanowiło kluczowy element podejścia obronnego. Uzupełniały go inne środki, w tym m.in.: aktywne pozyskiwanie informacji wywiadowczych, zaawansowane systemy wczesnego ostrzegania, jedne z najbardziej zaawansowanych na świecie systemów obrony przeciwrakietowej oraz wojska zmechanizowane (około 2500 czołgów podstawowych i ponad 5000 transporterów opancerzonych)[367]. Ponadto, służba wojskowa była obowiązkowa dla każdego pełnoletniego obywatela (od 18 lat), dlatego obywatele Izraela posiadali w większości przeszkolenie wojskowe.

Jak wykazały wyniki badań, od początków kształtowania się państwowości Izraela, kraj ten wydawał znaczną część swojego produktu krajowego brutto na obronność w latach 1980 było to nawet prawie 25% PKB. Wydatki obronne Izraela rozpoczęto obniżać po podpisaniu traktatów pokojowych z Egiptem i Jordanią, ale nadal należały one do najwyższych na świecie. Według raportu sztokholmskiego instytutu SIPRI na temat światowych wydatków zbrojeniowych w 2021 r., wydatki Izraela wyniosły 24,3 miliardy USD (niewiele mniej niż Iranu – 24,6 miliarda USD), co dało temu krajowi piętnaste miejsce w skali globalnej. Izrael , przeznaczający na zbrojenia 5,2% PKB, wydał więcej niż m.in. Polska, Turcja, Brazylia, Hiszpania, Tajwan, Szwecja i Norwegia. Łącznie, wydatki wojskowe na Bliskim Wschodzie wyniosły w 2022 r. 186 miliardy USD. Sześć spośród 10 krajów o największym udziale wydatków wojskowych w PKB znajduje się na Bliskim Wschodzie: Oman (7,3% PKB), Kuwejt (6,7% PKB), Arabia Saudyjska (6,6% PKB), Izrael (5,2% PKB), Jordania (5% PKB) i Katar (4,8% PKB)[368].

Na potencjał obronny personelu wojskowego i służb bezpieczeństwa Izraela składa się około 173 000 personelu czynnej służby (130 000 wojsk lądowych, 9 000 marynarki wojennej i 34 000 sił powietrznych)[369]. Powszechny charakter obrony, gdzie zdecydowana większość społeczeństwa odbywa trwającą do 2,5 roku obowiązkową służbę wojskową, jest cechą charakterystyczną sposobu przeciwdziałania zagrożeniom – także hybrydowym – przez Izrael.

---

[367] *Israel Defense Forces,* Encyclopedia Britannica, 20 Oct. 2022, https://www.britannica.com/topic/Israel-Defense-Forces [dostęp: 14.12.2022].

[368] *Trends in world military expenditure 2021*, SIPRI 2022 https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf [dostęp: 10.12.2022].

[369] *Israel*, The World Factbook, CIA 2022 https://www.cia.gov/the-world-factbook/countries/israel/#military-and-security [dostęp: 18.12.2022].

Siły lądowe posiadały wysoki współczynnik zmechanizowania będąc wyposażone w ponad 3,5 tys. czołgów i 11 tys. transporterów opancerzonych[370]. Podstawowymi jednostkami bojowymi wojsk lądowych były brygady, a ich dowódcy dysponowali stosunkowo wysoką autonomią decyzyjną. Jak wykazały wyniki badań, siły powietrzne Izraela należały do najlepszych na świecie pod względem zarówno wyszkolenia pilotów, jak i sprzętu (wśród ok. 250 myśliwców znajdowały się najnowocześniejsze na świecie amerykańskie myśliwce piątej generacji F-35 Lightning II)[371]. Marynarka wojenna Izraela zapewniała z kolei bezpieczeństwo wybrzeża, którego linia brzegowa liczy łącznie 272 kilometry[372]. Siły morskie dysponowały trzema bazami morskimi (Hajfa, Ashdod i Ejlat), z których największe znaczenie miała położona nad Morzem Śródziemnym baza w mieście Hajfa. Stacjonowała tam większa część floty. Izrael dysponował 8. okrętami rakietowymi, 3. korwetami, 45. łodziami patrolowymi oraz 5 okrętami podwodnymi. Dla porównania, Iran posiadał ponad 30 okrętów podwodnych, pięć fregat, trzy korwety i ponad 200 łodzi patrolowych[373].

Służba wojskowa w Izraelu, co ujawniły prace badawcze, opierała się na połączeniu armii zawodowej i żołnierzy z poboru[374]. Stanowiła ona formę milicji obywatelskiej, która jest uzupełniona przez stosunkowo nieliczny korpus oficerów zawodowych[375]. Izraelskie siły obronne, mimo posiadania komponentu wojsk zawodowych, były w dużym stopniu uzależnione od służby rezerwowych. To one zapewniały większość siły wojsk lądowych. Poborowi stanowili około 70% izraelskich sił lądowych (2021 r.).

---

[370] Ł. Pacholski, A. Rokosz, op. cit.

[371] *Izrael czy Iran? Kto dysponuje większą siłą militarną?,* Rzeczpospolita 07.06.2018 https://www.rp.pl/konflikty-zbrojne/art9762901-izrael-czy-iran-kto-dysponuje-wieksza-sila-militarna [dostęp:7.12.2022].

[372] Z czego 263 km znajduje się nad Morzem Śródziemnym, a pozostałe 9 km nad Morzem Czerwonym. Ł. Pacholski, A. Rokosz, op. cit.

[373] Ponadto, Iran dysponuje wsparciem antyizraelskich organizacji paramilitarnych na Bliskim Wschodzie w postaci m.in. Hezbollahu i Hamasu. *Izrael czy Iran? Kto dysponuje większą siłą militarną?...*

[374] Jeśli chodzi o szczegóły poboru oraz przebiegu służby wojskowej, armia „gwarantuje każdemu możliwość uzyskania średniego wykształcenia przed odbyciem służby. Jeśli kandydat dostanie się na studia, otrzymuje indeks, który jest zamrażany na czas odbycia służby. Istnieje także możliwość odsłużenia wymaganego czasu po ukończeniu studiów. (…) Zwolnienia ze służby z powodów zdrowotnych lub innych są rzadkością. Służba nie obowiązuję jedynie ortodoksyjnych żydów studiujących w szkołach religijnych, około kilkaset osób." Ł. Pacholski, A. Rokosz, op. cit. https://defence24.pl/sily-zbrojne/sily-zbrojne-izraela [dostęp:7.12.2022].

[375] *Israel Defense Forces,* Encyclopedia Britannica…

W toku badań stwierdzono, że każdy Izraelczyk musiał zgłosić się do czynnej służby wojskowej na obowiązkowy okres czasu, który wynosił 32 miesiące dla mężczyzn i 24 miesiące dla kobiet. Po odsłużeniu 2-2,5 roku wszystkie takie osoby były kierowane do obowiązkowej rezerwy (do 50 roku życia dla kobiet i 55 roku życia dla mężczyzn)[376]. W sytuacji kryzysu lub wojny zostawały one powołane z powrotem do czynnej służby w trybie pilnym. Wiek 17 lat umożliwiał zgłoszenie się na ochotnika do służby wojskowej. Żydów i Druzów wcielano do wojska obowiązkowo. Natomiast Chrześcijanie i Muzułmanie nie są objęci obligatoryjną służbą, ale mogli zgłaszać się na ochotnika[377].

W trakcie badań stwierdzono, że w sposób szczególnie dokładny ścigane były wszelkie przypadki zdrady, ujawnienia informacji niejawnych lub złamania przepisów bezpieczeństwa narodowego. Znana była historia skazania na 18 lat pozbawienia wolności byłego pracownika izraelskiego ośrodka atomowego Mordechaja Vanunu, który sprzedał zdjęcia tajnych obiektów nuklearnych mediom („The Sudany Times"). Pojmano go w wyniku zakrojonych na szeroką skalę poszukiwań prowadzonych w różnych miejscach na świecie z udziałem izraelskich instytucji, służb i formacji[378]. Ponadto, w kraju bardzo poważnie podchodziło się do edukacji i zwiększania świadomości społecznej na temat zagrożeń związanych ze sferą hybrydową (m.in. dezinformacją). Stosowane były kampanie odwołujące się do emocji patriotycznych obywateli (jedno z haseł głosiło: „twoja gadatliwość może narazić na śmierć twoje dziecko, lub dziecko twoich sąsiadów")[379].

W rezultacie badań należy stwierdzić, że forma organizacji politycznej oraz struktura kierowania systemem bezpieczeństwa i obrony Izraela miała duże znaczenie dla zdolności przeciwdziałania zagrożeniom hybrydowym tego państwa. Dowódcą sił zbrojnych Izraela był szef sztabu generalnego, któremu podlegali dowódcy poszczególnych rodzajów wojsk. Z kolei, szef sztabu generalnego podlegał cywilnemu nadzorowi ministra obrony. Jednak, w izraelskich realiach politycznych, zarówno premier, jak i wielu ministrów posiadało w swojej karierze służbę w siłach specjalnych i/lub wywiadowczych. Ponadto, związki

[376] Tamże.

[377] Siły zbrojne rekrutowały nie-izraelskich Żydów oraz osoby nie będące Żydami z co najmniej jednym żydowskim dziadkiem, a także konwertytów na judaizm. Pierwsza jednostka piechoty, w której – obok mężczyzn – służyły kobiety, została utworzona w 2004 r. (batalion Caracal). *Israel*, *The World Factbook*, CIA 2022, https://www.cia.gov/the-world-factbook/countries/israel/#military-and-security [dostęp: 18.12.2022].

[378] Ł. Pacholski, A. Rokosz, op. cit.

[379] Tamże.

społeczeństwa z armią były zdecydowanie silniejsze niż w krajach bez obowiązkowej służby wojskowej. Kierowanie krajem przez byłych wojskowych miało zaletę w postaci faktu, że rozumieli oni doskonale uwarunkowania i priorytety bezpieczeństwa kraju. Miało to szczególne znaczenie dla państwa takiego jak Izrael, które stawało w obliczu fundamentalnych zagrożeń występujących na Bliskim Wschodzie[380].

Istotnym narzędziem w zakresie przeciwdziałania zagrożeniom hybrydowym, jak dowiedziono w badaniach, były siły specjalne, które mogły być wykorzystane zarówno do zwalczania ataku hybrydowego z użyciem sił nieregularnych, jak i operacji w kraju i za granicą – w tym na terenie wroga. Od 2011 r. dowództwo wojskowe Izraela rozważało możliwość zwiększenia zdolności sił specjalnych do prowadzenia operacji w głębi terytorium wroga. W ramach Sztabu Generalnego powstał Departament Operacji Głębokich, przed którym postawiono zadanie opracowywania planów i monitorowania przebiegu tego typu działań w znacznej odległości poza granicami państwa. Izrael podejmował też działania mające na celu poprawę zdolności służb i sił specjalnych w zakresie nowoczesnych technologii, co zapewniło przewagę informacyjną względem wroga. Pod operacyjne podporządkowanie tego departamentu zostało włączonych szereg jednostek, w tym – pułk specjalnego przeznaczenia Sztabu Generalnego Sayeret Matkal (wzorowany na brytyjskim SAS) oraz Shayette 13[381]. Shayetet 13, który działał w ramach marynarki wojennej posiadając doświadczenie w zwalczaniu dywersji morskiej i misjach zwiadowczych. Była to jedna z najbardziej uznanych sił specjalnych na świecie, dorównująca amerykańskiej piechocie morskiej (US Navy SEALs). Od momentu powstania w 1964 r., Shayetet 13 brał udział w większości wojen toczonych przez Izrael angażując się w różne działania operacyjne, w tym – strategiczne niszczenie infrastruktury morskiej wroga oraz zbieranie wysokiej jakości informacji wywiadowczych.

W toku badań stwierdzono, że w siłach zbrojnych Izraela umiejscowiony był wywiad i kontrwywiad wojskowy – Zarząd Wywiadu Wojskowego (Aman), który – wraz z cywilnymi agencjami: Mossadem (operacje zagraniczne) i Szin Betem (bezpieczeństwo

[380] *Israel Defense Forces…*

[381] Y. Matvienko, *How Israel reformed the intelligence and special services,* BulgarianMilitary.com January 9, 2022 https://bulgarianmilitary.com/amp/2022/01/09/how-israel-reformed-the-intelligence-and-special-services/ [dostęp: 6.12.2022].

wewnętrzne) – tworzył trzy filary służb wywiadowczych Izraela[382]. Wszystkie te instytucje znajdowały się w gotowości celem przeciwdziałania zagrożeniom hybrydowym: wyprzedająco lub reaktywnie (akcje odwetowe, jak ta po „Masakrze w Monachium"). Ponadto, w ramach izraelskiej praktyki wywiadowczej, istniała formuła współpracy z osobami pochodzenia żydowskiego, które zamieszkiwały poza granicami Izraela (określanymi mianem pomocników – „sayan"). Zwykle byli oni rekrutowani spośród diaspory żydowskiej.

W sytuacji wojny lub w przypadku innego kryzysu, istotną zaletą Izraelskich Sił Obronnych, jak wynika z informacji Departamentu Wojskowego Ambasady Izraela w Polsce, była „szybka mobilizacja rezerwistów z całego kraju do właściwych jednostek, co pozwala w ciągu 72 godzin zwiększyć stan osobowy armii trzykrotnie. (…) Izraelskie Siły Obronne to jedna z najbardziej zaprawionych w bojach armii na świecie (…) odstrasza wrogów (…) zarówno na terenie Izraela, jak i poza jego granicami. (…) Ze względu na niewielkie terytorium kraju, CAHAL musi przejmować inicjatywę (…) bezzwłocznie przenieść działania wojenne na terytorium przeciwnika. (…) Armia prowadzi programy edukacji uzupełniającej dla cywilów, przyczynia się także do szybszej integracji społecznej nowych imigrantów[383]."

Jak dowiodły badania, uzupełnieniem potencjału obronnego w postaci żołnierzy był sprzęt wojskowy, którego większość składała się z broni produkowanej w kraju lub importowanej od wiodących producentów z Europy i USA (Stany Zjednoczone są wiodącym dostawcą broni do Izraela od 2010 r.). Izrael posiadał dobrze rozwinięty przemysł zbrojeniowy, który był w stanie opracowywać, produkować i utrzymywać szeroką gamę systemów uzbrojenia. Broń ta, którą stanowiły w szczególności pojazdy opancerzone, drony, systemy obrony powietrznej i pociski kierowane, była przeznaczona przede wszystkim na potrzeby własnych sił zbrojnych, ale była także eksportowana[384]. Jedną z firm tego sektora był Rafael Advanced Defense Systems Ltd., który udoskonalał system obrony przeciwrakietowej (ang. Iron Dome). Do innych izraelskich firm o ugruntowanej pozycji

[382] *Israel Defense Forces…*

[383] *Siły Obronne Izraela*, Ambasada Izraela w Polsce (Departament Wojskowy) https://embassies.gov.il/warsaw/Departments/Wojskowy/Pages/wojskowy.aspx dostęp: 31 stycznia 2022 r.

[384] *Israel*, *The World Factbook*, CIA 2022 https://www.cia.gov/the-world-factbook/countries/israel/#military-and-security [dostęp: 18.12.2022].

produkujących broń należał Elbit Systems wraz z należącą do niego spółką IMI Systems (Israel Military Industries). Ta ostatnia, była uznanym wytwórcą zwłaszcza broni palnej i amunicji (m.in. rozpowszechniany na świecie pistolet maszynowy Uzi). Liczący niespełna 10 milionów obywateli Izrael był także producentem podstawowych czołgów pola walki „Merkava", co nie udało się dotąd krajom o znacznie większym potencjale gospodarczym, jak Polska (konieczność importu czołgów niemieckich oraz wyprodukowanych w USA i Korei Południowej w 2022 r.)[385]. Ponadto, po wojnie Jom Kipur Izrael doprowadził do zbudowania własnej sieci satelitów szpiegowskich, przez co dołączył do wąskiego grona państw dysponujących takimi zdolnościami rozpoznania[386].

Izraelskie siły zbrojne korzystały w dużej mierze z nowoczesnych systemów uzbrojenia, które zostały w znacznym stopniu zaprojektowane i wyprodukowane w Izraelu. Nawet zakładając wsparcie zagraniczne dla Izraelczyków, było to duże osiągnięcie zważywszy na fakt pozostawania przez Izrael małym krajem. Uzupełnienie wyposażenia armii pochodziło z importu, głównie ze Stanów Zjednoczonych. Stany Zjednoczone i Izrael rozwijały też wspólnie system obrony antyrakietowej Arrow[387].

Mimo, że Izrael nie potwierdził oficjalnie posiadania broni atomowej, jak wykazały wyniki badań, kraj ten posiada arsenał jądrowy (w sile około kilkuset głowic), który był kluczowym elementem stosowanej przez niego doktryny odstraszania. W przeszłości, wypowiedzi najwyższych izraelskich polityków, a także niektórych polityków amerykańskich sugerowały, że kraj ten ma broń nuklearną oraz środki jej przenoszenia (m.in. pociski Lance oraz międzykontynentalne Jerycho)[388]. Władze Izraela rozważały możliwości

[385] Ł. Pacholski, A. Rokosz, op. cit.

[386] Ponadto, Izrael, jako jedyny kraj na Bliskim Wschodzie, nie podpisał Układu o Nierozprzestrzenianiu Broni Jądrowej. Władze w Tel Awiwie nie podpisały także Konwencji o broni biologicznej oraz podpisały, ale nie ratyfikowały Konwencji o zakazie broni chemicznej.

[387] Stany Zjednoczone są strategicznym sojusznikiem Izraela, co przejawia się we wzmocnionej współpracy: „Od 1983 r. regularnie dwa razy do roku zbierają się wspólne amerykańsko-izraelskie grupy polityczno-wojskowe. Armia Stanów Zjednoczonych uczestniczy z Siłami Obrony Izraela we wspólnych ćwiczeniach wojskowych i sztabowych. Oba państwa współpracują ze sobą w dziedzinie wymiany informacji, technologii i rozwoju nowych rodzajów broni. Od 1976 r. Izrael jest największym odbiorcą amerykańskiej pomocy zagranicznej. W 2009 r. Izrael otrzymał w ten sposób pomoc wojskową o wartości 2,55 miliarda USD – 26% tej kwoty musiała być przeznaczona na zakup sprzętu wojskowego w amerykańskim przemyśle zbrojeniowym.". *Siły obronne Izraela*, Konflikty.pl 19.11.2006 https://www.konflikty.pl/technika-wojskowa/na-ladzie/sily-obronne-izraela/ [dostęp:7.12.2022].

[388] Chociaż Izrael obsługuje jądrowe reaktory badawcze, nie ma elektrowni atomowych. Jednak możliwość budowy elektrowni nuklearnych była rozważana przez władze Izraela w różnych momentach na przestrzeni lat.

pozyskania broni nuklearnej już wcześniej, ale dopiero Kryzys Sueski w 1956 r. (ZSRR zagroziło Izraelowi użyciem broni jądrowej, w razie odmowy wycofania się z zajętych terenów) zintensyfikował działania na tym kierunku. Według niektórych źródeł, Izrael rozpoczął produkcję broni jądrowej od 1968 r. (korzystając ze wsparcia Francji przy rozwoju cywilnego programu elektrowni atomowych)[389].

W świetle wyników przeprowadzonych badań, bardzo istotny w kontekście odstraszania przeciwko zagrożeniom hybrydowym był aspekt dążenia przez Izrael do bazowania przede wszystkim na swoich zasobach w zapewnieniu bezpieczeństwa narodowego. W perspektywie długoterminowej, jak zauważyli Louis René Beres i Zalman Shoval, Izrael, musi stać się „jeszcze bardziej samowystarczalny w kształtowaniu podstawowej polityki bezpieczeństwa narodowego kraju. Władze w Jerozolimie nigdy tak naprawdę nie liczyły wyłącznie na rodzaj amerykańskiego „parasola" nuklearnego – potwierdzenia strategicznej niezależności Izraela. W związku z tym nie należy już automatycznie zakładać, że (...) zagrożeniom nienuklearnym – czy to ze strony poszczególnych państw, sojuszy państw, grup terrorystycznych, czy nawet „hybryd" państwowo-terrorystycznych – należy koniecznie stosować symetryczne odpowiedzi[390]."

Ponadto, jak pokazują wyniki badań, skuteczny system obrony powinien „uwzględniać przeciwników zarówno państwowych, jak i niepaństwowych, w tym znaczących aktorów „hybrydowych". Przykładami namacalnie zhybrydyzowanego wroga byłyby formalne lub nieformalne sojusze między Iranem a Hezbollahem lub Iranem a Hamasem. Mówiąc dokładniej, izraelskie kierownictwo państwa będzie musiało rozważyć strategiczne korzyści płynące ze znaczącego wyjścia poza „tradycyjne" rozróżnienia między odstraszaniem nuklearnym i konwencjonalnym[391]."

Jeśli chodzi o konwencjonalne zagrożenia ze strony wroga (nie będące atakami nuklearnymi ani biologicznymi), ale mogące zagrozić istnieniu Izraela, kraj ten może zastosować groźbę odstraszania nuklearnego. W określonych sytuacjach, jak twierdzą L. R. Beres i Z. Shoval, Izrael może być „zmuszony polegać na nuklearnych formach

[389] Ł. Pacholski, A. Rokosz, op. cit.

[390] L. R. Beres, Z. Shoval, *Creating A Seamless Strategic Deterrent: An Israel Case Study,* 05.13.2019, Modern War Institute https://mwi.usma.edu/creating-seamless-strategic-deterrent-israel-case-study/ [dostęp:5.12.2022].

[391] Tamże.

odstraszania przeciwko egzystencjalnym zagrożeniom konwencjonalnym (…) Potencjalni agresorzy Izraela, zarówno dysponującymi środkami konwencjonalnym, jak i nuklearnymi, muszą być uświadomieni i przekonani, iż rząd izraelski posiada wymaganą gotowość i zdolność do rozpoczęcia wyważonych/skalibrowanych nuklearnych odwetów." Scenariusz taki byłby realny, na przykład, w sytuacji jednoczesnego, zmasowanego ataku kilku państw arabskich na Izrael[392]. Skalę zagrożenia dla Izraela pokazał początek konfliktu Jom Kippur. 7 października 1973 r., kiedy Izrael znalazł się w trudnej sytuacji w drugim dniu wojny, minister obrony tego kraju Moshe Dayan zaproponował możliwość dokonania demonstracji nuklearnej celem deeskalacji konfliktu. Spodziewane korzyści z odstraszania nuklearnego, jak wykazały wyniki badań, mogą dotyczyć także innych sfer. Jeśli, na przykład, Izrael kiedyś rozważy zainicjowanie nienuklearnego pierwszego uderzenia obronnego przeciwko Iranowi (jako formy wyprzedzającej samoobrony), prawdopodobieństwo doznania masowego konwencjonalnego odwetu ze strony władz w Teheranie może zostać zmniejszone[393].

Jednakże, jeśli chodzi o Izrael i jego deklaratywne zdolności nuklearne, jak trafnie zauważył Louis René Beres „sukces militarny [tego kraju] musi bazować na wiarygodnym odstraszaniu, a nie na faktycznej wojnie. Zgodnie ze starożytną chińską myślą wojskową przedstawioną przez Sun-Tzu (…) najbardziej korzystne jest przełamywanie oporu wroga bez walki (…) Z tego wszystkiego wynika, że izraelska broń nuklearna musi konsekwentnie pozostawać zorientowana na odstraszanie ex ante, a nie na faktyczne prowadzenie wojny lub zemstę ex post. Jako instrument odstraszania broń nuklearna może odnieść sukces tylko wtedy, gdy nie jest używana przez dłuższy czas. Gdy zdolności atomowe zostaną użyte w konkretnej bitwie, odstraszanie z definicji zawiedzie. Warto również zauważyć, że po faktycznym użyciu tej broni masowego rażenia wszelkie tradycyjne znaczenie zwycięstwa, zwłaszcza jeśli obie strony są już nuklearne, natychmiast stałoby się dyskusyjne (z uwagi na druzgocące w skutkach dla ludzi i środowiska efekty tej broni)[394]."

Siły Obronne Izraela, co podkreślił David E. Johnson, zdobyły duże doświadczenie w walce z hybrydowymi przeciwnikami w konfliktach w Libanie i Gazie (Hezbollahem

[392] Tamże.
[393] Tamże.
[394] L.R. Beres, *Israel's Nuclear Strategy: Enhancing Deterrence in the New Cold War (Part I), The Bridge,* May 29, 2018 https://thestrategybridge.org/the-bridge/2018/5/29/israels-nuclear-strategy-enhancing-deterrence-in-the-new-cold-war-part-i [dostep: 7.12.2022].

i Hamasem), dlatego mogą stanowić model dla wzmacniania zdolności przeciwdziałania zagrożeniom hybrydowym także w USA i w innych krajach. Do skutecznego radzenia sobie z zagrożeniami hybrydowymi, potrzebne są wszechstronne, odpowiednio liczne, wytrenowane i wyposażone siły wojskowe, które posiadają wsparcie powietrzne, artyleryjskie i bezzałogowych systemów powietrznych i morskich. Ponadto, znaczenie sił zbrojnych w walce z nieregularnymi przeciwnikami wzrasta wszędzie tam gdzie wymagane jest fizyczne wkroczenie armii, aby opanować sytuację. Istotą zagrożenia ze strony hybrydowych przeciwników jest to, iż zwiększają oni wyzwania dla sił zbrojnych, zwłaszcza – lądowych. Jednostki dysponujące ciężkim uzbrojeniem (czołgi, bojowe wozy piechoty) są kluczowym elementem zwalczania nieregularnych przeciwników, ponieważ – jak ocenił D. Johnson – zmniejszają ryzyko operacyjne i minimalizują straty sojuszników[395].

Obecna doktryna wojskowa Izraela, w ocenie Yuriya Matvienko, zakłada, że połączone siły jego przeciwników przekraczają możliwości mobilizacyjne tego kraju. Biorąc to pod uwagę, izraelscy stratedzy zalecili stworzenie warunków umożliwiających pokonanie wroga lub wrogów w krótkim czasie na ich terytorium lub wyrządzenie przeciwnikowi na tyle dotkliwych szkód, że skłonią go do zawarcia pokoju[396].

W wyniku przeprowadzonych badań stwierdzić należy, że współpraca w zakresie bezpieczeństwa narodowego USA z Izraelem należy do jednej z najbardziej pogłębionych relacji tego typu na świecie. Stany Zjednoczone, jako pierwsze na świecie uznały Izrael za państwo w 1948 r. Były też pierwszym krajem, który uznał Jerozolimę za stolicę Izraela w 2017 r.[397] Jak poinformował amerykański resort spraw zagranicznych na swoich stronach, Izrael jest „wspaniałym partnerem Stanów Zjednoczonych, a Izrael nie ma większego przyjaciela niż Stany Zjednoczone. (…) Nierozerwalna więź między (oboma) krajami nigdy nie była silniejsza. (…) Bezpieczeństwo Izraela jest od dawna kamieniem węgielnym

[395] D. E. Johnson, *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza,* RAND Corporation 2010, https://www.rand.org/pubs/occasional_papers/OP285.html [dostęp: 6 grudnia 2022].

[396] Y. Matvienko, *How Israel reformed the intelligence and special services,* BulgarianMilitary.com January 9, 2022 https://bulgarianmilitary.com/amp/2022/01/09/how-israel-reformed-the-intelligence-and-special-services/ [dostęp: 6.12.2022].

[397] W opracowaniu przyjęto, że stolicą kraju oraz władz jest Tel Awiw, z uwagi na funkcjonowanie cały czas polskiej misji dyplomatycznej (ambasady) w tym mieście. Stany Zjednoczone utrzymują cały czas duży oddział ambasady w Tel Awiwie. Ambasada USA w Izraelu przeniosła się z Tel Awiwu do tymczasowego obiektu w Jerozolimie 14 maja 2018 r.

amerykańskiej polityki zagranicznej[398].” Izrael, jako jedyny kraj na świecie, jest wspierany przez USA w tak znaczący sposób: Stany Zjednoczone corocznie przekazują 3,3 miliarda USD w ramach zagranicznego finansowania wojskowego i 0,5 miliarda USD na programy współpracy w zakresie obrony przeciwrakietowej. Ponadto, Stany Zjednoczone współpracują z Izraelem w zakresie wspólnych ćwiczeń wojskowych oraz badań i rozwoju nowoczesnego uzbrojenia. W ramach dorocznej Wspólnej Grupy ds. Zwalczania Terroryzmu i regularnych dialogów strategicznych, Stany Zjednoczone i Izrael współpracują, aby przeciwdziałać szeregowi regionalnych zagrożeń[399]. Bliska kooperacja z USA w dziedzinie bezpieczeństwa narodowego zapewnia wzmocnienie potencjału obronnego Izraela, także w kontekście odstraszania.

Odstraszanie, jak wykazały wyniki badań, było głównym, ale nie jedynym elementem izraelskiej strategii walki z wrogami. Pełne spektrum zapobiegania atakom hybrydowym, jak dowodzi Graham Allison, obejmuje działania polegające na wzmacnianiu sił zbrojnych w odniesieniu do wykrywania i identyfikacji zagrożeń (głęboka penetracja na terytorium wroga) oraz rozbudowy systemów obrony (m.in. systemu obrony przeciwrakietowej Żelazna Kopuła, zabezpieczenia na wszystkich granicach)[400].

W koncepcję odstraszania, jak wykazały wyniki badań, wpisane jest ryzyko stałej niepewności odnośnie zapewniania przez ten środek wystarczającego poziomu bezpieczeństwa. Władze Izraela mają tę świadomość i wspierają monitoring oraz usprawnianie swoich zdolności odstraszania. Izraelskie czerwone linie są wyraźnie, publicznie i wielokrotnie ogłaszane przez izraelskich polityków i urzędników. Jest to dokonywane w komunikatach i wypowiedziach nie tylko po hebrajsku, ale także po arabsku[401]. W 2006 r. Izrael zdecydował o specjalnej operacji wojskowej w południowym Libanie (druga wojna libańska), która była wymierzona w Hezbollah. Przykład ten pokazuje, że zagrożenia hybrydowe mogą zaskoczyć nawet kraje z tak silnymi zdolnościami obronnymi jak Izrael.

---

[398] Znacząca jest też dynamika ogólnej współpracy gospodarczej. Stosunki handlowe USA-Izrael są oparte na dwustronnym handlu towarami i usługami o wartości prawie 50 miliardów USD rocznie. Czyni to Stany Zjednoczone największym partnerem handlowym Izraela. *U.S. Relations With Israel*, US Department of State, JANUARY 20, 2021 https://www.state.gov/u-s-relations-with-israel/ [dostęp:18.12.2022].

[399] *U.S. Relations With Israel*…

[400] G. Allison, *Why ISIS Fears Israel,* The National Interest, August 8, 2016, https://www.belfercenter.org/publication/why-isis-fears-israel [dostęp:7.12.2022].

[401] Tamże.

W świetle wyników przeprowadzonych badań stwierdzić należy, że konfrontacja Izraela z siłami hybrydowego przeciwnika w postaci Hezbollahu w 2006 r. pokazała jednak znaczenie stałego monitorowania zdolności bojowych sił zbrojnych i zagrożenia związane z zaniedbaniami na tym polu. W 2006 r. Izrael zdecydował o specjalnej operacji wojskowej w południowym Libanie (druga wojna libańska), która była wymierzona w Hezbollah. Jednak, w rezultacie, ponad 30 tysięcy żołnierzy izraelskich nie było w stanie pokonać bojowników, co zakończyło się zawieszeniem broni. Była to tym dotkliwsza porażka, ponieważ Izrael, jak dowodzi S. Lewicki, nie walczył z siłami zbrojnymi żadnego państwa, ale tylko z milicją jednej z organizacji. Potwierdziła to strona izraelska badając udział swoich sił zbrojnych w tym konflikcie. W raporcie zawarto m.in. takie dobitnie wskazano, że ”paramilitarna organizacja złożona z kilku tysięcy ludzi stawiała opór, przez kilka tygodni, najsilniejszej armii na Bliskim Wschodzie, która cieszyła się pełnym panowaniem w powietrzu oraz przewagą liczebną i technologiczną[402]”.

W sytuacji zagrożenia, zgodnie z ówczesną doktryną obronną – jak dowiodły badania informacji przedstawionych przez Łukasza Pacholskiego i Aarona Rokosza – w pierwszej kolejności wykorzystywane były wyposażone w środki precyzyjnego rażenia siły powietrzne oraz artyleria. Natomiast użycie jednostek pancernych i piechoty było traktowane jako ostateczność. Za te zmiany odpowiadał szef sztabu generalnego w latach 2002-2005 gen. Mosce Ya’alona, oraz jego następca, gen. Dan Halutz. Obaj reprezentowali sił powietrzne. W rezultacie, obniżył się poziom wyszkolenia zwłaszcza kadry dowódczej wojsk lądowych, które po 2000 r. były wykorzystywane głownie do walki ze słabo zorganizowanymi bojówkami w strefie Gazy i na Zachodnim Brzegu Jordanu. Zaniedbano także ćwiczenia na większą skalę oraz ograniczono wydatki na uzbrojenie. Taktyka ta sprawdzała się wobec palestyńskich grup terrorystycznych, ale zwiodła kiedy Izrael został zaatakowany przez lepiej zorganizowane i wyposażone siły Hezbollahu w 2006 r. Podejście bazujące na wykorzystaniu lotnictwa i artylerii nie sprawdziło się w związku z czym Izrael musiał wprowadzić do walki na szerszą skalę siły lądowe. Okazały się one mało skuteczne, co przyczyniło się, że działania mające na celu zneutralizowanie Hezbollahu, zakończyły się po 34 dniach rozejmem. W efekcie, działania izraelskiego dowództwa oceniono jako porażkę

[402] S. Lewicki, *Jak silny jest Izrael?,* Portal Myśli Konserwatywnej – Konserwatyzm.pl, 4 września 2021, https://konserwatyzm.pl/lewicki-jak-silny-jest-izrael/ [dostęp:7.12.2022].

i gen. Dan Halutz poddał się do dymisji w styczniu 2007 r. Od tego czasu izraelskie władze i kadra dowódcza dążyły do przywrócenia odpowiednich proporcji w zakresie rozwoju poszczególnych rodzajów sił zbrojnych[403].

Badania pokazały, że rządowa komisja śledcza w sprawie przeglądu przygotowań i prowadzenia operacji wojskowej Izraela podczas wojny z Hezbollahem w 2006 r. (Komisja Winogradu) stwierdziła, że – mimo precyzyjnych operacji sił powietrznych i bohaterstwa wielu żołnierzy – wojna była izraelską porażką. Przyznano, że „kiedy najsilniejsza armia na Bliskim Wschodzie (Izrael) wyrusza do walki z organizacją zbrojną taką jak Hezbollah i nie odnosi nad nią zdecydowanego zwycięstwa, to sytuacja ta ma daleko idące negatywne implikacje dla statusu Izraela[404].” To jest rezultat, którego Izrael powinien był uniknąć, przeprowadzając tylko ostrą, ale krótką akcję, zamiast przedłużającej się konfrontacji wojennej, jak podsumował raport komisji.

Władzom Libanu zarzucano bierność względem antyizraelskich działań grup bojowników na jego terytorium. Struktury państwowe Libanu, jak uznano, były nieefektywne i umożliwiały swobodne operowanie w tych warunkach zbrojnej organizacji takiej jak Hezbollah, która – jako siła subpaństwowa (ang. a sub-state force) – charakteryzowała się cechami organizacji wojskowej, milicji i fanatycznego ruchu ideologicznego i religijnego. Wskazano, że Hezbollah był powiązany ideologicznie, ekonomicznie i militarnie z organizacjami i państwami spoza Libanu, ale reprezentował także społeczność libańską. Hezbollah w rzeczywistości kontrolował południowy Liban i utrzymywał obecność wojskową w całym kraju. Celowo, jak zauważono, atakował obywateli Izraela podejmując próby uderzeń na cele infrastrukturalne, w tym instalacje elektryczne i petrochemiczne. Masowo wykorzystywał nieprecyzyjną amunicję – kierował ją także w stronę izraelskich skupisk ludności. Co więcej, przez całą wojnę armia libańska nie podejmowała prób ograniczania działań militarnych Hezbollahu z terytorium Libanu. Natomiast sam Izrael, w ocenie ustaleń komisji, ograniczył ataki na ośrodki władzy i obiekty infrastrukturalne, które nie były bezpośrednio utożsamiane z Hezbollahem i jego zdolnością

[403] Ł. Pacholski, A. Rokosz, op. cit.

[404] B. S. Lambeth, *The Winograd Commission's Findings*, [w:] *Air Operations in Israel's War Against Hezbollah: Learning from Lebanon and Getting It Right in Gaza,* RAND Corporation, 2011, s. 220 https://www.jstor.org/stable/pdf/10.7249/mg835af.14.pdf?addFooter=false [dostęp: 12.12.2022].

do walki[405]. Ponadto, komisja dowiodła, że zdolność Izraela do zwalczania Hezbollahu w bezpośredni sposób była bardzo ograniczona, ponieważ jej bojownicy prawie nie posiadali stałych ośrodków (widoczne bazy i dowództwa). Ponadto, trudność sprawiało ustalenie czy dane osoby z tej organizacji (aktywiści) byli bojownikami, czy cywilami. W wielu przypadkach bojownicy działali wśród ludności cywilnej i na terenie zabudowanym. Co więcej, niektóre rodzaje uzbrojenia ofensywnego Hezbollahu były celowo ukrywane w domach mieszkalnych, a nawet w miejscach kultu, co utrudniło działania izraelskie[406].

Jak wykazały wyniki badań, przykład starać Izraela z siłami Hezbollahu jest dobrą ilustracją wyzwań w zakresie rozwoju odstraszającego potencjału obronnego. Okres względnie pokojowej koegzystencji Izraela z sąsiadami spowodował, że władze w Tel Awiwie zbyt mały nacisk położyły na wyszkolenie i koordynację działań sił lądowych. Udowodniło to, że w bezpieczeństwo i przeciwdziałanie zagrożeniom hybrydowym oraz zagrożeniom wszelkiego innego rodzaju – należy inwestować przede wszystkim w czasach pokoju. Powinno to zostać uwzględnione m.in. w działaniach Polski i innych krajów, które dążą do długoterminowego wzmocnienia swojego bezpieczeństwa przed zagrożeniami hybrydowymi.

Władze Izraela przed 2006 r. oceniały, że głównym zadaniem sił zbrojnych będzie w przyszłości przeciwdziałanie zagrożeniom asymetrycznym o niskiej intensywności. W założeniu, jak dowodzi David E. Johnson, siły powietrzne miały odstraszać przeciwników państwowych, co – w przypadku konfliktu zbrojnego – umożliwi mobilizację żołnierzy rezerwy. Ponowną wojnę z jednym z sąsiadów, władze w Tel Awiwie oceniły jako mało prawdopodobną. Obecność sił USA w Iraku w tamtym okresie także działała uspokajająco na izraelskich strategów. Na podstawie tych przesłanek, co podkreśla David E. Johnson, budżety wielu jednostek zostały obcięte oraz zlekceważono szkolenia jednostek pancernych, których przydatność w konflikcie o niskiej intensywności została zakwestionowana. Co więcej, struktury i procesy w izraelskich siłach zbrojnych, które zapewniały wysoki poziom integracji operacji powietrznych i naziemnych, zostały usunięte z poziomu brygad.

[405] *Israel, Report of the Winograd Commission*, How does law protect in war? (the "Online Casebook"), The International Committee of the Red Cross, https://casebook.icrc.org/case-study/israel-report-winograd-commission [dostęp:12.12.2022].

[406] Tamże.

Przeprowadzono także niewiele szkoleń w zakresie integracji wspólnych działań lotnictwa z wojskami lądowymi[407].

Błędem, w ocenie Davida E. Johnsona, było prawie całkowite skoncentrowanie się na walkach nieregularnych, co uczyniło siły zbrojne w praktyce niezdolnymi do prowadzenia dużych działań wojskowych: operacji połączonego ognia i skoordynowanych zdolności manewrowych związanych z głównymi operacjami bojowymi[408]. Tego typu wyzwanie pojawiło się przez izraelskim wojskiem, które miało problemy z unieszkodliwianiem sił Hezbollahu broniących swoich pozycji z użyciem m.in. przeciwpancernych pocisków kierowanych. Stosunkowo małe jednostki Hezbollahu były w 2006 r. dobrze wyszkolone, zorganizowane i uzbrojone w zaawansowaną broń (w tym: przeciwpancerne pociski kierowane, rakiety średniego i dalekiego zasięgu oraz przenośne systemy obrony powietrznej). W 2006 r. Izrael poniósł duże straty w walkach z hybrydowym przeciwnikiem jakim był Hezbollah. Co więcej, szkody poniosła również reputacja izraelskich sił zbrojnych, jako niezwyciężonej armii, która ma fundamentalne znaczenie dla skuteczności koncepcji obrony opartej na odstraszaniu[409].

W wyniku przeprowadzony badań stwierdzono, że Izrael wyciągnął wnioski z drugiej wojny libańskiej i ponownie położył nacisk na znaczenie sił lądowych. Przed tym konfliktem około 75 procent czasu szkoleń dotyczyło walki o niskiej intensywności, a 25 – o wysokiej intensywności. Proporcje te uległy odwróceniu. Doceniając ponownie znaczenie ciężkiego uzbrojenia wznowiono również produkcję czołgów Merkava IV (wstrzymaną wcześniej w wyniku oszczędności), a także zintensyfikowano szkolenie sił pancernych i rezerw. Skutki tych usprawnień pomogły Izraelowi przeprowadzić pomyślną interwencję w Strefie Gazy w 2008 r., gdzie wkroczyły – jak twierdziła strona izraelska – aby przeciwdziałać atakom rakietowym (operacja „Płynny Ołów"). Sprawne działania jednostek pancernych były najważniejszym elementem operacji, zapewniając osłoniętą, mobilną precyzyjną siłę ognia, która wywołała efekt zastraszenia u wroga. Działania te pomogły stronie izraelskiej odzyskać utraconą wcześniej reputację, ponieważ zreformowane wojska okazały się tym razem już znacznie lepiej przygotowane do walki z hybrydowym przeciwnikiem. Chociaż nie udało się

[407] David E. Johnson, *Preparing for "Hybrid" Opponents: Israeli Experiences in Lebanon and Gaza,* RAND Corporation, 2011. https://www.rand.org/pubs/research_briefs/RB9620.html [dostęp: 21.12.2022].
[408] Tamże.
[409] Tamże.

całkowicie powstrzymać wystrzeliwania rakiet z Gazy w kierunku Izraela, operacja znacząco je ograniczyła. Kampania „Płynny Ołów", którą przeprowadzono dwa lata po uznawanej za porażkę interwencji z 2006 r., była kluczem do przywrócenia wiarygodności odstraszania sił zbrojnych Izraela[410].

Doświadczenia izraelskie pokazały, w ocenie Davida E. Johnsona, że zagrożenie hybrydowe może zostać wytworzone w relatywnie krótkim czasie za pomocą transformacji działań podmiotów o różnych poziomach kompetencji wojskowych[411]. Co istotne, to względna łatwość przejścia od zagrożenia niskiego stopnia, które generują zbrojne organizacje pozapaństwowe, do zdolności hybrydowych organizacji sponsorowanych przez wrogie państwo lub ich grupę. Potrzebny jest do tego jedynie sponsor państwowy, który zdecyduje się dostarczyć broń i wyszkolić nieregularne siły. W Afganistanie w latach 80., Stany Zjednoczone, stworzyły taką hybrydową siłę zbrojną przekazując pociski Stinger Mudżahedinom. Przekształciło to opozycyjnych względem ZSRR bojowników w hybrydowego przeciwnika dysponującego bronią zagrażającą wojskom radzieckim i zmuszając je ostatecznie do wycofania się[412].

W świetle wyników przeprowadzonych badań stwierdzono, że siły wywiadowcze i specjalne Izraela są dobrym przykładem, w jaki sposób państwo może starać się zapobiec powtarzającym się przypadkom ataków o naturze hybrydowej. Po zamachu dokonanym przez terrorystyczną organizację Czarny Wrzesień podczas igrzysk olimpijskich w Monachium w 1972 r., władze Izraela zdecydowały o rozpoczęciu specjalnej misji wywiadowczej.

Podczas igrzysk olimpijskich w Monachium w 1972 r. doszło do uprowadzenia i zamordowania 11 izraelskich sportowców przez palestyńską organizację terrorystyczną „Czarny Wrzesień". Mimo, że na miejscu zamachu byli obecni przedstawiciele Izraela, występowali oni tylko w charakterze obserwatorów. Próba odbicia zakładników została przeprowadzona przez jednostki niemieckie, które nie były wówczas należycie przygotowane kadrowo i organizacyjnie i nie wykazały się profesjonalizmem. Trzech z ośmiu porywaczy przeżyło i kilka tygodni później zostało zwolnionych z aresztu przez rząd RFN (w wymianie – w zamian za załogę uprowadzonego odrzutowca Lufthansy).

[410] Tamże.
[411] Tamże.
[412] Tamże.

Pozostałych pięciu zamachowców zginęło w wymianie ognia w czasie nieudanej próby uratowania zakładników[413].

Zamach na Żydów na terenie Niemiec miał także znaczenie symboliczne przywołując najgorsze wspomnienia drugiej wojny światowej. Śmierć wszystkich izraelskich zakładników na niemieckiej ziemi, była szczególnie niekorzystna dla – odbudowywanego po II wojnie światowej – wizerunku tego kraju. Po „Masakrze w Monachium", pamiętająca Holokaust ówczesna premier Izraela, Golda Meir, zarządziła wytropienie i ukaranie porywaczy i powiązanych z nimi osób. Celem było nie tylko ukaranie terrorystów, ale także wzmocnienie efektu odstraszania, aby tego typu zagrożenie dla Izraelczyków nie powtórzyło się. Zlecona przez ówczesną premier Izraela, Goldę Meir, operacja „Gniew Boży" miała na celu odszukanie i pojmanie sprawców „Masakry w Monachium", w której zginęło 11 izraelskich sportowców. Premier Izraela, która pamiętała czasy zagłady Żydów w Niemczech i krajach przez nie okupowanych w czasie II wojny światowej, wykazała determinację, aby tego typu zagrożenie dla jej współobywateli nie powtórzyło się. Chociaż Izrael przeprowadzał już wcześniej ataki na przywódców palestyńskich organizacji, które uznała za terrorystyczne (m.in. Fatah, Organizacja Wyzwolenia Palestyny, Ludowy Front Wyzwolenia Palestyny), po wydarzeniach w Monachium, częstotliwość takich zabójstw znacząco wzrosła[414].

Jak wynika z informacji Eriki Pearson, specjalna izraelska komisja pod przewodnictwem premier Goldy Meir i ministra obrony Moshe Dayana wydała aprobatę dla fizycznej eliminacji wszystkich bezpośrednio lub pośrednio zaangażowanych w „Masakrę w Monachium". Za cel obrano „Czarny Wrzesień" – organizację powiązaną z Fatahem, którą oskarżono o zorganizowanie zamachu na Izraelczyków podczas olimpiady w Niemczech[415]. Wykonawcami operacji był zespół składający się z funkcjonariuszy izraelskich służb wywiadu zagranicznego (Mosadu), którzy byli wspierani przez żołnierzy jednostek specjalnych Sił Obronnych Izraela.

W świetle wyników przeprowadzonych badań stwierdzono, że identyfikowanie i tropienie osób podejrzanych o planowanie i/lub udział w zamachu w Monachium zajęło

[413] E. Pearson, *Operation Wrath of God*. Encyclopedia Britannica, 2 May. 2018, https://www.britannica.com/topic/Operation-Wrath-of-God [14.12.2022].
[414] Tamże.
[415] Tamże.

szereg lat. Izrael przeprowadzał już w przeszłości operacje fizycznej likwidacji przywódców palestyńskich (m.in. Organizacja Wyzwolenia Palestyny, Fatah). Jednak skala i okres trwania „Gniewu Bożego" były bezprecedensowe w historii tego kraju[416]. Operacja odwetowa po wydarzeniach w Monachium trwała przez ponad 20 lat – aż do lat 90-tych XX w.[417]

Pierwszą ofiarą działań, które nosiły kryptonim „Bagnet", był Waela Zwaitera, aktywista Organizacji Wyzwolenia Palestyny i kuzyn Yāsira Arafāta. Izraelczycy zastrzelili go w Rzymie w październiku 1972 r. (zginął w holu apartamentowca, w którym mieszkał). Następnie został wyeliminowany Mahmoud Hamshari – przedstawiciel Organizacji Wyzwolenia Palestyny w Paryżu. Jeden z Izraelczyków, udający włoskiego dziennikarza, namówił go w grudniu 1972 r. do udzielenia wywiadu telefonicznego. Wcześniej, inni członkowie izraelskiego zespołu uderzeniowego włamali się do domu Hamshariego i umieścili ładunek wybuchowy w jego stacjonarnym aparacie telefonicznym. W umówionym na wywiad telefoniczny czasie, Palestyńczyk odebrał telefon, a kiedy przedstawił się – zdetonowano zdalnie bombę zabijając go. W ciągu następnych kilku miesięcy zlikwidowano czterech innych podejrzanych o wsparcie „Masakry w Monachium": Basila al-Kubaisiego, Husseina Abada al-Chira, Zaida Muchassiego i Mohammeda Boudia[418]. Poza tymi akcjami, także wiele innych zabójstw lub ich prób na palestyńskich aktywistach na całym świecie, w tym w Polsce[419], również było wiązanych z izraelską operacją po zamachu w Monachium.

Cała kampania „Gniew Boży", jak ukazały badania, choć zakończyła się sukcesem Izraela[420], nie była idealna. W 1973 r. strona izraelska omyłkowo zabiła niewinnego

[416] Tamże.
[417] Tamże.
[418] Tamże.
[419] Chodzi o próbę zabicia Abu Daouda, który był jednym z. przyznał się publicznie do wsparcia planowania ataku terrorystycznego w Monachium. Zginął on od strzałów z broni palnej w sierpniu 1981 r. w holu warszawskiego hotelu Victoria.
[420] Niektórzy badacze twierdzili, że Izraelowi nie udało się zlokalizować i pojmać Palestyńczyków faktycznie odpowiedzialnych za Masakrę w Monachium, dlatego skoncentrował swoje wysiłki na pokazowym ukaraniu głównie działaczy Organizacji Wyzwolenia Palestyny przebywających w krajach zachodnich. Miało to na celu przekazanie jasnego komunikatu do aktywistów palestyńskich i innych wrogów Izraela, że tego typu ataki na jego obywateli spotkają się z bezlitosną reakcją. W czasie operacji zginęło szereg niewinnych osób, w tym w Lillehammer w Norwegii, gdzie zatrzymano kilku oficerów izraelskich służb i oskarżono pod zarzutem morderstwa (przypadkową ofiarą był marokański kelner Ahmed Bouchiki). W rezultacie, cała siatka izraelskich służb wywiadowczych w Europie Zachodniej poważnie ucierpiała (częściowo wyszły na jaw m.in. jej sposoby komunikacji, dane agentury i mieszkania operacyjne w Paryżu). Ponadto, pojawiły się także twierdzenia, że skoncentrowanie się na odwecie i prowadzenie poszukiwań

człowieka w Lillehammer w Norwegii. Pierwotnym celem Izraelczyków w Lillehammer był Ali Hassan Salameh z kierownictwa Fatahu i Czarnego Września, znany jako „Czerwony Książę”[421]. Po nieudanym zamachu, części Izraelczyków nie udało się uciec z Norwegii i zostali pojmani. W wyniku dochodzenia prowadzonego przez władze norweskie aresztowano i skazano pięciu agentów Mossadu. Zdekonspirowano także rozległe sieci agentów i kryjówek Mossadu w całej Europie. Premier Izraela Golda Meir, w odpowiedzi na presję międzynarodową, poinformowała o oficjalnym zawieszeniu odwetowych zabójstw. Było to jednak fałszywa deklaracja wydana do celów politycznych, ponieważ likwidowanie istotnych działaczy palestyńskich cały czas trwało[422].

W ramach kampanii „Gniew Boży”, przeprowadzono także atak na palestyńskie cele w stolicy Libanu Bejrucie w kwietniu 1973 r. (Wiosna Młodości). Izrael uderzył wówczas za pomocą sił specjalnych w palestyńskie cele w stolicy Libanu Bejrucie, m.in. – w kierownictwo Organizacji Wyzwolenia Palestyny. Wojska przerzucono za pomocą desantu, a wsparciem na miejscu służyli działający niejawnie w tym mieście agenci Mossadu. Atak, który należy rozpatrywać w kategoriach odstraszania przez karę – uświadomił palestyńskim organizacjom siłę ich przeciwnika. Podobnie jak w przypadku odbicia zakładników w Ugandzie, Izrael pokazał, że posiada determinację i zdolności do precyzyjnego uderzenia w hybrydowego nieprzyjaciela na terytorium państwa trzeciego.

Warunkami pomyślnej realizacji tych skomplikowanych i wymagających misji odwetowych, był wcześniejszy rozwój zarówno sił wywiadowczych, specjalnych, jak i innych zdolności Izraela w zakresie środków bezpieczeństwa narodowego (odpowiednie środki technologiczne, nowoczesne uzbrojenia, sprawna logistyka, kontakty międzynarodowe, wsparcie diaspory).

Jak wykazały wyniki badań, kampania „Gniew Boży” potwierdziła znaczenie sił wywiadowczych i specjalnych Izraela w zakresie zapobiegania oraz redukcji przypadków zagranicznych ataków o naturze hybrydowej, których celem było to państwo i jego obywatele. Przyniosła ona korzyści dla Izraela, nawet z uwzględnieniem znaczących błędów

sprawców po całym świecie przyczyniło się do zlekceważenia sygnałów wskazujących na przygotowywanie przez państwa arabskie ataku zbrojnego na Izrael w postaci wojny Yom Kippur w 1973 r. E. Pearson, op. cit.

[421] W 1979 r. Izrael dokonał na niego zamachu w Bejrucie (zdetonowano samochód-pułapkę na trasie jego przejazdu). E. Pearson, op. cit.

[422] E. Pearson, *op. cit.*

jakich się dopuszczono (omyłkowe zabójstwo w Lillehammer i dekonspiracja europejskich zasobów wywiadowczych).

Początkowo Czarny Wrzesień także próbował ataków wymierzonych w Izraelczyków (m.in. plan strącenia samolotu premier Goldy Meir podczas jej wizyty w Rzymie w styczniu 1973 r., ataki z użyciem przesyłek pocztowych z ładunkami wybuchowymi kierowane do izraelskich placówek dyplomatycznych). Działania Izraela polegające na likwidowaniu palestyńskich terrorystów na całym świecie spowodowały zahamowanie bardziej znaczących palestyńskich zamachów na obywateli tego kraju przebywających poza granicami Izraela[423].

Likwidowanie palestyńskich terrorystów na całym świecie oraz zwiększona czujność służb Izraela zahamowały znaczące zamachy na obywateli tego kraju przebywających za granicą. Strona palestyńska nie pozostała jednak bierna wobec działań Izraela. Czarny Wrzesień próbował ataków, w tym brawurowego strącenia za pomocą pocisku rakietowego samolotu premier Izraela Goldy Meir podczas jej wizyty w Rzymie (styczeń 1973 r.). Odnotowano także przypadki przesyłek pocztowych z ładunkami wybuchowymi kierowane do izraelskich ambasad i konsulatów[424].

W wyniku badań ustalono, że strona izraelska przeprowadziła także akcję uwolnienia pasażerów porwanego samolotu przeprowadzona w Entebbe w Ugandzie z 3 na 4 lipca 1976 r. Tydzień wcześniej, 27 czerwca 1976 r., ponad 100 izraelskich i żydowskich pasażerów lotu Air France zostało porwanych przez członków Ludowego Frontu Wyzwolenia Palestyny i Niemieckich Komórek Rewolucyjnych. Samolot został porwany 27 czerwca 1976 r. na trasie z Izraela do Francji. Po zatrzymaniu się w Atenach francuski odrzutowiec uprowadzili członkowie Ludowego Frontu Wyzwolenia Palestyny i zachodnioniemieckiej, radykalnej lewicowej grupy –Frakcji Czerwonej Armii. Po przemieszczeniu maszyny do Ugandy, do terrorystów dołączyli dodatkowi wspólnicy. Na miejscu (samolot wylądował na lotnisku koło ugandyjskiego Entebbe), porywacze uwolnili tych z 258 pasażerów, którzy nie wyglądali na Izraelczyków ani Żydów. Resztę z nich przetrzymywali jako zakładników z zamiarem ich wymiany. Celem sprawców było doprowadzenie do uwolnienia 53.

[423] Tamże.
[424] Tamże.

oskarżonych m.in. o terroryzm bojowników uwięzionych w Izraelu, Kenii, Niemczech Zachodnich i innych miejscach[425].

Szczegóły operacji, jak pokazały badania, świadczą o wyjątkowych zdolnościach Izraela do skutecznych akcji ratunkowo-odwetowych daleko poza granicami kraju – nawet na innym kontynencie. Po tygodniowym planowaniu akcji ratunkowej „Piorun" (ang. „Thunderbolt"), która trwała około godziny, 3 lipca 1976 r. Izrael wysłał cztery samoloty transportowe Hercules C-130H przewożące około 100–200 żołnierzy i eskortowane przez myśliwce odrzutowe Phantom. Izraelskie maszyny przemierzyły ponad 4000 kilometrów dostarczając w nocy do Ugandy komandosów. Uratowano prawie wszystkich zakładników. Zabito wszystkich siedmiu porywaczy i 45 ugandyjskich żołnierzy[426]. Zniszczono także 11 myśliwców MiG, które zostały wcześniej dostarczone do Ugandy przez Związek Radziecki. Izraelczycy stracili podczas operacji jednego żołnierza i trzech zakładników. W drodze powrotnej izraelskie samoloty spotkały oczekujący samolot szpitalny i uzupełniły paliwo w Nairobi w Kenii.

W efekcie prac badawczych stwierdzono, że sukces operacji w Entebbe znacznie podniósł izraelskie morale i wzmocnił zdolności odstraszania tego kraju. Izrael udowodnił, że był w stanie przeprowadzić skomplikowaną operację odbicia swoich obywateli na terenie państwa trzeciego. Była to nowość w porównaniu z sytuacją z Monachium, gdzie Izraelczycy byli jedynie obserwatorami, nie angażując się w odbicie zakładników[427].

Wyjątkowość izraelskich instytucji bezpieczeństwa, jak dowodzi Ronen Bergman korespondent izraelskiej gazety Yediot Ahronoth i autor publikacji na temat Mossadu i innych służb i formacji, polegała zawsze na przekonaniu większości osób w nich służących, że jeśli nie wykonają swojego zadania perfekcyjnie, następnego dnia wszyscy mogą zginąć. Ten element szkolenia był obecny w nastawieniu większości formacji, służb i instytucji odpowiedzialnych za bezpieczeństwo Izraela. Wyrażał się on w przekonaniu, jak dowodził

[425] *Entebbe raid*, Encyclopedia Britannica, 2 Sep. 2022, https://www.britannica.com/event/Entebbe-raid [dostęp: 22.12.2022].

[426] Wśród ofiar było też trzech zakładników, ale udało się ocalić zdecydowaną większość – 102 zakładników. 5 komandosów zostało rannych, a jeden – dowódca jednostki, ppłk Yonatan Netanjahu, zginął. Warto zauważyć, że po brawurowej akcji władze ugandyjskie zemściły się na przebywających tam Kenijczyków – w odwecie za rzekome wsparcie Izraelskiej akcji pozbawiono życia ponad 200 z nich. *Israeli Commando of Entebbe to give first hand account of the Greatest Hostage Rescue in History*, 11/08/2022 https://www.southtahoenow.com/story/11/08/2022/israeli-commando-entebbe-give-first-hand-account-greatest-hostage-rescue-history [dostep: 15.12.2022].

[427] *Entebbe raid*…

R. Bergman, że „jeśli dziś nie zrobimy wszystkiego, co w naszej mocy, by się obronić jutro – stanie się coś potwornego[428].” Pierwszy premier Izraela, urodzony na terenie dzisiejszej Polski, Dawid Ben Gurion motywował swoich współpracowników mówiąc, że on sam – starając się uniknąć błędów i zaniedbań – „nie może spać spokojnie, obawiając się, że sprowadził do Izraela nowy Holocaust; że tym razem zagłada odbędzie się w żydowskim państwie, na ich własnej ziemi[429].”

Odniesienia do historii konfliktów z udziałem Izraela są wskazywane, jako źródło cennych lekcji dla Stanów Zjednoczonych, a pośrednio także – innych krajów zachodnich. Analiza mechanizmów wojny, w tym hybrydowej, może dostarczyć wartościowych wskazówek jak przeciwdziałać tego rodzaju zagrożeniom w przyszłości. Warto w tym kontekście przytoczyć cały czas aktualne słowa byłego szefa Centralnego Dowództwa USA Johna Abizaida, który – na rok przed atakiem Rosji na Ukrainę w 2022 r. – tak pisał o wnioskach z wojny w Donbasie w 2014 r.: „Chociaż strategia wojny politycznej (political warfare) Rosji nie jest nowa, analiza jej taktyki w Donbasie pokazuje, jak może wyglądać w XXI w. wojna z nowoczesnym państwem. (…) Podobnie jak badania doświadczeń izraelskich w Wojnie Sześciodniowej w 1967 r. przyczyniły się do rozwoju amerykańskiej doktryny wojskowej (US Army AirLand Battle doctrine – okazała się tak skuteczna w wojnie w Zatoce Perskiej w 1991 r.), konflikt ten (Donbas) należy zbadać w celu wypracowania najlepszych sposobów przeciwdziałania omawianym zagrożeniom biorąc pod uwagę rozwój współczesnych technologii. Wykorzystanie przez Rosję dronów, walka elektroniczna, informacyjna i cybernetyczna, wojna typu proxy, w połączeniu z intensywnymi działaniami artylerii, broni przeciwpancernej dostarczają cennych lekcji. Znaczenie zrozumienia prawdziwej natury rosyjskiej wojny hybrydowej i jej związków z sowiecką przeszłością pozwoli nam przygotować się na przyszłe działania Rosji. Choć może się to wydawać mało prawdopodobne w 2021 r., historia Rosji wskazywałaby, że będzie próbować dokonania podobnej inwazji w przyszłości. Jednym ze sposobów, aby

[428] K. Turecki, P. Jagielski *Ronen Bergman: niektórzy moi rozmówcy zostali zabici, Onet* 26 marca 2019 r. https://wiadomosci.onet.pl/tylko-w-onecie/ronen-bergman-niektorzy-moi-rozmowcy-zostali-zabici/q1f4bk3 [dostęp: 15.12.2022].

[429] Tamże.

zapobiec takiej inwazji jest zapewnienie, że nie istnieją dla niej warunki wstępne (preconditions)[430]."

Oprócz wojny w Syrii oraz innych przykładów współczesnych zagrożeń hybrydowych, odnotowywanych najczęściej przez zachodnich analityków (aneksja Krymu), w świetle wyników przeprowadzonych badań, definicje te znajdują zastosowanie także w odniesieniu do innych konfliktów. W kontekście kolejnego starcia izraelsko-palestyńskiego w maju 2021 r.[431], jak wykazały wyniki badań, zagrożenie ze strony Hamasu (a także libańskiego Hezbollahu) od wielu lat było określane przez izraelskich ekspertów wojskowych, jako zagrożenie hybrydowe. W tej wojnie Siły Obrony Izraela (IDF) walczą z organizacjami szczególnego rodzaju, które nie tylko są wyposażone w zaawansowaną technologię, ale także są wspierane przez państwowych sponsorów terroryzmu. Przeciwdziałanie temu zagrożeniu, w ich ocenie, wymaga specjalnego podejścia i ciągłego doskonalenia innowacji w strategii i taktyce wojskowej. Armia Stanów Zjednoczonych oraz siły zbrojne pozostałych krajów NATO, w tym Polski, powinny czerpać z doświadczeń Izraela i adaptować się nie mniej niż Siły Obrony Izraela[432]. Mimo zmniejszenia się aktywnego zaangażowania USA w działania wojenne (np. wycofanie wojsk z Afganistanu) walka z terrorystami i partyzantami będzie trwać dalej w ocenie Maxa Boota. Ameryka wciąż będzie zatem potrzebować zdolności przeciwdziałania zagrożeniu ze strony bojowników i partyzantki – także w ujęciu przeciwdziałania terroryzmowi w kraju i za granicą[433].

Obok Izraela, Australia i Nowa Zelandia są przykładami krajów, które także blisko współpracują z USA i innymi państwami zachodnimi stawiając czoła wzrastającym

[430] K. DeBenedictis, *Russian Hybrid Warfare and the Annexation of Crimea The Modern Application of Soviet Political Warfare*, Londyn 2022.

[431] Z uwagi na bezpieczeństwo cywilnych samolotów w strefie konfliktu, część linii lotniczych zawiesiła loty w regionie, co wynikało z obaw w kontekście zestrzelenia przez Iran ukraińskiego samolotu pasażerskiego 176 osobami na pokładzie w styczniu 2020 r.

[432] E. S. Berman, *Meeting the hybrid threat: the Israel Defense Force's innovations against hybrid enemies*, 2000-2009, Washington DC, April 16, 2010, s. 3, https://repository.library.georgetown.edu/bitstream/handle/10822/553449/bermanEleazar.pdf [dostęp: 21.05.2021].

[433] M. Boot, *America Still Needs Counterinsurgency. The "Forever Wars" Are Ending, But the Fight Against Terrorists and Guerrillas Will Go On*, Foreign Affairs, June 2, 2021, https://www.foreignaffairs.com/articles/afghanistan/2021-06-02/america-still-needs-counterinsurgency?utm_medium=newsletters&utm_source=fatoday&utm_campaign=America%20Still%20Needs%20Counterinsurgency&utm_content=20210602&utm_term=FA%20Today%20-%20112017 [dostęp: 20.06.2021].

w ostatnich latach zagrożeniom hybrydowym w regionie ze strony takich graczy takich, jak Chiny. 26 maja 2022 r. chiński myśliwiec przechwycił australijski lot nadzoru morskiego. Incydent, o którym poinformował minister obrony Australii był kontynuacją podobnych wrogich działań wobec samolotów kanadyjskich. Ten rodzaj zastraszania przez chińskie wojsko, jak zauważył Lesley Seebeck, był zwykle skierowany przeciwko innym krajom regionu (Filipinom, Malezji i Indonezji), ale aktywność hybrydowa Pekinu rozszerza się na kraje zachodnie lub ich sojuszników. W lutym 2022 r. okręty marynarki wojennej chińskiej Armii Ludowo-Wyzwoleńczej użyły lasera do namierzenia australijskiego samolotu w wyłącznej strefie ekonomicznej Australii. Takie działania wpisują się niewątpliwie w wojnę hybrydową[434].

Ekspert Centrum Wilsona w Waszyngtonie, Anne-Marie Brady, w raporcie dotyczącym chińskiej kampanii wpływu w Nowej Zelandii ukazała przypadki stosowania przez władze w Pekinie narzędzi tzw. miękkiej siły, które kwalifikują się do działań hybrydowych. Obawy profesor Uniwersytetu Canterbury wzbudziły m.in. powiązania między Pekinem, a byłymi politykami Nowej Zelandii, darowizny polityczne w wysokości setek tysięcy USD i funkcje kierownicze oferowane byłym nowozelandzkim ministrom i ich krewnym.[435] Badanie Brady nawiązuje do analiz i ustaleń przeprowadzonych przez Australijską Organizację Bezpieczeństwa i Wywiadu. W raporcie „Magiczna broń: chińskie działania polityczne pod rządami Xi Jinpinga" autorstwa Brady, zauważono, iż działania Chińskiej Republiki Ludowej mające na celu pozyskiwanie wpływów politycznych za granicą są szeroko rozpowszechnione nie tylko w Australii, ale także w Nowej Zelandii. Ten ostatni kraj, jak wskazano, także nie jest odporny na wrogie działania podmiotów państwowych lub powiązanych z państwem, które bezwzględnie wykorzystują swobodę działania w demokracjach liberalnych.

Z racji położenia geograficznego, Nowa Zelandia jest dogodnym miejscem prowadzenia badań zjawisk na dużych wysokościach, w pobliżu kosmosu. Obszar ten jest ważny dla Chin z uwagi na zastosowanie cywilne, ale także testy precyzyjnych pocisków

[434] L. Seebeck, *Indo-Pacific needs to establish a center for countering hybrid threats*, Nikkei Asia, 11.06.2022, https://asia.nikkei.com/Opinion/Indo-Pacific-needs-to-establish-a-center-for-countering-hybrid-threats [dostęp: 14.10.2022].

[435] M. Nippert, D. Fisher, *Revealed: China's network of influence in New Zealand*, NZ Herald, 20.09.2017, https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11924169 [dostęp: 14.10.2022].

dalekiego zasięgu. W tym kontekście, w swoim opracowaniu Brady zwraca również uwagę na możliwe zastosowania wojskowe testów z użyciem balonów przeprowadzonych na farmach mlecznych w Nowej Zelandii należących do firmy Shanghai Pengxin. Znaczenie Nowej Zelandii dla Chin jest istotne także w kontekście Antarktydy, odnośnie której Nowa Zelandia jest znaczącym interesariuszem[436].

Mimo braku członkostwa w NATO, Australia i Nowa Zelandia są uczestnikami sojuszu wywiadowczego Pięciorga Oczu (ang. The Five Eyes, FVEY), który obejmuje również Stany Zjednoczone, Wielką Brytanię i Kanadę. Kraje te są stronami porozumienia o wspólnej współpracy w zakresie wywiadu sygnałowego, a początki współdziałania tej grupy sięgają, co najmniej czasu II wojny światowej.

Ponadto, warto zaznaczyć, że w kontekście wzrastającego zagrożenia ze strony Chin w Azji i Pacyfiku, NATO zacieśnia stosunki z partnerami w regionie: Australią, Japonią, Republiką Korei i Nową Zelandią. Rada Północnoatlantycka regularnie spotyka się z partnerami z Azji i Pacyfiku. W czerwcu 2022 r. czterej partnerzy z regionu Azji i Pacyfiku po raz pierwszy uczestniczyli w szczycie NATO w Madrycie. W kwietniu 2022 r. ministrowie spraw zagranicznych tych krajów uczestniczyli w spotkaniu ze swoimi odpowiednikami z NATO. Było to następstwem pierwszego w historii spotkania szefów resortów spraw zagranicznych NATO z partnerami z Azji i Pacyfiku w grudniu 2020 r., podczas którego omówiono wzrost znaczenia Chin. Partnerzy NATO, w tym Australia i Nowa Zelandia, wzmacniają świadomość sytuacyjną – w tym dotyczącą zagrożeń hybrydowych – w Azji i Pacyfiku[437].

Zarzadzanie kwestiami przeciwdziałania zagrożeniom hybrydowym w Australii i Nowej Zelandii różni się jednak od rozwiązań znanych w UE i NATO. Bliska współpraca państw w tych organizacjach umożliwia kompleksowe podejście do przeciwdziałania zagrożeniom hybrydowym. Wyraża się ono w praktyce badań eksperckich tego zjawiska i wymiany informacji między partnerami. Działalność w Europie takich struktur jak Europejskie Centrum Doskonałości ds. Zwalczania Zagrożeń Hybrydowych (Hybrid CoE)

[436] Tamże.

[437] Ponadto, kraje partnerskie Azji i Pacyfiku opracowały programy współpracy, w ramach których koncentrują się na kwestiach będących przedmiotem wspólnego zainteresowania (m.in. cyberbezpieczeństwo, nieproliferacja, gotowość cywilna oraz kobiety, pokój i bezpieczeństwo). *Relations with Asia-Pacific partners*, NATO 12.06.2022, https://www.nato.int/cps/en/natohq/topics_183254.htm [dostęp: 14.10.2022].

z siedzibą w Finlandii, jest możliwe dzięki strukturom kooperacji, które już istnieją w Europie w ramach takich instytucji jak NATO i UE. W regionie Indo-Pacyfiku, gdzie leżą m.in. Australia i Nowa Zelandia, nie ma takich równoważnych regionalnych instytucji bezpieczeństwa. W przyszłości mogą się one rozwinąć m.in. na bazie będących w początkowej fazie kształtowania się struktur AUKUS[438] i Quad[439] (ewentualnie rozszerzanych o kolejne kraje)[440].

Przykład Australii pokazuje, że wzrost zagrożeń hybrydowych ze strony podmiotów państwowych i niepaństwowych stanowi wyzwanie także dla sił zbrojnych państwa broniącego się. Siły specjalne, w połączeniu z operacjami wywiadowczymi, stanowią istotne narzędzia w zakresie przeciwdziałania zagrożeniom hybrydowym. Konieczność dostosowania zdolności Australijskich Sił Specjalnych w kontekście rosnącego znaczenia konfliktów hybrydowych, zagrożeń asymetrycznych i tzw. „szarej wojny", jest zauważana przez niektórych ekspertów, takich jak generał Angus Campbell[441].

Doświadczenia takich krajów, jak Nowa Zelandia, wskazują, że dla przeciwdziałania zagrożeniom hybrydowym w domenie cyber korzystne może być zwiększenie poziomu dzielenia się informacjami przez podmioty prywatne z różnych sektorów (m.in. zdrowia, transportu infrastruktury. Firmy zwykle nie chcą jednak ujawniać przypadków wycieku lub wykradzenia danych w wyniku działania cyberprzestępców. W wielu przypadkach istnieje luka w zakresie gromadzenia właściwych danych o określonym cyberataku, co uniemożliwia policji skuteczne ustalenie sprawców i udowodnienie przestępstwa.

Warto zauważyć, że państwa mogą także stosować środki hybrydowe bez włączania się do otwartego konfliktu zbrojnego. Przykładem zastosowania takich hybrydowych metod

[438] AUKUS to porozumienie między Australią, Wielką Brytanią i Stanami Zjednoczonymi w zakresie współpracy obronnej.

[439] Quadrilateral Security Dialogue (Quad) to zainicjowany w 2007 r. dialog strategiczny na temat bezpieczeństwa między Australią, Indiami, Japonią i Stanami Zjednoczonymi.

[440] L. Seebeck, op. cit.

[441] Wojna hybrydowa, jak ocenił Stephen Kuper analizując sytuację Australii i otoczenie międzynarodowe w tym zakresie, jako „coraz potężniejsze narzędzie (…) była z powodzeniem wykorzystywana zarówno przez Stany Zjednoczone, jak i jednego z ich głównych rywali, Rosję, do skutecznego wpływania i okupowania terytoriów lub prowadzenia wojen zastępczych w celu dalszego poszerzania interesów narodowych w ważnych geostrategicznie części świata; (…) zarówno władze amerykańskie, jak i rosyjskie oskarżają się wzajemnie o prowadzenie takich operacji, które mają utrudniać wpływ i skuteczność ich znaczących zdolności konwencjonalnych, a także podważać wzajemnie bezpieczeństwo swoich narodów". S. Kuper, *Hybrid warfare and a new role for Australia's Special Forces?,* Defence Connect 4.07.2019 https://www.defenceconnect.com.au/key-enablers/4355-hybrid-warfare-and-a-new-role-for-australia-s-special-forces [dostęp:14.10.2022].

poniżej progu wojny – jako aktywnej obrony wobec kinetycznego zagrożenia – są działania Nowej Zelandii wobec agresji Federacji Rosyjskiej na Ukrainę. W marcu 2022 r. Nowa Zelandia poinformowała, że zwiększa pomoc humanitarną oraz przekaże Ukrainie nieśmiercionośną pomoc wojskową (ang. non-leathal equipment). Wyposażenie, jak poinformowano, zostanie przekazane za pośrednictwem funduszu powierniczego NATO i będzie obejmować m.in. ponad 1000 kamizelek kuloodpornych, kilkaset hełmów i kamizelek maskujących, racje żywnościowe, środki łączności, zestawy pierwszej pomocy. Zastosowano także narzędzia w postaci sankcji – rozszerzona została grupa osób/organizacji zaangażowanych pośrednio lub bezpośrednio w działania zbrojne na terytorium Ukrainy. Biorąc pod uwagę tradycyjną politykę niezaangażowania Nowej Zelandii, wprowadzone sankcje były bezprecedensowe (chociaż warto nadmienić, że Australia udzieliła prawie dziesięciokrotnie wyższego wsparcia niż strona nowozelandzka). Wpływ na nie miało niewątpliwie nastawienie sojuszników Nowej Zelandii – USA i UE – w kontekście budowania międzynarodowej koalicji państw aktywnie wspierających Ukrainę .

Mając na uwadze zaprezentowane wcześniej argumenty, należy stwierdzić, że Australia jest przykładem kraju, który skupia się na budowaniu zdecentralizowanego modelu przeciwdziałania zagrożeniom hybrydowym, w którym różne państwa narodowe przejmują wiodącą rolę w zakresie różnych rodzajów zagrożeń, opierając się na swoich mocnych stronach. W przypadku Australii oznacza to skupienie się na przeciwdziałaniu dezinformacji. Mocne strony innych krajów to przykładowo: zagrożenia morskie – Singapur, odporność infrastruktury – Japonia. Zdecentralizowany model przeciwdziałania zagrożeniom hybrydowym ma zalety postaci wysokiej specjalizacji danego kraju na zabezpieczeniu konkretnego obszaru narażonego na zagrożenia hybrydowe. Jego wadą jest natomiast ryzyko, że nie uda się stworzyć systemu świadomości i zrozumienia zagrożeń hybrydowych w całym ich zakresie[442].

Doświadczenia krajów pozaeuropejskich takich jak Izrael, Australia i Nowa Zelandia mogą wesprzeć proces usprawniania sposobów przeciwdziałania zagrożeniom hybrydowym w Polsce i w krajach euroatlantyckiej strefy bezpieczeństwa.

[442] L. Seebeck, op. cit.

3.4. Wnioski

Rozwiązania w zakresie przeciwdziałania zagrożeniom hybrydowym w Polsce i w innych krajach na świecie są zróżnicowane, ponieważ wynikają z polityki bezpieczeństwa narodowego, którą każdy suwerenny kraj kształtuje samodzielnie. Z racji przynależności Polski do NATO i UE określone rozwiązania prawne są zaimplementowane w krajowym systemie legislacyjnym; inne planuje się wdrożyć. Polska aktywnie działała w ramach tych organizacji międzynarodowych w kontekście wypracowywania nowych procedur i aktów prawnych. Cześć regulacji i rozwiązań, które występują w systemach państw pozaeuropejskich, także może zostać wykorzystana dla usprawnienia metod przeciwdziałania zagrożeniom hybrydowym w Polsce.

Państwa NATO i UE, jak zaprezentowano wcześniej, podejmują liczne działania w zakresie wsparcia aktywności związanej z obroną przed zagrożeniami hybrydowymi na poziomie narodowym. NATO było instytucją, która jako pierwsza poświęciła dużo uwagi przeciwdziałaniu zagrożeniom hybrydowym i ta sfera jest w Sojuszu znacznie bardziej zaawansowana, niż w UE. Jednak, Unia, z uwagi na znaczące możliwości odziaływania gospodarczego posiada wiele skutecznych instrumentów właściwych tylko sobie (np. sankcje ekonomiczne).

Wsparcie w zakresie przeciwdziałania zagrożeniom hybrydowym ze strony organizacji międzynarodowych może być cenne jednak jego charakter powinno się postrzegać jedynie w kategoriach uzupełnienia adekwatnie rozbudowanych zdolności krajowych. To poszczególne państwa ponoszą w pierwszej kolejności ciężar odpowiedzialności za reagowanie na tego typu zagrożenia niekonwencjonalne (podobnie, jak w przypadku wyzwań wojny konwencjonalnej)[443]. Badania dowiodły, że państwa narodowe, które posiadają odpowiednie narzędzia odziaływania (np. formacje i służby, środki komunikacji z obywatelami), dysponują najważniejszym elementem przeciwdziałania zagrożeniom hybrydowym. Zapewnienie bezpieczeństwa dla swoich obywateli stanowi podstawę funkcjonowania każdego państwa. W odróżnieniu od organizacji międzynarodowych, instytucje krajowe mogą reagować szybciej na wrogie działania hybrydowe[444]. Dla przykładu, Polska powinna zadbać o to, by narzędzia i środki UE i NATO

[443] P. Szymański, op. cit.
[444] Tamże.

były w odpowiednim stopniu angażowane w odpowiedzi na zagrożenia ze wschodu. Z punktu widzenia interesów bezpieczeństwa Polski wzmacnianie autonomii UE, powinno być komplementarne wobec gwarancji bezpieczeństwa NATO.

Izrael, Australia i Nowa Zelandia są przykładami krajów, które blisko współpracując z USA i NATO rozwijają dostosowane do swoich potrzeb autorskie metody przeciwdziałania zagrożeniom hybrydowym. Państwa pragnące usprawnić metody przeciwdziałania zagrożeniom hybrydowym powinny czerpać z doświadczeń krajów pozaeuropejskich, jak Izrael, Australia czy Nowa Zelandia, gdzie także prowadzi się prace nad doskonaleniem metod przeciwdziałania zagrożeniom hybrydowym. Atutem współpracy z tymi krajami i ewentualnego zastosowania wdrożonych przez nie rozwiązań, jest m.in. możliwość czerpania z nieszablonowego spojrzenia na kwestię przeciwdziałania zagrożeniom hybrydowym (np. polityka odstraszania Izraela, wysoki poziom specjalizacji Australii czy wymiana informacji z sektorem prywatnym władz Nowej Zelandii).

Największe znaczenie dla skutecznego przeciwdziałania zagrożeniom hybrydowym ma polityka odstraszania, którą skutecznie stosuje m.in. Izrael. Wykorzystanie koncepcji odstraszania zapewniło Izraelowi na przestrzeni dekad ochronę przed licznymi zagrożeniami hybrydowymi. Przykład Izraela, stosunkowo niewielkiego kraju o liczbie ludności nieprzekraczającej 10 milionów, pokazuje, że skuteczne odstraszanie i przeciwdziałanie znaczącym atakom jest możliwe. Oczywiście, w przypadku izraelskim, zdolności odstraszania tego kraju zostały wzmocnione dzięki wsparciu sojuszników (głównie – USA), które było zapewniane od dziesięcioleci. Przykład ten pokazuje jednak, iż jest możliwe zbudowanie skutecznej obrony przed zagrożeniami hybrydowymi i innymi w skrajnie niekorzystnych warunkach i wrogim otoczeniu oraz pozostając krajem małym.

4. Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym

Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym, jak wykazały wyniki badań, wynika z wrażliwości na nie współczesnych państw. W tym kontekście, ważnym aspektem jest skuteczność przeciwdziałania zagrożeniom hybrydowym w warunkach państwa demokratycznego. Zagrożenia hybrydowe to nowe określenie wyzwań bezpieczeństwa XXI w., które polegają na skoordynowanych i synchronizowanych działania celowo wykorzystujących luki państw i instytucji demokratycznych za pomocą szerokiego wachlarza środków.

W świetle wyników przeprowadzonych badań stwierdzić należy, że zagrożenia hybrydowe są niebezpieczne dla krajów demokratycznych z uwagi na redukowanie przez nie pola manewru rządzących, co jest dokonywane m.in. przez: uderzenie w istotę ich wartości, próbę wymuszenia podjęcia działań obronnych niezgodnych z zasadami demokratycznymi, wpływając na algorytm decyzyjny oraz doprowadzając do przesycenia systemu demokratycznego eskalacją czynników zakłócających. Państwa demokratyczne, jak wykazały wyniki badań, nie mogą być stroną inicjującą atak hybrydowy, ponieważ w tych krajach brakuje możliwości wydawania rozkazów / zadaniowania firm prywatnych. Władze krajów demokratycznych nie kontrolują ponadto mediów (poza publicznymi środkami przekazu). Państwa demokratyczne posiadają oparte o rządy prawa ograniczenia normatywne, których nie da się łatwo zmieniać. Co więcej, skryte operacje są o wiele trudniejsze do przeprowadzania i jeśli wyjdą na jaw (kontrolna funkcja parlamentu, rządy prawa) będą niosły ze sobą negatywne konsekwencje dla inicjatora.

Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika także z wyzwań w tym zakresie dla najważniejszych sojuszników Polski. Amerykańska strategia odpowiedzi na zagrożenie ze strony Rosji, jak zauważył J. Välimäki, nie uwzględnia w wystarczający sposób podejścia do wojny strony rosyjskiej, co naraża zarówno USA, jak i ich sojuszników na ryzyko strategicznych porażek w różnych lokalnych teatrach działań (*high risk of strategic defeats*). Waszyngton postrzega rosyjskie podejście do działań hybrydowych, jako operacje poniżej progu konwencjonalnego konfliktu zbrojnego. Tymczasem, Federacja Rosyjska włączyła konwencjonalny konflikt na dużą skalę w swoją koncepcję i realizację wojny hybrydowej (*Russia includes significant conventional conflict in its conception and execution of hybrid war*).

Jeśli USA, jak kontynuuje autor, będą kontynuować koncentrację wysiłków na „przeciwdziałaniu rodzajowi wojny, której dowódcy rosyjscy nie zamierzają prowadzić, przy jednoczesnym niedocenianiu roli, którą siły zbrojne mogą i powinny pełnić w zakresie udaremnienia osiągniecia przez Kreml celów za pomocą działań hybrydowych, wówczas Waszyngton ryzykuje, że może stać się stroną pokonaną[445]". Taki scenariusz staje się prawdopodobny, przynajmniej, jeśli chodzi o lokalne teatry działań / konfrontacji. Rosja, a wcześniej ZSRR, posiada długą tradycję działań niekonwencjonalnych. Termin „wojna hybrydowa" jest autorstwa zachodnich polityków i nie pochodzi z rosyjskiej myśli wojskowej. Działania ofensywne Rosji w ostatnich latach (m.in. w Gruzji, na Ukrainie w 2014 r.) były przykładami operacji z wykorzystaniem koncepcji rozwijanych od czasów sowieckich, m.in.: głębokich operacji, środki aktywne i odruchowej teorii kontroli. Byłoby błędem niedostateczne uwzględnianie tych koncepcji i próba wpasowywania działań Rosji w zachodnie konstrukcje strategii wojskowej.

Skala wyzwań stwarzanych przez działania niekonwencjonalne Rosji, jak pokazały badania, jest znacząca. Koncepcja tzw. „głębokich operacji" (ang. *deep operations*), jak przypomina Andrew J. Duncan, przedstawiciel kanadyjskiego środowiska wywiadowczego w Waszyngtonie (*Canadian Forces Intelligence Liaison Office*), zakładała, że najskuteczniejszym sposobem pokonania przeciwnika było przeprowadzenie serii ataków dotykających go w jego głębi operacyjnej (ang. *operational depth*). Było to realizowane m.in. przez stronę radziecką, która stosowała uderzenia na wiele różnych celów, włącznie z wdarciem się w strefę taktycznej obrony za pomocą sił mobilnych dalekiego zasięgu. Podejście to miało skutkować załamaniem się strony broniącej. Współcześnie, teoria głębokich operacji daje rosyjskim decydentom ramy wspierające proces integracji instrumentów dyplomatycznych, informacyjnych, militarnych i ekonomicznych[446]. Oprócz stosowania przemocy, aktywne działania polegają na: manipulacjach medialnych, dezinformacji i propagandzie. Kontrola odruchowa (ang. *reflexive control*) to teoria behawioralna, która – poprzez połączenie opisanych narzędzi walki informacyjnej – zmierza

[445] J. Välimäki, *ISIS as A Hybrid Threat Actor: From Iraq And Syria To A New Rise In Africa*, [w:] *Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence*, Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf [dostęp: 12.4.2022].

[446] A. J. Duncan, *New 'Hybrid War' or Old 'Dirty Tricks'? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment*, Canadian Military Journal, Vol. 17, No. 3, Summer 2017, http://www.journal.forces.gc.ca/Vol17/no3/PDF/CMJ173Ep6.pdf [dostęp: 22.11.2022].

do przekazania przeciwnikowi specjalnie przygotowanych danych, aby skłonić go do dobrowolnego podjęcia korzystnej dla agresora decyzji. Koncepcja ta pojawiła się w latach 60 XX w. w rosyjskiej teorii wojskowej[447]. Stosowanie przez Rosję kontroli odruchowej można było wykryć w operacjach informacyjnych podczas aneksji Krymu w 2014 r. Były one ukierunkowane, jak ocenił A. J. Duncan, na spowodowanie zamieszania i wątpliwości na poziomie międzynarodowym. Przekaz do odbiorców zewnętrznych, który można określić jako szum lub „zaśmiecanie informacyjne" (ang. *informational pollution*), był tak skonstruowany, aby wszystkie raporty medialne z regionu były niewiarygodne. Oznaczało to osłabienie działań informacyjnych USA i reszty państw NATO skierowanych do broniącej się populacji ukraińskiej, jak i międzynarodowej opinii publicznej[448].

Ponadto, potrzeba wzmocnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika także z faktu, że mają one charakter ewoluujący. Zagrożenia hybrydowe mogą stanowić niebezpieczeństwo dla danego kraju oraz ich grupy nawet jeśli dotyczą oddalonego regionu lub kraju znajdującego się na innym kontynencie. Występowanie zagrożeń hybrydowych jest coraz częściej obserwowane w Afryce stanowiąc wyzwanie dla operacji państw europejskich na tym kontynencie. Niestabilność polityczna w wielu krajach afrykańskich stanowi podatny grunt dla operacji hybrydowych. Utrudnia to działanie w już znacząco skomplikowanym przez ekstremizm i terroryzm środowisku bezpieczeństwa afrykańskiego[449].

Szybki rozwój Internetu i platform społecznościowych, który datuje się od mniej więcej roku 2000, także stanowi przesłankę zmian podejścia do zwalczania zagrożeń hybrydowych. W XIX w. istniały dwa wymiary działań wojennych, które były realizowane za pośrednictwem sił lądowych i morskich. W XX w. pojawił się trzeci wymiar – lotnictwo. Natomiast rozwój technologii komputerowych w wieku XXI przyniósł czwarty wymiar: prowadzenie działań zbrojnych – w sferze cyfrowej (Internet, technologie satelitarne i pochodne). Początkowo dostęp do stron internetowych był możliwy wyłącznie za pomocą komputerów. Około 2015 r. nastąpił rozwój dostępu do Internetu i powiązanych usług za pomocą urządzeń mobilnych jak nowoczesne telefony (ang. *smartfon*). Liczba urządzeń,

[447] Tamże.
[448] Tamże.
[449] G., Faleg, N. Kovalčíková, *Rising Hybrid Threats in Africa. Challenges and implications for the EU*, 3 March 2022 https://www.iss.europa.eu/content/rising-hybrid-threats-africa [dostęp 13.4.2022].

która korzysta z Internetu przewyższyła liczbę ludzi dlatego pojawiło się zjawisko Internetu rzeczy. Natura tych urządzeń ewoluuje coraz bardziej w kierunku niezależnego, autonomicznego działania z wykorzystaniem sztucznej inteligencji. Ta rewolucja – dotykając wszystkich aspektów życia społecznego – dotyczy także sfery bezpieczeństwa[450].

Jak wykazały wyniki badań, cyberataki nie są zjawiskiem statycznym, ale dynamicznie ewoluują, dlatego wymagają adekwatnej odpowiedzi. Środki przeciwdziałania zagrożeniom hybrydowym w obszarze cyber muszą nadążać za szybkim rozwojem tego rodzaju zagrożeń. Wśród zalewu bardzo zróżnicowanych cyberincydentów, najbardziej niebezpieczne ataki cybernetyczne pochodzą ze strony państw lub są przez nie inspirowane. Rozwój zdolności ofensywnych zrobił ogromny postęp w ostatnich latach (zwłaszcza w okresie 2010-2020). Działania cybernetyczne zostały na stałe włączone do arsenału środków prowadzenia działań hybrydowych i wojennych przez siły zbrojne wielu krajów. Przyszłość może zawierać wzrost zagrożeń ze strony sztucznej inteligencji (AI) w zaprezentowanym wcześniej kontekście[451].

4.1. Znaczenie przeciwdziałania zagrożeniom hybrydowym

W świetle wyników przeprowadzonych badań wykazano, że środowisko bezpieczeństwa należy postrzegać w kategoriach dynamicznych – procesu, a nie stanu. Dokonują się w nim zmiany charakteru graczy poziomu ambicji największych państw, zmian uwarunkowań środowiska technologicznego. Same zagrożenia hybrydowe, stanowiące element środowiska bezpieczeństwa danego państwa, są zatem także procesami o naturze dynamicznej, a nie statycznej. Zagrożenia hybrydowe odnoszą się do szerokiego spektrum metod i działań używanych przez wrogie podmioty państwowe i pozapaństwowe w skoordynowany sposób w celu wykorzystania słabych punktów. Poza cały czas aktualnymi zagrożeniami hybrydowymi związanymi z kampanią hybrydową Rosji i aneksją Krymu w 2014 r., różne rodzaje działań hybrydowych (m.in. cyberataki, dezinformacja, ale także manipulacja rynkiem energii, czy instrumentalizacja migracji), stanowiły w ostatnich latach rosnące wyzwanie dla Polski i pozostałych państw członkowskich UE i krajów NATO. Dezinformacja wymierzona w kraje europejskie dotyczyła w ostatnich latach głównie pandemii COVID-19, służyła zwłaszcza podważeniu roli szczepień. W jej szerzenie angażowały się przede wszystkim Chiny i Rosja. Za

[450] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

[451] Tamże.

głównego aktora hybrydowego państwa członkowskie UE i NATO, a wiec pośrednio także Polska, uznawały w ostatnich latach Rosję, ale coraz więcej uwagi poświęcano presji (zwłaszcza informacyjnej, gospodarczej) ze strony Chin, a także innych państw (np. Turcja, Białoruś). W ujęciu uwzględniającym pozycję – usytuowanej obecnie w euroatlantyckich strukturach bezpieczeństwa – Polski, celami aktorów hybrydowych są m.in.:

a) osłabianie państw Zachodu i ich modelu rządów demokratycznych;
b) manipulowanie państwami zachodnimi i prowokowanie do podejmowania przez nie niewłaściwych decyzji;
c) uzyskiwanie przewagi w geopolityce i w międzynarodowych strukturach władzy;
d) ochronę wewnętrznej legitymacji swojej (autorytarnej) władzy[452].

Intensywność wykorzystania działań hybrydowych można porównać do wzrostu zagrożenia terroryzmem po atakach 9/11, które wymagały przeformułowania niemal całego podejścia do obrony. W efekcie, po raz pierwszy użyto artykułu 5 Traktatu Waszyngtońskiego. Poważny atak hybrydowy może i powinien wywołać reakcję obronną z wykorzystaniem sojuszniczej obrony w ramach NATO[453].

Po okresie wieloletniego zaangażowania i rozwoju polskich i zachodnich sił zbrojnych oraz innych służb i formacji w kierunku przeciwdziałania terroryzmowi, zagranicznym misjom ekspedycyjnym i wojnie partyzanckiej (po 9/11), ponowne pojawienie się Rosji jako otwartego przeciwnika jest dla Zachodu zjawiskiem niepożądanym. Tym bardziej wskazane jest, aby w sposób pełny zrozumieć to zagrożenie. Wrogie działania Kremla, zwłaszcza od aneksji Krymu, można było odczytywać, jako zagrożenie hybrydowe. Jednak rok 2022 pokazał, iż przekształciło się ono w wojnę, co pokazuje znaczenie właściwego rozpoznania i zwalczania zagrożeń hybrydowych[454]. Zlikwidowane w początkowym etapie, mogą stanowić ważny sygnał zniechęcający agresora do działań zakrojonych na szerszą skalę (np. otwarty konflikt zbrojny – wojna).

Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika także z ich złożonego charakteru. Rosja, która w ocenie zachodnich polityków jest odpowiedzialna

[452] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*
[453] M. N. Schmitt, *Counter-Terrorim and the Use of Force in International Law*, The Marshall Center Papers, No 5, 2002, s. 17-18.
[454] Zob. więcej: A. J. Duncan, op. cit.

za szereg ataków hybrydowych z użyciem środków cybernetycznych, poinformowała, że sama jest ich ofiarą. Już miesiąc po agresji na Ukrainie przedstawicie Federacji Rosyjskiej oznajmili, że obserwują wzrost liczby cyberataków na organy rządowe, media, obiekty infrastruktury krytycznej, za które obwinili – jak to określi – armię zagranicznych cyberhakerów. Bezprecedensowa skala działań i ich skoordynowany charakter, jak oświadczyło rosyjskie Ministerstwo Spraw Zagranicznych, wskazują, że „oprócz ukraińskich sił specjalnych szkolonych przez Stany Zjednoczone i inne siły NATO, w wojnę cybernetyczną przeciwko nam coraz bardziej zaangażowani są anonimowi hakerzy i prowokatorzy działający na zlecenie zachodnich mocodawców kijowskiego reżimu". Mają oni, w ocenie Moskwy, określone zadania bojowe, często graniczące z jawnym terroryzmem. Strona rosyjska zapewniła, że wyspecjalizowane instytucje skutecznie przeciwdziałają tym atakom i odpowiadają na nie w zdecydowany sposób. Rosja przestrzegła także osoby mogące angażować się we wrogą dla niej działalność typu hybrydowego, że źródła ataków zostaną zidentyfikowane, a sprawcy nieuchronnie, zgodnie z prawem poniosą odpowiedzialność za swoje czyny[455].

Argumentem za jest także nasilone wykorzystanie środków masowego przekazu do ataków hybrydowych w postaci dezinformacji. Kraje będące agresorami w wymiarze hybrydowym starają się przeciwdziałać takiemu ich postrzeganiu na arenie międzynarodowej. Niektóre z nich zainwestowały znaczące środki finansowe w rozwój globalnych środków masowego przekazu, a nawet uczelnie, aby zmienić niekorzystny dla siebie obraz funkcjonujący w sferze publicznej. Mimo, że związek tych sfer z bezpieczeństwem nie jest bezpośredni, długoterminowo wpływają one w strategiczny sposób na jego poziom[456]. Przykładem jest rosyjska stacja telewizyjna Russia Today. W efekcie przeprowadzonych badań stwierdzono, że środki masowego przekazu, którymi dysponują państwa, mają duże znaczenie w zakresie kształtowania pozytywnego dla nich obrazu rzeczywistości, co jest istotnym elementem działań hybrydowych. Władze w Moskwie doskonale to rozumieją, co znajduje wyraz w rosnących od wielu lat wpływach tego rodzaju mediów na międzynarodowym rynku informacji. Russia Today (RT), jak to

[455] *MSZ Rosji: Armia cybernajemników prowadzi przeciwko nam wojnę, Rzeczpospolita,* 29.03.2022, https://www.rp.pl/dyplomacja/art35965491-msz-rosji-armia-cybernajemnikow-prowadzi-przeciwko-nam-wojne [dostęp: 12.10.2022].

[456] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

określiła redaktor naczelna tej stacji telewizyjnej M. Simonian, jest potrzebna Rosji, tak samo, jak Ministerstwo Obrony. Znalazło to wyraz we wsparciu państwa dla Russia Today, które szacuje się na 1,3 miliarda USD. Efektem jest ponad 760 tys. artykułów rocznie oraz globalny zasięg obejmujący ponad 100 państw na 5 kontynentach (6 wersji językowych, 8 kanałów, Russia Today działa także w pobliżu USA – ogromny wzrost popularności w Ameryce Południowej). Model rozwoju rosyjskich mediów w Ameryce Łacińskiej (Russia Today, Sputnik) polegał na początkowej koncentracji na nadawaniu popularnych tam wydarzeń sportowych (głównie piłki nożnej), aby potem – po zbudowaniu znaczącej bazy odbiorców – przemycać treści polityczne korzystne dla Kremla. Dla porównania, budżet unijnej komórki East StratCom Task Force wynosi zaledwie 20 milionów EUR. Dezinformacja, rozumiana jako cześć działań o charakterze hybrydowym, poniżej kinetycznego progu wojny, jest więc naturalnym orężem Kremla w swoich operacjach (także w trakcie wojny na Ukrainie). Oprócz mediów państwowych, jak wykazały wyniki badań, należy wskazać na rozległe powiązania pozornie niezależnych nadawców z rosyjskimi biznesmanami lub nawet służbami specjalnymi. Ponadto, zidentyfikowano znaczne nasycenie źródeł Wikipedii treściami pochodzącymi od mediów zależnych – pośrednio lub bezpośrednio – od aparatu państwowego Federacji Rosyjskiej, co także jest niebezpieczne w kontekście potrzeby zachowania bezstronności przekazu w szczególnie popularnych internetowych źródłach encyklopedycznych tego typu[457]. Rosyjskie placówki dyplomatyczne są w naturalny sposób intensywnie wykorzystywane jako narzędzie kremlowskiej propagandy. Coraz częściej zakładane są konta na alternatywnych platformach społecznościowych, w tym VK czy Telegram. Rosyjska machina dezinformacyjna zintensyfikowała kolportowanie treści w mediach społecznościowych również za pośrednictwem placówek dyplomatycznych. Zespół EUvsDisinfo, opisując modus operandi Rosji w zakresie dezinformacji, zaproponował akronim SWAMPED (z znaczeniu – zalanie informacjami), który dobrze oddaje istotę tego zjawiska. Poszczególne litery reprezentują konkretne działania:

- straw man – strach na wróble (atakowanie poglądów przeciwnika – wmawiając mu cechy, których nie posiada);

[457] *Dezinformacja jako główna oś kampanii hybrydowych,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

- whataboutism (odrzucenie oskarżenia przy jednoczesnym oskarżeniu go o podobne postepowanie, np. „A co USA robiły na Bliskim Wschodzie?", „Rosja nie ma historii kolonialnej, a kraje zachodnie – tak");
- atak (stosowanie brutalnego języka służącego zastraszeniu przeciwnika / użytkownika forum lub portalu społecznościowego);
- mockery (szyderstwo);
- prowokacje;
- exhaust (wyczerpanie – uwagi odbiorcy poprzez zalanie przestrzeni informacyjnej nieistotnymi lub fałszywymi przekazami);
- denial (zaprzeczenie)[458].

W rosyjskich działaniach dezinformacyjnych, jak ustalili unijni specjaliści, wciąż powtarza się schemat: zaprzeczania, oskarżeń, przerzucania winy oraz rozproszenia uwagi. Ważną taktyką jest też wprowadzanie szumu informacyjnego, aby rozmyć skuteczność odbioru ważnych informacji w atakowanym kraju.

Narracje dotyczące Polski koncentrowały się na atakach zmierzających do pogorszenia relacji polsko-ukraińskich, zawierających informacje antagonizujące Polaków i Ukraińców oskarżające o rasizm, eksploatujące tragiczne wydarzania historyczne między oboma społeczeństwami. Rozpowszechniane były twierdzenia dotyczące rzekomej chęci przejęcia terytorium zachodniej Ukrainy przez Polskę. Na początku marca 2022 r. popularność w sieci zdobywały twierdzenia dotyczące rzekomej segregacji uchodźców na granicy polsko-ukraińskiej ze względu na pochodzenie. Regularnie pojawiają się twierdzenia dotyczące rzekomej niechęci Polaków wobec Ukraińców czy uprzywilejowanego traktowania uchodźców z Ukrainy w Polsce. Eksplorowanie zaszłości historycznych, w tym dotyczących ukraińskich zbrodni na Wołyniu to motyw regularnie powtarzany i zdobywający popularność w mediach społecznościowych[459].

Dezinformacja, jak wykazały wyniki badań, jest także elementem działań hybrydowych służących instrumentalizacji migracji. „Władze białoruskie wykorzystują migrantów jako instrument presji politycznej, czemu towarzyszy szeroko zakrojona

[458] Tamże.
[459] Tamże..

kampania dezinformacyjna", jak zauważył Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa Josep Borrell, w czasie nasilenia kryzysu migracyjnego w listopadzie 2021 r. Oprócz fizycznego zorganizowania sztucznych rzesz uchodźców i zmuszeniem ich do szturmowania przejść granicznych z Polską i Litwą, agresorzy stosowali także instrumentarium dezinformacyjne. Pojawiały się fałszywe twierdzenia, że kryzys migracyjny jest konsekwencją destrukcyjnej polityki państw Zachodnich na Bliskim Wschodzie. Wskazywano, że migranci są wymówką dla Polski po to, aby zgromadzić wojska na granicy. Utrzymywano, że wina nie leży po stronie Białorusi, która nie wypowiedziała wojny hybrydowej. Sytuacja jest natomiast wynikiem bezmyślnej polityki Zachodu oraz porażki UE w przestrzeganiu własnych wartości. Kreatywność autorów fałszywych narracji była znacząca ("Polscy funkcjonariusze pobili Kurdyjkę, która w efekcie straciła dziecko", "Polscy żołnierze otwierają ogień do migrantów" itp.). Model przekazów bazował na założeniu: „dobrzy Białorusini" kontra „źli Polacy". Co więcej, publikując zdjęcia polskich funkcjonariuszy Straży Granicznej (określanych przez agresora mianem "Polskich katów") wraz z danymi personalnymi próbowano zastraszyć ich przed sumiennym wykonywaniem obowiązków związanych z ochroną granicy[460].

Zarzuty wobec Polski. wysuwane przez zbiegłego żołnierza Emila Czeczkę, obejmowały m.in. twierdzenia:

a) rzekomych masowych egzekucjach dokonywanych przez SG i WP na migrantach (w tym na kobietach i dzieciach) oraz wolontariuszach;
b) upijaniu i narkotyzowaniu żołnierzy przez dowódców;
c) wskazujące że Polska stara się zdyskredytować Czeczkę, który mówił prawdę;
d) okrucieństwach wobec migrantów inspirowanych przez polskie służby specjalne[461].

Dezinformacja jest także stosowana przez agresorów hybrydowych na potrzeby wewnętrzne. Jak wykazały wyniki badań, publiczny dostęp do wiarygodnych informacji w Rosji kurczył się w szybkim tempie. Kreml próbuje zająć przestrzeń informacyjną,

[460]Tamże.
[461] Tamże.

zalewając ją sprzecznymi wersjami wydarzeń. Celem jest nie tylko odwrócenie winy, ale także prewencyjne kształtowanie narracji w celu i dyskredytowania wszelkich dowodów lub śledztw w sprawie rosyjskich zbrodni wojennych na Ukrainie. Jedną z powtarzających się narracji w czasie agresji rosyjskiej w 2022 r. były oskarżenia o złe traktowanie cywilów przez Ukraińców, w tym wykorzystywanie ich jako "ludzkich tarcz". Regularnie pojawiały się materiały mające ośmieszyć prezydenta Zelenskiego i podważyć jego wiarygodność. Kolportowane są również narracje dot. jego rzekomej ucieczki z Ukrainy. W tym celu wykorzystuje się m.in. sfabrykowane fotografie czy technologię zaawansowanego fałszowania rzeczywistości (deepfake). Realizowany jest także fałszywy fact checking. Profil „War on Fakes", który przedstawia się jako obalający „wojnę informacyjną przeciwko Rosji", tak naprawdę rozpowszechnia dezinformację i propagandę pod fasadą ośrodka sprawdzającego fakty. Dane Telegram Analytics wskazują , że konto War on Fakes powstało 23 lutego , czyli dzień przed inwazją Rosji na Ukrainę. Celem fałszywej operacji fact checkingowej było m.in. wzbudzenie wątpliwości wśród rosyjskojęzycznych widzów, napotykających w sieci na niekorzystne dla Rosji przekazy[462].

Skalę wyzwań związanych z dezinformacją i aktywnością prorosyjskich narracji w Europie pokazuje przykład Słowenii. W tym kraju byłej Jugosławii wiosną 2022 r. nastąpił wzrost lewicowej, pacyfistycznej i prorosyjskiej narracji w środkach masowego przekazu (apele profesorów, organizacja antyrządowych wiecy społeczno-politycznych). W przestrzeni medialnej pojawiały się ponadto informacje o próbach wstrzymywania dostaw czołgów dla Ukrainy. Dostawy te, określone kręgi w słoweńskim wojsku uzależniały od przekazania sprzętu zastępczego z Niemiec. Za niezrozumiałe troski o bezpieczeństwo kraju należy uznać pojawiające się wówczas w przestrzeni medialnej głosy krytykujące opisane podejście na bazie argumentu, że posiadane przez słoweńską armię czołgi miały być wykorzystywane jedynie do ćwiczeń i trudno uznać je jako ważny element sił obronnych tego kraju. Każdy element uzbrojenia i wyposażenia sił zbrojnych ma znaczenie dla obrony danego kraju, zwłaszcza w tak nieprzewidywalnej sytuacji, jaka miała miejsce po inwazji Federacji Rosyjskiej na Ukrainę w 2022 r.

Potrzeba usprawnienia metod przeciwdziałania zagrożeniom hybrydowym wynika także z braku pełnej zgodności krajów UE i NATO w stosunku do polityki względem Rosji. Już

[462] Tamże.

po rozpoczęciu wojny na Ukrainie w 2022 r. we Włoszech planowano przeprowadzenie kampanii przeciwdziałającej tworzeniu w pełni negatywnego wizerunku Rosji (ukazywanie rosyjskiej kultury, dorobku cywilizacyjnego itp.). Także działania władz najważniejszych krajów UE pokazują, że nie ma tam woli jednoznacznego zerwania swoich relacji z Rosją, która bezpośrednio zagraża wschodniej flance zarówno UE jak i NATO[463]. Współpraca UE oraz Organizacji Traktatu Północnoatlantyckiego – jak dowodzi Aleksander Olech, stypendysta francuskiego Université Jean Moulin Lyon 3 i Fundacji im. Kazimierza Pułaskiego – jest kluczowa w skutecznym przeciwdziałaniu zagrożeniom hybrydowym i powinna być priorytetem w ramach wspólnych działań na rzecz bezpieczeństwa obu organizacji[464]. UE i NATO posiadają instrumenty do budowania bezpieczeństwa w Europie, zwłaszcza w otoczeniu krajów członkowskich położonych na wschodniej flance obu organizacji. Instrumentem w tym zakresie, powinna być intensyfikacja prac umożliwiających połączone misje zagraniczne UE i NATO, co umożliwiłoby skuteczne przeciwdziałanie zagrożeniom hybrydowym i terrorystycznym zanim dotrą one na kontynent europejski. Wśród przeszkód w zakresie współpracy UE i NATO. A. Olech, wymienia strukturalne trudności w szybkim uzgadnianiu zadań z podmiotami w poszczególnych krajach członkowskich, zbyt wolne tempo wymiany informacji między UE i NATO, co prowadzi do nieefektywnych, opóźnionych reakcji oraz brak ujednoliconej strategii zwalczania zagrożeń hybrydowych w różnych regionach (Europa Środkowa, Afryka, Bliski Wschód)[465].

Jak wykazały wyniki badań, szkodliwe działania w sferze informacyjnej często były powiązane z atakami cybernetycznymi. Rosła liczba ataków *ransomware*[466], w tym na infrastrukturę krytyczną, dokonywanych przez cyberprzestępców powiązanych z Rosją. W kwietniu 2021 r. USA przypisały Rosji przeprowadzenie masowej, cybernetycznej kampanii szpiegowskiej (*SolarWinds*). Choć USA były jej głównym celem, to cyberatak stał się incydentem międzynarodowym (oprogramowanie amerykańskiej firmy jest dystrybuowane globalnie)[467].

---

[463] Tamże.

[464] A. Olech, *Współpraca NATO i Unii Europejskiej w obliczu zagrożeń hybrydowych, ze szczególnym uwzględnieniem terroryzmu, Instytut Nowej Europy*, 11 grudnia 2020, https://ine.org.pl/wspolpraca-nato-i-unii-europejskiej-w-obliczu-zagrozen-hybrydowych-ze-szczegolnym-uwzglednieniem-terroryzmu/ [dostęp: 29.11.2022].

[465] Tamże.

[466] Polegają one na blokowaniu przez hackerów określonych systemów komputerowych i najczęściej żądanie okupu za ich odblokowanie.

[467] Reagując na rosnącą skalę cyberataków, UE zadeklarowała solidarność z USA w związku z wykryciem kampanii *SolarWinds*. We wrześniu 2021 r., wobec ataku *Ghostwriter* i połączonej z tymi

Cyberatak[468] może dla przykładu sparaliżować logistykę przeciwnika zakłócając dostawy kluczowych produktów i sprzętu na potrzeby sil zbrojnych, co utrudni prowadzenie działań zbrojnych. To może mieć większe znaczenie dla wyniku wojny lub jej kluczowego etapu niż spektakularny atak na system dowodzenia lub inne obiekty infrastruktury krytycznej. W czasie inwazji Federacji Rosyjskiej na Ukrainę w 2022 r. zaobserwowano intensywne ataki cybernetyczne na instytucje ukraińskie. W określonych przypadkach, kryminale z pozoru ataki cybernetyczne mogą być w istocie zlecone przez państwo zainteresowane osłabieniem przeciwnika za pomocą technik hybrydowych. Atakujący pozostaje w ukryciu w tym przypadku i jego wykrycie w początkowej fazie ataku może być bardzo utrudnione, jeśli nie w praktyce niemożliwe. Niektóre z narzędzi mających zastosowanie przy atakach hybrydowych, zwłaszcza cybernetycznych oraz dezinformacji, mogą być zakupione za pomocą ukrytej sieci internetowej Dark Web. To część Internetu, do której nie można uzyskać dostępu przez standardowe przeglądarki. Umożliwia ona skryte nabycie różnych produktów i usług, które są w większości nielegalne (m.in. broń palna, fałszywe karty kredytowe, prawa jazdy i paszporty, narkotyki, operacje hackerskie). Mimo, że narkotyki są nadal najczęstszym zakupem w Dark Web, to szybko rozwijają się usługi, które mogą posłużyć, jako element kampanii hybrydowej (np. złośliwe oprogramowanie, hakerzy do wynajęcia) [469].

W wyniku przeprowadzony badań stwierdzono, że potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika także z innowacyjnych i trudnych do wykrycia i zneutralizowania komputerowych metod z użyciem wysokich technologii. Cyberataki są obecnie coraz bardziej istotnym elementem kampanii hybrydowych. Wynika to

działaniami kampanii dezinformacyjnej, Wysoki Przedstawiciel UE ogłosił deklarację przyjętą w ramach mechanizmu *EU Cyber Diplomacy Toolbox.* Stanowiło to wspólną reakcję UE-27 i wyraz solidarności. *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

[468] Cyberprzestepczość, o czym warto pamiętać, może być jednak nie tylko instrumentem aktorów wykorzystujących go, jako oręż walki hybrydowej, ale także może stanowić cel sam w sobie (służący np. kradzieżom mienia, szantażowi, uzyskiwaniu okupu). Przypadki działalności na szkodę przedsiębiorców i osób prywatnych są coraz częściej odnotowywane wraz z postępem digitalizacji życia współczesnego społeczeństwa. Obecnie, jak wykazały wyniki badań, można zakupić za niewygórowane kwoty specjalne narzędzia hackerskie (boty), które mogą zainfekować nawet 1 milion urządzeń. Transakcji tego typu istnieje m.in. na internetowym czarnym rynku w postaci sieci, takich jak Dark Net / Dark Web. *Cybersecurity & Cyber Diplomacy*, European Security Defence College 2022.

[469] Aby uzyskać dostęp do ciemnej sieci wymagane jest specjalistyczne oprogramowanie (open source), takie jak „Tor". Użytkownicy tego czarnego rynku polegają na swoich unikalnych pseudonimach w celu ustalenia tożsamości i budowania reputacji. Zarządzanie wiarygodnością kontrahentów jest jednym z najważniejszych elementów transakcji, ponieważ zmniejsza ryzyko namierzenia danego sprzedawcy przez organy ścigania. Największe rynki Dark Web zatrudniają pełną obsługę klienta i opracowały wysoce zaawansowane platformy technologiczne i sprzedażowe. *Cybersecurity & Cyber Diplomacy*…

z rozpowszechnienia się informatyzacji i cyfryzacji procesów istotnych dla administracji państwowej, firm oraz funkcjonowania społeczeństw w obecnym kształcie. Przypadek cyberataków w ramach kampanii „GhostWriter", która miała na celu uderzenie w wiele państw Europy Środkowej i Wschodniej (m.in. w Polskę), był znaczący w tym kontekście. „GhostWriter" była skoordynowaną kampanią dezinformacyjną realizowaną przy wykorzystaniu narzędzi cyfrowych (cyber ataków) na osoby publiczne, instytucje. Ta seria cyberataków wymierzonych w polityków i instytucje demokratyczne, dotknęła m.in. Niemcy i Polskę. Agresorzy wykorzystali w niej takie działania, jak kradzież prywatnej korespondencji elektronicznej, jej modyfikację / sfałszowanie i upublicznianie w celach dezinformacyjnych czy przejmowanie kont w mediach społecznościowych. Analizą i budowaniem świadomości na temat tego zagrożenia zajmuje się w Polsce m.in. CERT.

W toku badań stwierdzono, że działalność grupy „GhostWriter" rozpoczęła się w 2016 r., na krótko po zakończeniu szczytu NATO, jak wynika z informacji firmy Mandiant[470]. Za atakami hybrydowymi „GhostWriter', jak wykazały wyniki badań, stała białoruska grupa o nazwie UNC1151, a ich celem było dokonanie szkód w atakowanych państwach za pomocą narządzi hybrydowych. Grupa „GhostWriter" była znana z działań aktywnych koncentrujących się z zwłaszcza na personelu wojskowym[471]. Nazwę grupy (w tłumaczeniu – „Autor Widmo") zaczerpnięto ze schematu jej działania, który polegał na uzyskiwaniu dostępu do stron internetowych mediów np. poprzez wykradanie danych do logowania. Dzięki działalności hackerów dokonywano kradzieży tożsamości/loginów/haseł osób publicznych (także do późniejszych działań), wywoływanie szumu informacyjnego oraz niepokojów społecznych, polaryzowanie dyskursu społecznego, podważanie przynależności do struktur NATO i obecności wojsk sojuszniczych. Realizowana była w ten sposób strategia inicjatorów tych działań[472]. Kampanię, która była przykładem cyberszpiegostwa, oparto o takie metody cyberataków, jak kradzież danych / haseł do logowania (Phishing / Spear-phishing), wykorzystywanie złośliwego oprogramowania (malware). Dochodziło do tworzenia sfałszowanych materiałów (m.in. pism, maili, artykułów), które były rozpowszechniane w różny sposób. Miało miejsce tworzenie fikcyjnych profili w mediach społecznościowych („ekspertów", „dziennikarzy") oraz rozpowszechnianie „fake news" na nielegalnie przejętych portalach. Poprzez przechwycone strony

[470] *Cyberataki jako element kampanii hybrydowych…*
[471] Tamże.
[472] Tamże.

internetowe oraz konta w mediach społecznościowych „GhostWriter" uwiarygodniała fikcyjnych „ekspertów" (Twitter, Facebook, Instagram).[473] Pierwszymi ofiarami ataków padły Łotwa, Litwa oraz Polska.

Główny nacisk wczesnego etapu działań „GhostWriter" był położony na dyskredytację NATO ze szczególnym naciskiem na przeciwdziałanie obecności sojuszniczej w krajach wschodniej Europy. Zidentyfikowano ponad 10 operacji skierowanych m.in. wobec Łotwy i Litwy z użyciem kilkunastu sztucznie wygenerowanych profili „dziennikarzy" i „ekspertów". Profile te wykorzystywano następnie do rozpowszechniania dezinformacji[474]. Charakter poszczególnych ataków był zróżnicowany (podważanie decyzji po szczycie NATO w lipcu 2016 r., fałszywe oskarżenie o szpiegowanie na rzecz Rosji dowódcę niemieckiego kontyngentu wojskowego na Litwie w 2017 r., zarzucanie przygotowywania ataku na Białoruś organizatorom ćwiczeń NATO pk. ANAKONDA 2018, sfabrykowane zarzuty o napaść na tle seksualnym pod adresem litewskiego ministra obrony narodowej – 2018 r. oraz rzekome zbezczeszczenie przez niemieckich żołnierzy cmentarza żydowskiego na Litwie w 2019 r.[475]

Polska także stała się celem kampanii „GhostWriter". Pierwszy znany atak miał miejsce w kwietniu 2020 r. kiedy to przejęto kontrolę nad stroną internetową Akademii Sztuki Wojennej. Umieszczono na niej wówczas sfabrykowany list rektora, wzywający do buntu przeciwko współpracy z NATO. Nasilenie działań grupy stojącej za „GhostWriter" nastąpiło po nieuznanych przez Zachód wyborach prezydenckich na Białorusi oraz po zdecydowanym poparciu Polski dla białoruskiej opozycji (wybory w sierpniu 2020 r.). Jesienią 2020 r. doszło do przejęcia licznych kont mailowych oraz w mediach społecznościowych osób publicznych: parlamentarzystów, dziennikarzy, członków rządu RP oraz aktywistów z organizacji pozarządowych[476]. Miało miejsce utworzenie dedykowanego kanału na rosyjskim portalu Telegram do rozpowszechniania rzekomych maili wykradzionych z prywatnej skrzynki min. Dworczyka. Dodatkowym zagrożeniem było w tym przypadku fałszowanie wykradzionych wiadomości pocztowych, co

[473] Tamże.
[474] Tamże.
[475] Tamże.
[476] Do przykładów ofiar grupy stojącej za „GhostWriter" zaliczyć można ministrów: Michała Dworczyka i Marlenę Maląg; posłów m.in. Marcina Duszka, Marka Suskiego, marszałek Sejmu Elżbietę Witek, dziennikarzy: Tomasza Sakiewicza, Agnieszkę Kamińską; media – strony internetowe Tygodnika Solidarność.

wprowadzało dodatkowy chaos oraz dezinformację. Mogło to być ujawnione dzięki analizie tzw. metadanych przez zachodnich specjalistów analizujących te fałszywki[477].

Widoczna byłą synchronizacja działań w Polsce i na Litwie. Np. w kwietniu 2021 r. z przejętego konta A. Kamińskiej (Radio) krytykowano praktykę wspierania finansowego przez Zachód opozycjonistów białoruskich przebywających w Polsce. W tym samym czasie na Litwie trwał atak informacyjny przeciwko białoruskim opozycjonistom: Swiatłanie Cichanouskiej i Pawłowi Łatuszce[478].

Ataki przeprowadzono takie na inne państwa, m.in. .Niemcy i Ukrainę. Mimo wzrostu świadomości grupa kontynuowała działalność i polscy użytkownicy nadal są narażeni na ataki oraz dezinformację (według stanu na 1.12.2022 r., portal „Poufna Rozmowa" pod adresem https://poufnarozmowa.top/ nadal funkcjonował). Sytuacja ta, biorąc pod uwagę dominację USA w obszarze kontroli światowych zasobów Internetu, pokazuje skalę wyzwań dla krajów takich jak Polska. Ponadto, intensywne działania grupy UNC1151 nastąpiły po rosyjskiej inwazji na Ukrainę w 2022 r. Metody ataków były stale doskonalone. Jedną z nich, jest tzw. przeglądarka w przeglądarce, która polega na instalacji specjalnej nakładki na prawdziwą stronę internetowa[479]. Ponadto, ofiarą intensywnej kampanii dezinformacyjnej stały się też Czechy po tym, jak przypisały Rosji przeprowadzenie akcji sabotażowej w 2014 r. (eksplozja magazynu amunicji). W czerwcu 2021 r. na Litwę zaczęli napływać nielegalni imigranci, sprowadzeni do Europy przez Białoruś (co z kolei stanowiło odwet A. Łukaszenki za sankcje unijne nałożone po zmuszeniu do lądowania rejsowego samolotu linii Ryanair). Od września 2021 r. takie same działania Białoruś podjęła wobec Polski. Ponadto, istotne zagrożenie stanowiły działania wojskowe poniżej progu wojny, które uwidoczniły się w 2021 r. w postaci koncentracji wojsk rosyjskich na granicy z Ukrainą, nietransparentnych ćwiczeń ZAPAD oraz niebezpiecznych manewrów okrętów i samolotów)[480].

O potrzebie usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym świadczy też wykorzystanie przez agresorów bardzo groźnego, nowego instrumentarium – broni migracyjnej. Wydarzenia takie jak nieuznanie przez kraje zachodnie wyborów prezydenckich na Białorusi (zarzut fałszerstwa), próby odsunięcia od władzy Łukaszenki przez ludność wychodzącą na ulicę czy represje i zdecydowane stłumienie protestów przez reżim w Mińsku

[477] *Cyberataki jako element kampanii hybrydowych....*
[478] Tamże.
[479] Tamże.
[480] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

(m.in. przymusowe lądowanie samolotu Ryanair), zainicjowały kolejną fazę zbliżenia Rosji i Białorusi. W kilka miesięcy po wymienionych wyżej zajściach, nastąpiło wywołanie sztucznego kryzysu migracyjnego na granicy z Polską. Białoruś znalazła się niemal całkowicie pod kontrolą Rosji, o czym świadczy zgoda Mińska na stacjonowanie wojsk rosyjskich na terenie tego kraju. Kontrolowane w sensie formalno-prawnym prze Mińsk terytorium oraz siły zbrojne powinny być w tym sensie traktowane jako element machiny wojennej Federacji Rosyjskiej. Prawdopodobne jest dalsze zwiększenie obecności ofensywnych sił rosyjskich na Białorusi, włącznie z rozmieszczeniem broni atomowej na jej terytorium.

Usprawnienie sposobów przeciwdziałania zagrożeniom hybrydowym jest wymagane także z uwagi na ich kompleksowy charakter, co stanowi bezprecedensowe wyzwanie dla współczesnego państwa i wymaga jego odpowiedniej reakcji obronnej. Złożoną naturę wyzwań generowanych przez zagrożenia hybrydowe przedstawili S. Jasper i S. Moreland, którzy stwierdzili, że charakteryzują się one następującymi cechami:

1. taktyka mieszana (Blended Tactics) – zagrożenia hybrydowe łączą konwencjonalne zdolności wojskowe z taktyką partyzancką małych jednostek, atakami asymetrycznymi i wysoce mobilnymi systemami walki dystansowej;
2. elastyczna i zdolna do adaptacji struktura –hybrydowe metody odziaływania są generowane na ogół za pomocą sił paramilitarnych, które mogą organizować się zarówno w zmasowane formacje konwencjonalne, jak i małe, rozproszone komórki;
3. terroryzm – zagrożenia hybrydowe wykorzystują kampanie propagandowe w celu siania terroru, nienawiści oraz wzbudzania strachu u przeciwników. Ataki te wymierzone są m.in. w istotne dla danego społeczeństwa symbole kulturowe, co ma doprowadzi do zniszczenia tożsamości i dziedzictwa kulturowego, które jest (lub może stać się) potencjalnym źródłem oporu względem ideologii agresora;
4. propaganda i wojna informacyjna – zagrożenia hybrydowe wykorzystują globalne sieci informacyjne do rozpowszechniania dżihadystycznych treści, pozyskiwania funduszy i rekrutacji;
5. aktywność kryminalna – schematy zakładające użycie zagrożeń hybrydowych wykorzystują przestępczość jako niezawodne źródło pozyskiwania

funduszy niezbędnych do prowadzenia walki, organizacji treningu rekrutacji, zarządzania i utrzymywania operacji;

6. instrumentalizacja prawa międzynarodowego – podmioty generujące zagrożenia hybrydowe lekceważą prawo międzynarodowe i postrzegają je, jako czynnik ograniczający ich przeciwników, który może zostać wykorzystany do dalszego osłabiania ich pozycji[481].

Potrzebę usprawnienia instrumentów przeciwdziałania zagrożeniom hybrydowym należy także rozpatrywać w kontekście ich możliwego wykorzystania, zarówno jako metody osłabiania państwa uważanego za konkurenta lub jako fazy wstępnej przygotowującej grunt pod pełnoekranowe działania zbrojne. Ten drugi scenariusz zaobserwowano w czasie inwazji Rosji na Ukrainę, co było poprzedzone wieloletnimi działaniami natury hybrydowej (np. oficjalne podważanie legalności władz w Kijowie, cyberataki), a potem także agresją na integralność terytorialną tego kraju.

Wnioski ze zrealizowanych badań wskazują, że w sytuacji wzrostu napięcia między państwami, jednym z zagrożeń może być fala zewnętrznych kampanii dezinformacyjnych wymierzonych w atakowany kraj. Zwiększona aktywność mająca na celu szerzenie dezinformacji wewnątrz danego kraju jest bardziej prawdopodobna jeśli cel ataku odgrywa strategiczną lub istotną rolę w danym konflikcie, a język tego kraju nie jest niszowy, ale używany przez znaczącą regionalnie, opiniotwórczą grupę ludności. Tego typu narracje dezinformacyjne, wymierzone m.in. w Polskę, były obserwowane w związku z inwazją Federacji Rosyjskiej na Ukrainę w 2022 r. W mediach pojawił się wówczas sprzyjający Rosji przekaz dla mieszkańców zachodniej Ukrainy, który bazował m.in. na twierdzeniach, iż Polacy chcą zająć Lwów, napaść na Białoruś oraz Naddniestrze. Z kolei w Polsce rozpowszechniano fałszywe informacje o pracodawcy, który rzekomo zwolnił 70 Polaków, by zatrudnić Ukraińców (za rządowe pieniądze). Ukraińcy byli przedstawiani jako przestępcy albo zwolennicy wrogiej Polsce ideologii banderyzmu, którzy w przyszłości

[481] S. Jasper, S. Moreland, *The Islamic State is a Hybrid Threat: Why Does That Matter?*, Small Wars Journal, 12.02.2014, https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter [dostęp: 12.04.2022].

rozpoczną walkę z Polakami. Federacja Rosyjska stosowała także działania sztucznie zmieniające proporcje prorosyjskiej populacji na spornych terenach.

W kontekście stosowania hybrydowej wojny informacyjnej, metody władzy na Kremlu dobrze ilustrują wystąpienia prezydenta Putina, w tym to z 30 września 2022 r. z okazji ceremonii przyjęcia nowych podmiotów w skład Federacji Rosyjskiej, co było sformalizowaniem aneksji okupowanych terytoriów (obwodów: ługańskiego, donieckiego, chersońskiego i zaporoskiego).

Wśród głównych elementów w narracji rosyjskiej pojawiają się m.in. następujące zarzuty wobec Zachodu, w tym te o stosowanie taktyk hybrydowych (dezinformacja):

- państwa zachodnie prowadzą przeciw Rosji wojnę hybrydową;
- celem wszystkich politycznych działań Zachodu jest podporządkowanie sobie współczesnego świata, żeby móc go grabić jak w czasach kolonialnych;
- główny cel USA i Zachodu: rozbić suwerenną, opartą na wartościach Rosję, żeby potem łatwo złamać opór wszystkich, niezgadzających się z dyktatem Zachodu;
- przywoływanie przykładu państw zachodnich, które w reakcji na kryzysy miały rzekomo rozpętywać wojny światowe;
- państwa zachodnie przyczyniły się do rozpadu ZSRR i uznały, że cały świat pogodzi się z ich dyktatem;
- lata 90-te omal nie doprowadziły do rozpadu Rosji, ale pokonano kryzys; jednak Zachód nie zaprzestał prób zniszczenia Rosji – trwają one do dziś;
- zerwano wszelkie porozumienia rozbrojeniowe, zwodzono Rosjan fałszywymi obietnicami nierozprzestrzeniania NATO na Wschód;
- przywołanie faktu, że Stany Zjednoczone są jedynym państwem na świecie, które dwukrotnie użyło broni jądrowej[482].

Jak wykazały wyniki badań, ataki, które można określić mianem hybrydowych, pod adresem Polski następowały nie tylko ze strony oficjalnych czynników politycznych, ale

[482] *Full text of Vladimir Putin's speech of September 30, 2022, transcript of the speech on the DPR, LPR, Zaporozhye and Kherson regions*, Eprimefeed.com, October 11, 2022, https://eprimefeed.com/latest-news/full-text-of-vladimir-putins-speech-of-september-30-2022-transcript-of-the-speech-on-the-dpr-lpr-zaporozhye-and-kherson-regions/192853/ [dostęp: 11.10.2022].

także ze strony najważniejszych osób ze służb specjalnych. Słowa szefa wywiadu Rosji Siergieja Naryszkina, że Polska i USA szykują wspólnie „polską aneksję zachodniej Ukrainy" zostały nad Wisłą odebrane jako przykład wrogiej operacji informacyjnej, a w mediach ukraińskich i zachodnich spowodowały szum informacyjny osłabiający pozytywny wizerunek Polski. Jako przykład wrogich wobec Polski działań o charakterze hybrydowym można uznać także artykuł byłego prezydenta Rosji D. Miedwiediewa, w którym pojawiły się m.in. zarzuty rzekomych planów przejęcia przez Polskę kontroli nad zachodnią Ukrainą oraz nieprawdziwe doniesienia dot. niewłaściwego traktowania uchodźców pochodzących spoza Ukrainy.

W toku badań stwierdzono, że w sferze cyberprzestrzeni występuje skomplikowany układ zależności, w którym możemy mieć do czynienia z atakiem lub wrogą działalnością pochodzącą zarówno w wyniku działalności realnej osoby, jak i zautomatyzowanego systemu (tzw. botów). Intencja wrogiej aktywności w świecie realnym oraz w cybersferze jest taka sama: dokonanie szkód. Te dwie sfery działania różni *modus operandi*: rodzaj zastosowanych narzędzi. W przypadku cyberprzestrzeni, narzędzia są cyfrowe, w odróżnieniu od obszaru fizycznej działalności. W obszarze cybernetycznym mamy ponadto do czynienia z większą swobodą działania aktorów pozapaństwowych (mogących realizować interesy konkretnych państw).

Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika z zastosowania metod charakterystycznych dla świata przestępczego i działalności terrorystycznej. Podczas wojny Rosji z Ukrainą w listopadzie 2022 r. pojawiły się tez przypadki wskazujące na używanie metod terrorystycznych. Chodzi o ładunek wybuchowy wysyłany pocztą do ukraińskiej ambasady w Madrycie, do hiszpańskiego premiera, a także do kilku innych lokacji w Hiszpanii (m.in. w bazie wojskowej w pobliżu stolicy kraju). W późniejszym czasie podobne przesyłki mające zastraszyć polityków przed kontynuowaniem wsparcia Ukrainie pojawiły się w szeregu krajach Europy, w tym w Polsce (zawierały m.in. oczy zwierząt). Istotny element działań hybrydowych stanowić też mogą porwania przedstawicieli władz lub nawet instytucji odpowiedzialnych za bezpieczeństwo danego kraju. W 2014 r. miał miejsce przypadek porwania estońskiego oficera Policji Bezpieczeństwa (KaPo), Estona Kohvera, co zbiegło się w czasie ze szczytem NATO i wizytą prezydenta USA w Tallinie. Porwany został

osadzony w rosyjskim areszcie i oskarżony o działalność szpiegowską[483]. Z kolei, strona estońska oznajmiła, iż Kohver został porwany z terytorium Estonii, kiedy znajdował się na granicy estońsko-rosyjskiej prowadząc działania związane ze zwalczaniem przestępczości transgranicznej. Ponadto, pomysłowość inicjatorów działań hybrydowych ilustruje przypadek ujawnienia przez Służbę Bezpieczeństwa Ukrainy zneutralizowania grupy przestępczej, która – w trakcie trwania wojny rosyjsko-ukraińskiej w 2022 r. – organizowała przemyt mężczyzn chcących uniknąć służby wojskowej. Co istotne, przemytnicy współpracowali z funkcjonariuszami służby granicznej Federacji Rosyjskiej, która była zainteresowana osłabieniem poboru żołnierzy do ukraińskiej armii. W zamian za 2,5 tys. do 8 tys. USD chętnym proponowano transport na Kaukaz Południowy lub do UE przez terytorium Federacji Rosyjskiej[484].

4.2. Podatność współczesnego państwa na nowe i prognozowane zagrożenia hybrydowe

W wyniku przeprowadzonych badań należy stwierdzić, że istnieje szara, nieuregulowana w prawie międzynarodowym strefa, w której mamy do czynienia z zagrożeniami hybrydowymi. Autokratyczne kraje usiłują doprowadzić do wprowadzenia zasad międzynarodowych opartych na zasadzie siły – wygrywa silniejszy. Kraje UE i NATO coraz częściej muszą się mierzyć z nowymi zagrożeniami poniżej progu wojny, które jednocześnie rodzą coraz poważniejsze konsekwencje. W związku z eskalacją wojny na Ukrainie i aktywnym zaangażowaniem we wsparcie dla władz w Kijowie (m.in. główny węzeł dostaw broni), istnieje wysokie ryzyko nasilonych ataków hybrydowych zwłaszcza na Polskę. Polska, jak wykazały wyniki badań, cały czas (niemal codziennie) była celem ataków ze strony Rosji, które nie są widoczne dla opinii publicznej. Chodzi m.in. o cyberataki na różne instytucje.

[483] Według rosyjskiej FSB, Estończyk został zatrzymany na terytorium Rosji z bronią (pistoletem Taurus), środkami w wysokości 5 tys. EUR w gotówce i sprzętem nagrywającym. Miał on realizować tajną operację estońskich służb specjalnych. Na podstawie tych oskarżeń sąd Federacji Rosyjskiej nakazał aresztowanie pod zarzutami szpiegostwa, nielegalnego przekroczenia granicy i nielegalnego posiadania broni. Kohver, jeden z najbardziej aktywnych oficerów Policji Bezpieczeństwa KaPo działających na kierunku rosyjskim, został uwolniony w wyniku wymiany więźniów między oboma krajami w 2015 r. i powrócił do Estonii.

[484] Organizacje terrorystyczne, co zauważają niektórzy badacze, są postrzegane jako „aktorzy hybrydowi", którzy są w stanie osiągnąć sukcesy o charakterze militarnym (przykład zdobyczy terytorialnych Państwa Islamskiego w Syrii i Iraku). Co więcej, aktywna obecność środowisk terrorystycznych w mediach społecznościowych również stanowi ważny element zagrożeń hybrydowych (propaganda, dezinformacja). Zob. więcej: A. Olech, op. cit.

Przypadek cyberataku na europejskich polityków w 2021 r. (m.in. w Polsce) był związany nie tylko z wykradzeniem poufnych informacji z ich prywatnych kont pocztowych, ale także zmanipulowaniu ich oraz dalszemu rozpowszechnianiu. Zamiarem było pogorszenie relacji tych krajów z NATO. Rozszerzeniem tych działań mogą być ataki na infrastrukturę krytyczną, zarówno na poziomie UE jak i NATO, co powinno przyspieszyć działania na rzecz wzmocnienia polityki bezpieczeństwa krajów Sojuszu.

Podatność współczesnego państwa na nowe i prognozowane zagrożenia hybrydowe wynika z ich szerokiego zakresu. Destabilizujące sytuację międzynarodową zjawiska, na przykład masowe migracje (także te sztucznie wytwarzane, jak w przypadku granicy polsko-białoruskiej w 2021 r.), konflikty zbrojne, czy zmiany klimatu, tworzą warunki sprzyjające proliferacji zagrożeń hybrydowych. Ten trend będzie się pogłębiał wraz z cyfryzacją kolejnych dziedzin życia społecznego. Dalsze zmiany technologiczne (usługi elektroniczne w administracji państwowej, sztuczna inteligencja, komputery kwantowe, eksploracja kosmosu, autonomiczne pojazdy)[485] niosą ryzyko pojawienia się nowych podatności w obszarze hybrydowym. Uszkodzenie gazociągów Nord Stream 1 i 2 w 2022 r. uświadomiło znaczenie ochrony infrastruktury krytycznej w kontekście działań hybrydowych. Tego typu uderzenia w rurociągi, tamy, kable telekomunikacyjne czy systemy wodociągów zaliczyć można do prognozowanych zagrożeń związanych z użyciem środków hybrydowych. Poważnym wyzwaniem może być zmaterializowanie się zagrożenia atakiem lub wywołaniem incydentu z użyciem substancji radioaktywnych (tzw. „brudna bomba"). Ponadto, w kontekście zagrożeń hybrydowych trzeba liczyć się z ewentualnością rozpoczęcia kilku konfliktów o konwencjonalnym i/lub niekonwencjonalnym charakterze jednocześnie. W kontekście rosyjskiej inwazji na Ukrainę w 2022 r., rosnące napięcia w separatystycznym Naddniestrzu mogą oznaczać, że kolejnym celem Federacji Rosyjskiej będzie Mołdawia[486]. Ponadto, kolejnym teatrem działań hybrydowych może być obszar

[485] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

[486] Wymiana ognia, którą obserwowano na wiosnę 2022 r. na granicy między separatystycznym regionem Mołdawii – Naddniestrzem a Ukrainą jest różnie interpretowana. Niektórzy widzą w niej próbę Rosji do rozszerzenia konfliktu z Ukrainą na kolejne obszary. Prorosyjscy separatyści naddniestrzańscy informowali z kolei, że to Ukraińcy przeprowadzają „ataki terrorystyczne" na terytorium ich samozwańczej republiki. Mają one polegać na ostrzale przygranicznych terenów (w tym – budynków służb wywiadowczych oraz wysyłaniu uzbrojonych dronów).

wokół Tajwanu, co – z uwagi na zaangażowanie USA w regionie – wpłynęłoby na osłabienie wsparcia Waszyngtonu dla Europy Środkowej w kontekście konfliktu na Ukrainie[487].

Jak pokazały badania, próbę wskazania prognozowanych zagrożeń, wynikających z działań hybrydowych Federacji Rosyjskiej wobec Ukrainy w wymiarze krajowym, regionalnym i ponadregionalnym, podjęła Agnieszka Rogozińska, w ocenie której: „Ukraina nie stanowi ostatecznego celu dla Putina, na co wskazują działania podejmowane przez Federację Rosyjską chociażby na terenie Państw Bałtyckich (…) Dla Rosji podbój Ukrainy jest krokiem do przebudowy porządku światowego i realizacji własnych interesów, potrzebną przesłanką dla dalszej ofensywy na Europę, przykładem dla zastraszenia niepokornych, a nie celem samym w sobie. Kijów walczy przede wszystkim i przeważnie o swoją przyszłość, ale, wygrawszy tę kampanię i otrzymawszy do rozporządzenia zasoby Ukrainy, Rosja stanie się o wiele pewniejsza siebie i bardziej agresywna. (…) Niepowstrzymanie na obecnym etapie agresywnych działań rosyjskich w krajach Europy Środkowo-Wschodniej skutkować będzie rosnącym zagrożeniem destabilizacji całego regionu. (…) Jedynym wydolnym narzędziem w zaistniałej sytuacji jest wzajemna pomoc i wspólna reakcja państw demokracji Zachodu i UE generująca znaczne straty finansowe i polityczne po stronie agresora. Działania z obszaru wojny hybrydowej powinny z założenia skutkować nie tylko stratami państwa atakującego, ale i jego izolacją na arenie międzynarodowej. Warunkiem realizacji tych postulatów jest jednomyślność i właściwa ocena skali zagrożeń. Ta ostatnia wskazuje, że Ukraina może stanowić tylko kolejną pozycję na liście odbudowy rosyjskiej strefy wpływów. Następna może być Litwa, Łotwa, Estonia. I Polska[488]". Te spostrzeżenia nie straciły wiele ze swojej aktualności kontekście rosyjskiej operacji wojskowej na Ukrainie w 2022 r. z wyjątkiem ukazania nowego aspektu tego

[487] Przebieg rosyjskiej inwazji na Ukrainę w 2022 r. jest obserwowany przez Chiny i wpływa na kalkulacje tego kraju co do ewentualnego ataku na Tajwan. Nie osłabi to determinacji Pekinu do przejęcia pełnej kontroli nad – uważanym za zbuntowaną prowincję – Tajwanem, ale może wpłynąć na analizy strony chińskiej, co do tego, jak i kiedy to osiągnąć. W interesie ChRL leży dalsze rozbudowywanie potencjału militarnego, także w zakresie broni hybrydowych i niekonwencjonalnych. Przedwczesny wybuch konfliktu zbrojnego z USA i/lub krajami zachodnimi nie jest korzystny dla Pekinu. Z kolei, z punktu widzenia Waszyngtonu, powstrzymanie wrogo nastawionych do Zachodu Chin może być realne tylko teraz lub w nadchodzących latach – zanim uzyskają one przewagę militarną nad USA / NATO (same lub w koalicji z Rosją oraz ewentualnie innymi podobnie myślącymi krajami).

[488] A. Rogozińska, *Niemilitarne zagrożenia dla Ukrainy w kontekście działań hybrydowych prowadzonych przez Federację Rosyjską*, INE 24 listopada, 2019, http://ine.org.pl/wp-content/uploads/2020/02/INE.niemilitarnezagrozeniadlaukrainywkontekscie dzialanhybrydowych.pdf [dostęp: 11.06.2022].

konfliktu polegającego na tym, iż zagrożenia hybrydowe mogą stanowić nie tylko formę jedynego ataku, ale być przygotowaniem gruntu pod operację z pełnowymiarowym użyciem konwencjonalnych sil zbrojnych.

W wyniku przeprowadzonych badań stwierdzono, że specyfika zagrożeń hybrydowych, których cechą jest działanie poniżej progu wojny, umożliwia ich sprawcom wybór bardzo szerokiego zakresu i narzędzi ataku. Nowe zagrożenia hybrydowe mogą ewoluować z już istniejących przykładów tego typu działalności, lub też stanowić nową, niespotykaną wcześniej kategorię. Wśród aktualnych trendów zagrożeń hybrydowych można zaliczyć m.in.:

a) masowe włamania do systemów informatycznych zachodnich rządów i parlamentów, co jest dokonywane w celu zwiększenia presji psychologicznej;

b) zwiększenie stanu obcego posiadania zachodniej infrastruktury krytycznej;

c) mnożenie aktorów niepaństwowych wykorzystywanych jako podmioty pośredniczące (prywatne firmy wojskowe, wspólnoty religijne itp.);

d) rosnące wykorzystanie instrumentalizacji prawa (ang. *lawfare*);

e) prawo narzędziem wpływu na kształtowanie innych domen istotnych z punktu widzenia zagrożeń hybrydowych;

f) instrumentalizacja migracji[489].

Do przykładów zagrożeń hybrydowych, które dobrze oddają ich wielowymiarowość i złożony charakter, można zaliczyć szeroką kategorię procesów, wydarzeń i incydentów związanych z pośrednim odziaływaniem wrogich aktorów na bezpieczeństwo narodowe współczesnych państw. Jednym z nich był lot Ryanair 4978 z Aten do Wilna, który został przechwycony przez służby białoruskie pragnące zatrzymać podróżującego nim opozycyjnego wobec rządu aktywistę. Prognozowane zagrożenia związane z użyciem środków hybrydowych, jak wynika z przeprowadzonych badań, mogą bazować na niekonwencjonalnych rozwiązaniach stosowanych w konfliktach (jak np. użycie określonego

[489] *Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO…*

uzbrojenia do niszczenia innych celów niż to przewidzieli jego konstruktorzy, co utrudnia obronę) lub wykorzystanie nowatorskich metod ataku (np. niszczenie infrastruktury za pomocą impulsu elektromagnetycznego, nowy rodzaj biologicznej broni masowego rażenia, która nie powoduje długotrwałego skażenia i/lub działa tylko na określonym terenie lub względem ściśle ograniczonej grupy etnicznej lub narodowej).

Wyniki przeprowadzonych badań wskazują, że potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym w Polsce i innych krajach wynika także ze wzrostu aktywności w tym zakresie ze strony Federacji Rosyjskiej, zwłaszcza od czasu objęcia tam rządów przez kręgi władzy zbliżone do W. Putina. Przypadki działania służb specjalnych likwidujących przeciwników za pomocą trucizny zaliczają się do zagrożeń hybrydowych, jako przykład skrytego zastosowania broni chemicznej. Atak na byłego rosyjskiego szpiega Siergieja Skripala w Salisbury w południowej Anglii w 2018 r. pokazuje, że jako ataków hybrydowych można wykorzystać broń chemiczną (podaną skrycie truciznę). Przykład zatrucia w angielskim Salisbury, o które oskarżono Rosję, pokazał wrażliwość Wielkiej Brytanii na tego typu ataki na jej terytorium. Zainicjowało to prace nad poprawą zabezpieczenia przed tego typu zagrożeniami hybrydowymi, ale także zintensyfikowało proces intensywnego zwalczania wrogich narracji w przestrzeni publicznej[490]. Skripal, były pułkownik rosyjskiego wywiadu wojskowego GRU, został wcześniej skazany w Rosji za szpiegostwo na rzecz Wielkiej Brytanii. On oraz towarzysząca mu córka trafili do szpitala w stanie krytycznym, ale przeżyli – po kilku tygodniach opuścili szpital. O próbę zabicia Skripalów władze brytyjskie oskarżyły Rosję, co doprowadziło do kryzysu dyplomatycznego w relacjach między Londynem i Moskwą (wydalenie grupy rosyjskich dyplomatów z Wielkiej Brytanii oraz z ponad 20 innych państw). Strona rosyjska odrzuciła te oskarżenia utrzymując, że była to prowokacja służb brytyjskich. Zamach w Wielkiej Brytanii był pierwszym znanym publicznie przypadkiem wykorzystania bojowego środka chemicznego na terytorium państw NATO. Do ataku użyto substancji z grupy bojowych środków trujących o działaniu paralityczno-drgawkowym (tzw. „nowiczoka), które – według informacji źródeł zachodnich – miały zostać wynalezione w ZSRR. Był to przykład jak Rosja używała

[490] Prezentacja o przeciwdziałaniu dezinformacji w Wielkiej Brytanii w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), *MSZ, 21 kwietnia 2022*.

instrumentów hybrydowych, aby zastraszyć nieprzychylne jej władze Wielkiej Brytanii[491]. Przypadek otrucia rosyjskiego dysydenta Skripala w Wielkiej Brytanii, który był przykładem hybrydowych działań poniżej progu wojny i skłonił władze w Londynie do szukania wsparcia wśród sojuszników.

Rosja, jak wykazały wyniki badań, buduje w innych krajach sieci powiązań (często korupcyjnych), które mogą zostać wykorzystane na rzecz prowadzenia aktywności hybrydowej w tych krajach. Sieci te – bez zaangażowania specjalnych narzędzi analityki wywiadowczej – są niewidoczne dla obserwatorów zewnętrznych. Używanie metod wciągania przedstawicieli władz, biznesu oraz organizacji pozarządowych, oraz osób indywidualnych w nieprzejrzystą, a często nawet przestępczą sferę działania ułatwia zadanie agresorowi. Kontakty, zasoby oraz terytorium danego kraju objętego taką działalnością, może zostać wykorzystane także do ataku hybrydowego na kraj trzeci. O podobne techniki są podejrzewane Chiny. Im bardziej skorumpowany jest dany kraj i jego społeczeństwo, tym łatwiej jest działać aktorowi hybrydowemu. Z kolei, w Finlandii w 2014 r. zidentyfikowano potencjalne zagrożenie hybrydowe w postaci wykupowania przez rosyjską firmę nieruchomości zlokalizowanych w strategicznych miejscach kraju, co zagrażało bezpieczeństwu narodowemu. Uznano, że tereny te mogły zostać wykorzystane do działań hybrydowych na terytorium fińskim w przypadku konfliktu zbrojnego.

Jednocześnie państwo atakujące usiłuje uzyskać wpływ lub kontrolkę na infrastrukturę krytyczną danego kraju, w tym zwłaszcza kolej i węzły komunikacyjne (lotniska, porty), media, sektor naftowo-gazowy i energii. Agresor może w ten sposób manipulować sytuacją np. poprzez ceny energii. Dobrym przykładem służy tu Rosja, która utrzymuje obecność we wszystkich 6 krajach Eurazjatyckiej Wspólnoty Gospodarczej. UE nie posiadała swoich przedstawicieli w tych państwach, ale podejście to ulega zmianie. Rosja wykorzystuje także organizacje regionalne, jako narzędzie nacisku. Ponadto, działa w regionie, jako siła destabilizująca, tylko po to, aby potem wystąpić, jako siła stabilizująca, co generuje dla niej zamierzone korzyści. Dla przykładu, w konflikcie zbrojnym na Kaukazie, Rosja dostarczała broń obu walczącym stornom – Armenii, ale także Azerbejdżanowi. Jak wykazały wyniki badań, zagrożenia hybrydowe są jednak generowane nie tylko przez Rosję. Chińskie inwestycje skupiają się na najważniejszych sektorach w krajach i regionach znajdujących się w orbicie zainteresowania Pekinu (m.in.

[491] *Countering Hybrid Threats and enhancing resilience,* The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

w Europie). Należą do nich m.in. sektor motoryzacyjny, lotniczy, rolno-spożywczy, finansowy i usług dla biznesu, zdrowia i biotechnologii, produktów i usług konsumenckich. Nowe zagrożenia hybrydowe, jak pokazuje przykład wojny na Ukrainie w 2022 r., mogą być powiązane ponadto z bezpieczeństwem energetycznym. Atak rosyjskich dronów na instalacje przesyłu energii elektrycznej spowodował znaczące utrudnienia w dostawach prądu. Dodatkowym czynnikiem był w tym przypadku okres jesienno-zimowy, kiedy nastąpiło to uderzenie skłaniając do ucieczki z kraju kolejne fale ludności cywilnej oraz zwiększając presję na ukraińskich decydentów.

Stosując metody hybrydowe w postaci dezinformacji, Rosja umiejętnie wykorzystywała wszelkie fakty i wydarzenia, aby wprowadzić insynuacje co do rzeczywistych zamiarów USA i ich zachodnich sojuszników w Europie, a zwłaszcza w krajach aspirujących do integracji ze strukturami zachodnimi. Sformułowane w 2017 r. rosyjskie zarzuty, że Lugar Center i inne laboratoria biologiczne na Kaukazie iw Azji Środkowej wytwarzają zakazaną broń biologiczną, są w ocenie wielu zachodnich ekspertów bezpodstawne. W serii oświadczeń, jak przypomniała Filippa Lentzos, reprezentująca brytyjski King's College London, Rosja zasugerowała, że „Pentagon tworzy na granicach swojej strefy wpływów sieć laboratoriów broni biologicznej. W centrum oskarżeń znalazło się Centrum Badań Zdrowia Publicznego im. Richarda Lugara w Republice Gruzji. Nazwany na cześć amerykańskiego senatora Richarda Lugara, który zainicjował renowację sieci laboratoriów w krajach byłego Związku Radzieckiego, Lugar Center rozpoczęło działalność w 2013 r. Stanowiło ono pierwsze laboratorium biologiczne w regionie o wysokim stopniu ochrony (poziom 3), co oznacza, że jest zdolne do badań poważnych i/lub śmiertelnych chorób służąc Gruzji i całemu regionowi, oferując możliwości wykrywania i diagnozowania ognisk infekcji[492].”

W wyniku przeprowadzonych badań stwierdzono, że cybertechnologie pozwalają atakującej stronie na wykorzystanie wielu nowych narzędzi, które nie są uregulowane prawnie. To tworzy szarą sferę sprzyjającą generowaniu zagrożeń hybrydowych. Wyzwania w zakresie cyberprzestepczości także są wymiarem przeciwdziałania zagrożeniom hybrydowym. Większość wycieków wrażliwych informacji, które można zakwalifikować do

[492] F. Lentzos *The Russian disinformation attack that poses a biological danger, the Bulletin of the Atomic Scientists,* November 19, 2018, https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/ [29.11.2022].

zagrożeń hybrydowych, pochodzi w wyniku działania przestępców w sferze elektronicznej (przypadki włamań do skrzynek emailowych). Ale zagrożenia hybrydowenie są równoznaczne z zagrożeniami cybernetycznymi, które mogą występować w wyniku działania przestępczości nie powiązanej z celami poza-kryminalnymi. Nie wszystkie ataki cybernetyczne są więc związane z hybrydowymi działalnymi[493]. Cyberbezpieczeństwo jest z natury nacechowane wysokim stopniem fragmentacji. Wraz z upowszechnieniem się trendu do podłączania coraz większej ilości urządzeń i sprzętów do sieci Internet, wzrastają także zagrożenia hybrydowe w sferze cyfrowej. Obecnie społeczeństwa funkcjonują w świecie połączonym siecią zależności. Cyberbezpieczeństwo odnosi się do szeregu domen, m.in.: komunikacyjnej, wojskowej, informacyjnej, fizycznej, pozarządowej i prywatnej (przedsiębiorcy) oraz publicznej. Domena cyber ma wpływ na przestrzeń fizyczną. Internet, który jest siecią połączeń cyfrowych, ma związek z funkcjonowaniem fizycznej infrastruktury (w tym – krytycznej takiej jak elektrownie), urządzeń i przemysłu[494].

W ostatnich latach domena cyber stała się jednym z priorytetów w dyskusji dotyczącej spraw bezpieczeństwa w wielu krajach. Przeciwdziałanie zagrożeniom hybrydowym również dotyczy tej ważnej sfery. W Europie, do jednych ze znaczących cyberataków można zaliczyć uderzenie na infrastrukturę Estonii w 2007 r. Cyberataki na Estonie w 2007 r. stanowiły nowy wymiar zagrożenia z uwagi na uderzenie w zasoby i sieci teleinformatyczne (IT), których funkcjonowanie jest istotne z punktu widzenia bezpieczeństwa kraju oraz jego obywateli. Technologie cyfrowe wykorzystane są obecnie na poziomie krajowym i międzynarodowym w szeregu domenach istotnych nie tylko dla obronności, ale także gospodarki, komunikacji ze społeczeństwem i innych wymiarach działalność współczesnego państwa. Technologie cyfrowe nie tylko ułatwiają szerzenie dezinformacji, ale także umożliwiają odcięcie społeczeństw przez autorytarne władze od rzetelnych informacji. Państwa autorytarne próbują ograniczać swobodę dostępu do Internetu cenzurując niewygodne dla siebie źródła informacji. Obok blokowania niewygodnych stron czy serwisów informacyjnych istnieją także inne narzędzia pośredniego działania. Niektóre kraje (np. Chiny) zwiększają czas ładowania się stron, które rząd uważa za zagrożenie (np. rzetelne informacje z niezależnych źródeł). W krajach

[493] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

[494] *Cybersecurity & Cyber Diplomacy*, European Security Defence College, seminarium online na zasadach Chatham House, 2022.

autorytarnych jak Korea Północna tylko niewielka cześć społeczeństwa ma pełny dostęp do stron międzynarodowych[495]. Postępujący wciąż rozwój technologiczny dostarczy zapewne także nowych narządzi do działań hybrydowych, ale zapewni też skuteczniejsze zdolności obronne (m.in. technologia blockchain, sztuczna inteligencja)[496]. Jednocześnie, innowacyjne technologie mogą wiązać się ze zwiększonym ryzykiem ich wykorzystania, także w kontekście zagrożeń hybrydowych. Chmura obliczeniowa (ang. cloud computing) to nowoczesna technologia do zarządzania danymi, która opiera się na współdzielonym oprogramowaniu i infrastrukturze teleinformatycznej. Miała być ona odpowiedzią na wyzwania bezpieczeństwa, jednak przypadki nieuprawnionego naruszenia tego systemu ukazały ryzyko szerszego nieuprawnionego dostępu do informacji niż miało to miejsce w przypadku starszego typu systemów. Informacje o incydentach związanych z chmurami obliczeniowymi były sygnałem ostrzegawczym w tym zakresie. Instytucje państwowe, zwłaszcza te odpowiedzialne za kwestie bezpieczeństwa, nie powinny korzystać z tego typu technologii, nawet jeśli miałoby to oznaczać wyższe koszty funkcjonowania.

W wyniku przeprowadzonych badań stwierdzono, że użycie migracji jako narzędzia hybrydowego ma na celu m.in. wytworzenie braku zaufania między państwami danej wspólnoty (np. UE) oraz przetestowanie wytrzymałości ich systemów zabezpieczeń. Może to być korzystne dla agresora w przypadku podjęcia przez niego działań eskalacyjnych, które mogą osiągnąć nawet fazę otwartego konfliktu zbrojnego[497]. Kryzys migracyjny na granicy polsko-białoruskiej także dobrze oddaje tu charakter tego typu zagrożeń. Na poziomie unijnych struktur współpracy – w ramach których funkcjonuje Polska[498] – zagrożenia hybrydowe rzucają wyzwanie sile regionalnej i globalnej pozycji UE, generują brak zaufania między państwami członkowskimi (m.in. ograniczenia dostaw energii, dezinformacja), a także testują spójność unijnych struktur, jak miało to miejsce w przypadku kryzysu

[495] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

[496] Technologia blockchain miała pierwotnie zastąpić tradycyjnie rozumiany system bankowy. Technologia kwantowa daje możliwość transferu i operowania znacznie większą ilością danych niż umożliwia to system zero jedynkowy. Wyzwaniem jest obecnie stabilność działania tych systemów w warunkach poza-laboratoryjnych. Z kolei, Rozwój AI i jej wdrożenie, jak wykazały wyniki badań, może zająć od 4 do 10 lat, a więc może nastąpić między 2026 – 2032 r.

[497] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

[498] Kluczowe zadania przeciwdziałania zagrożeniom hybrydowym znajdują się w rękach kompetencji PCZ, ale instytucje jak UE mogą wspomóc te działania.

migracyjnego na granicy polsko-białoruskiej. W przypadku fiaska, działania te są podejmowane przed adwersarzy ponownie (ewentualnie, w zmienionej formie). Natomiast, w wymiarze zewnętrznym zagrożenia hybrydowe osłabiają światowy porządek i zaburzają funkcjonowanie wielu struktur państwowych. Chodzi tu m.in. o starania Rosji zmierzające do kontroli politycznej i gospodarczej określonych krajów za pomocą działań najemników w Afryce oraz walkę o dostęp do zasobów surowcowych[499].

Stosowanie środków nacisku gospodarczego także może być rozpatrywane jak o jedno z zagrożeń hybrydowych (ang. *economic coercion*), które nasili się w przyszłości. Kraje, które są uzależnione od jednego dostawcy danej technologii czy towaru są na to najbardziej narażone. Przykładem są tu wrogie działania natury ekonomicznej Chin wobec Litwy, które nastąpiły po zaprzestaniu przez ten kraj kooperacji z Pekinem w formacie 17+1. W sferze gospodarczej, do zagrożeń hybrydowych należy celowe uzyskiwanie przez agresora wpływu na projekty o strategicznym znaczeniu w danym kraju (m.in. przez bezpośrednie inwestycje zagraniczne). Ponadto, do działań hybrydowych można zaliczać dokonywanie w danym kraju inwestycji niedochodowych, które są dźwignią wpływu na aparat rządzący kraju stanowiącego cel ataku (np. przez zadłużenie). Wreszcie, uzupełnieniem arsenału hybrydowego jest walka informacyjna, która ma za zadanie wytworzyć sfabrykowany, fałszywy obraz kraju uznanego za przeciwnika, co może być realizowane także z użyciem dyplomatycznych kanałów, propagandy w mediach. Często wykorzystuje się tu także odniesienia do historii, co można określić jako walkę z użyciem polityki historycznej.

Wykorzystanie podmiotów pozapaństwowych jest wzrastającym wyzwaniem w zakresie przeciwdziałania zagrożeniom hybrydowym. Naciski mogą być także realizowane przez organizacje międzynarodowe[500], szpiegostwo (w tym – przemysłowe), cyberataki, W wielu z tych domen agresor może wykorzystać działalność grup przestępczych (pośrednio lub bezpośrednio inspirowanych przez służby specjalne). Odnotować także

[499] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

[500] Organizacje międzynarodowe (globalne i regionalne), w oczach dominującego obecnie realizmu politycznego, posiadają jedynie ograniczone funkcje, które przekazują im państwa. Realiści widzą w organizacjach międzynarodowych instytucje międzypaństwowe, które służą realizacji partykularnych interesów poszczególnych krajów (silniejsze z nich uzyskują dominujące wpływy w danej organizacji). L. Fawcet, A. Hurrell, *Regionalism in World Politics*, Oxford University Press 2002, s. 12-13.

należy działalność coraz to nowych agentów wpływu, także w wirtualnej przestrzeni informacyjnej. Istotnym może być także finansowanie i zapewnienie przez stronę atakującą wsparcia innego typu dla osób oraz organizacji dezintegrujących tkankę społeczną w kraju obranym za atak. Intencją w tym przypadku może być wywołanie chaosu i zmniejszenie zdolności obronnych. Misja UE w Mali napotkała na poważne problemy, które wynikały w dużej mierze z hybrydowego zaangażowania strony rosyjskiej w tym kraju. Działalność Grupy Wagnera, prywatnej firmy wojskowej powiązanej z Kremlem, była jednym z głównych wyzwań przed UE. W 2022 r. rosyjscy najemnicy w Afryce nadal byli wiązani z masakrami, w których ginęli cywile. W Mali w incydentach, w których udział brała Grupa Wagnera – rosyjska prywatna firma wojskowa – zginęło prawie 500 malijskich cywilów, jak donosiły media brytyjskie. Ponadto, Grupa Wagnera miała duży wpływ na sytuację polityczną w Republice Środkowo-Afrykańskiej pozostając blisko kluczowych polityków.

Potrzeba usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym wynika także z nowego rodzaju broni, które mogą być użyte przez agresora. Działania hybrydowe mogą być prowadzone za pomocą nowoczesnych środków walki w postaci powietrznych, lądowych lub morskich dronów. Ich atrybucja jest utrudniona jak pokazuje sytuacja w czasie inwazji Rosji na Ukrainie w 2022 r., kiedy dokonano ataku na Kijów i inne miasta z użyciem właśnie tego środka. Przez długi czas zachodni eksperci nie mogli ustalić kraju pochodzenia dronów, co uniemożliwiało nałożenie sankcji albo zastosowanie innych środków odwetowych. Ostatecznie udało się poczynić pewne ustalenia. Rosja, jak poinformowała strona ukraińska, zamówiła prawie 2,5 tys. dronów kamikaze Shahed-136 od Iranu. Niebezpieczeństwo tej nowej broni zwiększał fakt, że ta amunicja krążąca była w stanie atakować cel za pomocą licznych pojedynczych ładunków formując tzw. rój. Stwarzało to poważne wyzwanie dla obrony przeciwlotniczej.

W wyniku przeprowadzonych badań stwierdzono, że do zagrożeń hybrydowych wielu ekspertów zaliczało w przeszłości dezinformację w sferze szczepień związanych z pandemią COVID[501]. Ponadto, pandemia koronawirusa wiązała się z transformacją cyfrową wielu obszarów życia zawodowego i prywatnego. Spowodowało to nasilenie incydentów i problemów dotyczących cyberbezpieczeństwa. Do nowych, potencjalnych zagrożeń zaliczyć

[501] *Countering Hybrid Threats and enhancing resilience*, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

m.in. stosowanie skryte broni biologicznej w postaci wywoływania epidemii wśród ludzi i/lub zwierząt mających znaczenie gospodarcze dla atakowanego państwa.

4.3. Wnioski

Jak wskazują wyniki przeprowadzonych badań, do czynników decydujących o potrzebie usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym zaliczyć można złożony charakter tego rodzaju zagrożeń, ich destrukcyjny wpływ na atakowane państwo oraz trudne do wykrycia oraz neutralizacji odziaływanie poniżej progu wojny. Stosowanie przez agresorów wyrafinowanych, wielopłaszczyznowych metod ataków hybrydowych stwarza wyzwania nowego typu dla instytucji, służb i formacji zajmujących się bezpieczeństwem narodowym. Specyfika zagrożeń hybrydowych, a także ich ewoluujący charakter powodują, że współczesnemu państwu trudno jest przygotować się na skuteczną obronę.

Dla Polski i innych krajów Europy Środkowej i Wschodniej (byłego bloku ZSRR) najpoważniejsze zagrożenie hybrydowe jest związane z działaniami Federacji Rosyjskiej, która usiłuje odbudować swoją dawną strefę wpływów. Polska, jako kraj frontowy NATO, który wielokrotnie w przeszłości padał ofiarą ataków hybrydowych, powinna wzmocnić zarówno krajowy potencjał odstraszania, jak i usprawnić mechanizmy sojuszniczego wsparcia w sytuacjach kryzysowych. Przemawia za tym m.in. stały niepokojący czynnik w postaci wzrostu wydatków zbrojeniowych Rosji, która jest uznawana za największego hybrydowego agresora Europy Środkowej i Wschodniej .„Władze na Kremlu zwiększyły wydatki obronne aż o 2,9% w 2021 r. do 65,9 mld USD (86% wszystkich wydatków wojskowych w Europie Wschodniej)[502]. Całkowite wydatki obronne w Europie w 2021 r. wyniosły 418 mld USD, o 3% więcej niż w 2020 r., przy czym wydatki w Europie Zachodniej wyniosły 305 mld USD i rosły w szybszym tempie (3,4%) niż w Europie Środkowej[503] (1,3%), która przeznaczyła na obronność 36,6 mld USD. Wzrost był napędzany głównie zwiększonymi wydatkami na zaopatrzenie w broń oraz badania i rozwój na potrzeby wojska.

[502] Definicja Europy Wschodniej wg SIPRI dotyczy: Abchazji, Armenii, Azerbejdżanu, Białorusi, Gruzji, Mołdawii, Rosji i Ukrainy.

[503] Definicja regionu Europy Środkowej w bazach danych SIPRI dotyczących wydatków obronnych obejmuje: Albanię, Bośnię i Hercegowinę, Bułgarię, Chorwację, Czechy, Estonię, Węgry, Kosowo, Łotwę, Litwę, Macedonię Północną, Czarnogórę, Polskę, Rumunię, Serbię, Słowację i Słowenię.

Europa Wschodnia odnotowała w 2021 r. wzrost wydatków obronnych o 2,3%, do poziomu 76,3 mld USD. W latach 2012-2022 tempo wzrostu było znaczące i wyniosło aż 15%. Głównym czynnikiem było zwiększenie rosyjskich wydatków na zbrojenia (rosyjski budżet stanowił aż 86% wydatków całego regionu).

Jak pokazują wyniki badań, w przypadku Polski, dodatkowym czynnikiem przemawiającym za usprawnieniem sposobów przeciwdziałania zagrożeniom hybrydowym jest różnica potencjałów militarnych, doświadczenia oraz pozycji międzynarodowej, która występuje między Polską i krajem uznawanym przez jej obecne władze za największe zagrożenie (Rosja). Zdolności oddziaływania hybrydowego władz w Moskwie, także za pośrednictwem Białorusi, prezentują poważne zagrożenie dla państwa polskiego. Stosowanie taktyki hybrydowej omija zabezpieczenia posiadane przez Polskę w postaci sojuszu obronnego, jakim jest NATO. Mimo, że NATO może interweniować w sytuacji zagrożenia swoich członków zagrożeniami niekonwencjonalnymi tego typu, w praktyce jest to bardzo trudne. To wyzwanie, jak pokazały badania, ujawniło się w 2021 r. podczas ataku hybrydowego na Polskę od strony białoruskiej granicy z wykorzystaniem sztucznych tłumów afrykańskich i bliskowschodnich migrantów. Przykład ten pokazuje, że zdolności odstraszania państwa polskiego, które zidentyfikowano jako główny mechanizm przeciwdziałania zagrożeniom hybrydowym, nie są wystarczająco skuteczne.

Metody przeciwdziałania zagrożeniom hybrydowym są uzależnione od taktyki stosowanej przez przeciwnika oraz od zdolności danego kraju lub ich sojuszu do skutecznej odpowiedzi. Ich zakres oraz nasilenie dobiera się obecnie stosując eskalację środków odpowiedzi oraz uwzględniając potrzebę elastyczności. Przykład ataku na byłego oficera rosyjskich służb specjalnych w brytyjskim Salisbury pokazuje znaczenie wzmocnienia potencjału obronnego wywiadu i kontrwywiadu, a także ich zdolności ofensywnych (odstraszanie przez groźbę kontrataku na terytorium wroga). W celu zmniejszenia ryzyka stania się ofiarą ataków hybrydowych w sferze gospodarczej, państwa podejmują działania zmierzające do wzmocnienia swoich systemów ekonomicznych oraz zróżnicowania partnerów gospodarczych w zakresie importu oraz eksportu towarów. Ważnym wymiarem przeciwdziałania zagrożeniom hybrydowym w obszarze gospodarczym jest energia. Do aktualnych sposobów przeciwdziałania zagrożeniom hybrydowym w obszarze bezpieczeństwa energetycznego należą wysiłki na rzecz dywersyfikacji źródeł produkcji

i/lub przesyłu dostaw nośników energii takich jak gaz, ropa czy energia elektryczna. Z kolei, ryzyko związane z naciskami wywieranymi na dany kraj za pośrednictwem organizacji międzynarodowych wymaga z kolei od państwa atakowanego wzmocnionych zdolności sojuszniczych oraz sieci sprawdzonych, lojalnych partnerów zagranicznych. W oparciu o relacje z nimi, państwo broniące się może niwelować uszczerbek na wizerunku w wyniku ewentualnej hybrydowej presji na forach organizacji międzynarodowych (na przykład pomawianie, szkalowanie danego państwa na w danej organizacji lub nawet próby jego wykluczenia).

W wyniku przeprowadzonych badań stwierdzono, że rozbudowa arsenału nowoczesnych środków obronnych, w którą inwestują współczesne państwa, jest z kolei niezbędna w celu przeciwdziałania atakom hybrydowym, także pasywnym – rozpoznanie, szpiegostwo) za pomocą dronów. Obecnie większość zdalnie kierowanych pojazdów tego typu (lądowych, morskich i powietrznych) wymaga przynajmniej po części sterowania przy udziale człowieka. Jednak, wraz z upowszechnieniem się systemów sztucznej inteligencji i aplikowania ich do modułów kierowania pojazdami bezzałogowymi, wyzwanie to będzie dodatkowo nasilać się. Analogiczna sytuacja, wymagająca stałego unowocześniania wyposażenia technicznego odnosi się do sfery cybernetycznej i konieczności przeciwdziałania atakom hackerskim. Co ważne, mogą one być wymierzone nie tylko w sieci teleinformatyczne (dezinformacja, kradzież danych, kompromitacja polityków, paraliż infostrad i kanałów komunikacji), ale także w systemy sterowania obiektów kwalifikujących się do infrastruktury krytycznej takich jak elektrownie czy lotniska.

Ponadto, jak pokazały wyniki badań, możliwości przeciwdziałania dezinformacji polegają na zwiększeniu świadomości społecznej oraz wzmacnianiu prawdziwego, korzystnego dla danego państwa przekazu informacyjnego w mass mediach oraz głównie w mediach społecznościowych. Może to przybierać postać kampanii informacyjnych, do których realizacji – oprócz aparatu państwowego – zaangażowane są podmioty instytucjonalne takie jak NATO czy UE. Inne metody opierają się na zdolnościach przeciwdziałania atakom ze strony mniejszości narodowych, grup terrorystycznych lub innych inspirowanych zewnętrznie aktorów. Dla sprawnego przeciwdziałania zagrożeniom hybrydowym – defensywnie oraz w zakresie potencjału do kontrataku informacyjnego – w omawianej sferze niezbędne są media o zasięgu międzynarodowym. Polska, mimo

rozpoczęcia prac nad tego typu zdolnościami, posiada znacznie słabszą pozycję w tym zakresie niż szereg innych krajów zachodnich. Obok ugruntowania pozycji mediów narodowych w postaci anglojęzycznego kanału telewizji, konieczne powinny być działania zakulisowe polegające na budowie siatki zagranicznych korespondentów, którzy znając oficjalne priorytety polskiej polityki oraz mając pełną wiedzę o wyzwaniach i uwarunkowaniach historycznych, relacjonowaliby wydarzenia dotyczące Polski w sposób obiektywny, poprawiający obraz kraju wśród opiniotwórczych kręgów społeczności międzynarodowej. Ważną sferą wskazującą na potrzebę usprawnienia środków przeciwdziałania zagrożeniom hybrydowym jest zagrożenie ze strony sztucznie wywoływanych migracji. W kontekście wyzwań związanych z tak zwaną pandemią koronawirusów, warto odnotować także możliwość użycia broni biologicznej, co obok dezinformacji, jest kolejnym polem do monitorowania przez odpowiednie instytucje i służby w tym ujęciu.

5. Możliwości poprawy sposobów przeciwdziałania zagrożeniom hybrydowym

W wyniku badań stwierdzono, że aktualne podejście współczesnych państw, w tym –Polski, do przeciwdziałania zagrożeniom hybrydowym – mimo znaczącego postępu w ostatnich latach – wymaga udoskonalenia. Dotychczasowa polska polityka bezpieczeństwa i obrony nadal opiera się przede wszystkim na zapisanym w traktatach, deklarowanym wsparciu sojuszników. Przykład aneksji Krymu i wojny w Donbasie w 2014 r. oraz późniejsza agresja Rosji na Ukrainę w 2022 r. pokazały wyzwania przed jakimi stoją małe i średnie kraje w Europie. Warto odnotować, że Ukraina, mimo pozostawania poza natowskimi strukturami bezpieczeństwa, posiadała gwarancje nienaruszalności swojego terytorium ze strony państw zachodnich. Związanie się przez Polskę z zachodnimi partnerami w obszarze bezpieczeństwa (NATO), jak i gospodarki (UE) było ogromną zmianą mającą swe źródło w zakończeniu Zimnej Wojny. Dzięki osłabieniu się ZSRR, a później Rosji, władze w Warszawie, przy aktywnym, bardzo intensywnym, wsparciu państw zachodnich, były w stanie zmienić kierunek rozwoju w stronę modelu charakterystycznego demokracji liberalnej.

Jak wynika z wykonanych badań, to instytucje, służby i formacje państwa są w pierwszej kolejności odpowiedzialne za przeciwdziałanie zagrożeniom hybrydowym, które najskuteczniej są niwelowane przez wzmocnienie potencjału obronnego danego kraju. Istotę pierwszoplanowej roli państw narodowych (a nie NATO czy UE) w przeciwdziałaniu zagrożeniom hybrydowym trafnie uchwycił P. Szymański, według którego to przede wszystkim „rządy dysponują odpowiednimi zasobami w postaci wyspecjalizowanych struktur wywiadowczych, kontrwywiadowczych i rozpoznania wojskowego (wspieranych przez instytucje odpowiedzialne za przestrzeganie porządku publicznego), narzędzi komunikacji z obywatelami czy zdolności do reagowania na incydenty w cyberprzestrzeni. Są też najbliżej potencjalnych zagrożeń, co – w połączeniu z krótszym niż w przypadku organizacji międzynarodowych procesem decyzyjnym – sprawia, że mogą reagować szybciej na wrogie działania hybrydowe. Ponadto, zapewnienie bezpieczeństwa wewnętrznego stanowi żywotny interes każdego państwa. Oznacza to, że poszczególne rządy są bardziej niż

struktury ponadnarodowe zainteresowane budowaniem odporności na zagrożenia hybrydowe[504].”

Wejście Polski do NATO (a także UE) podniosło niewątpliwie poziom bezpieczeństwa narodowego, stanowiło impuls do modernizacji armii pod względem uzbrojenia oraz zwiększyło atrakcyjność gospodarczą i inwestycyjną kraju. Jednak, w tym samym czasie, niewątpliwy sukces objęcia Polski gwarancjami artykułu 5 Traktatu Waszyngtońskiego spowodował osłabienie wrażliwości decydentów na zagrożenia, które cały czas były obecne w otoczeniu międzynarodowym kraju. W tym kontekście negatywnie należy ocenić decyzje polityczne i sam proces redukcji Sił Zbrojnych, które sprowadzono do poziomu zaledwie ok. 100 tys. Było to znacznie poniżej sił zdolnych stanowić element odstraszania, także w zakresie przeciwdziałania zagrożeniom hybrydowym. Rezygnacja z powszechnego obowiązku obrony i niezastąpienie jej chociażby obligatoryjnymi, cyklicznymi przeszkoleniami na poligonach, co praktykuje m.in. Szwajcaria, także była błędem. Skuteczną obronę przygotowuje się w czasach pokoju. Działania mające na celu zwiększenie zdolności obronnych, mimo że słuszne, nie mogą być podejmowane dopiero w reakcji na sytuację kryzysową u naszych granic, jak miało to miejsce w przypadku Ukrainy w 2022 r. Co więcej, brak obecności znaczących baz wojskowych NATO w Polsce i innych krajach wschodniej flanku Sojuszu, 20 lat od wstąpienia do tej organizacji, także powinien być sygnałem do wzmacniania krajowych sił zbrojnych.

W wyniku przeprowadzonych badań stwierdzono, że – z uwagi na uwarunkowania bezpieczeństwa Polski (m.in. znacznie silniejszy sąsiad w postaci dysponującej ogromną przewagą konwencjonalną i sił atomowych – Rosji), jej potencjał ludnościowy, gospodarczy i technologiczny – koniecznym gwarantem bezpieczeństwa jest program rozwoju własnych zdolności obrony nuklearnej, którą posiada część krajów zarówno w NATO, jak i UE. Także Izrael, który posiada broń jądrową, stanowi tu właściwy punkt odniesienia. Niestety, jak wskazują wyniki przeprowadzonych badań, władze w Warszawie nie tylko nie były w stanie rozpocząć skutecznych przygotowań do takiego rozwiązania, ale wieloletnim opóźnieniom uległ nawet program budowy cywilnych zdolności w zakresie produkcji energii jądrowej (rezygnacja z zaawansowanej budowy elektrowni w Żarnowcu, 50 km od Gdańska, o czym postanowiono we wrześniu 1990 r. – czyli w okresie, w którym kończyła się Zimna Wojna).

[504] P. Szymański, op. cit.

Niską skuteczność takiego podejścia pokazuje przykład zarówno omówionej w rozdziale drugim błyskawicznej aneksji Krymu przez Rosję w 2014 r. (armia ukraińska była wówczas bardzo słaba i niezdolna do obrony), jak i wydarzenia związane z wojną na Ukrainie w 2022 r. Mimo posiadania gwarancji bezpieczeństwa ze strony mocarstw, Ukraina została zaatakowana. Ponadto, abstrahując of faktycznie realnego wzmocnienia patriotycznych postaw i tożsamości narodowej tego kraju, Ukraina przez pierwszy rok wojny została w dużej części zniszczona, jeśli chodzi o infrastrukturę gospodarczą, tkankę ludzką (migracje, straty wojenne), a także sferę militarną (m.in. zniszczenie lub odcięcie dostaw prądu do większości zakładów produkujących amunicję i remontujących uzbrojenie). Stosowanie przez sprzymierzeńców Ukrainy sankcji, narzędzi dyplomatycznych oraz wsparcia wojskowego nie było w stanie zapobiec ani oderwaniu części terytorium ukraińskiego w 2014 r., ani od zniszczenia infrastruktury państwa w czasie inwazji rosyjskiej w 2022 r. Zapewnienie obecnie skutecznej odpowiedzi / obrony Polski powinno być zatem przemodelowane w kierunku zwiększenia własnych zdolności odstraszania sił konwencjonalnych i niekonwencjonalnych, a w dalszej kolejności – kontynuowanie wzmacniania wojskowych powiązań sojuszniczych oraz gospodarczych (NATO, UE).

5.1. Odstraszanie, jako główna metoda zwalczania zagrożeń hybrydowych (wzmocnienie konwencjonalnych i niekonwencjonalnych zdolności obronnych instytucji i służb odpowiedzialnych za bezpieczeństwo wewnętrzne)

Odstraszanie to metoda obrony wykorzystująca zarówno zdolności konwencjonalne, jak i niekonwencjonalne. Zapewnienie bezpieczeństwa poprzez odstraszanie może być realizowane przez połączenie sił konwencjonalnych – armii, sił specjalnych i wywiadowczych oraz niekonwencjonalnych (odstraszanie nuklearne, zdolności do kontrataku cybernetycznego). Rozwiązania pasywne takie, jak przeciwdziałanie dezinformacji powinny mieć rolę wspierającą, ale nie stanowić podstawy przeciwdziałania zagrożeniom hybrydowym w warunkach polskich. Przyjęcie postawy reaktywnej osłabia szanse na wyjście zwycięsko z danej hybrydowej konfrontacji, ponieważ to przeciwnik ma wówczas inicjatywę. Przykład prób eskalacji sporu granicznego Polski z Białorusią, mimo wybudowania muru przez władze w Warszawie, pokazuje dynamikę tego rodzaju zagrożeń.

Jak wynika z badań, koncepcja odstraszania ma długą historię. W czasach współczesnych wykorzystywano ją intensywnie w okresie Zimnej Wojny jako wiodącą

strategię zarządzania relacjami między dwoma supermocarstwami nuklearnymi – Stanami Zjednoczonymi i ZSRR. Jednak strategia odstraszania może być także stosowana przez średnie i małe kraje w celu skutecznej obrony przed zagrożeniami hybrydowymi a także innymi zagrożeniami dla bezpieczeństwa narodowego, co pokazuje przykład Izraela.

Michael Rühle, podaje, że odstraszanie to „groźba użycia siły w celu odwiedzenia przeciwnika od podejmowania niechcianych działań. Można to osiągnąć posługując się groźbą odwetu (odstraszanie przez karę), albo poprzez odmówienie przeciwnikowi szans na osiągnięcie celów działań wojennych (odstraszanie przez odmowę). (…) wszystko, czego potrzeba do odstraszania, to odpowiednia demonstracja siły. Tak długo, jak obie strony działają „racjonalnie", to jest zgodnie z rachunkiem zysków i strat, i żadna z nich nie ma skłonności samobójczych, ich potencjały wojskowe będą utrzymywać się wzajemnie w szachu[505]."

Inną definicję odstraszania podają generał Yossi Baidatz i Dmitry Adamsky, według których jest to „użycie groźby z zamiarem wpłynięcia na kalkulacje przeciwnika w celu utrzymania status quo, czyli rzeczywistości, która wyewoluowała w kontekście danego epizodu pomiędzy dwoma graczami. Odstraszanie miało na celu zapobieganie niepożądanym zachowaniom poprzez przekonanie przeciwnika, że korzyści, jakich może się spodziewać po danym ruchu (…) będą znikome w stosunku do związanych z tym kosztów[506]." Autorzy ci wymienili trzy podstawowe przesłanki ustanowienia reżimu odstraszania: (1) założenie, że obaj gracze są racjonalni (prowadzą kalkulację strategiczną na zasadach „opłacalności", każdy gracz na podstawie własnego świata wartości strategicznych); (2) istnieje wiarygodna groźba odstraszania (uwiarygodnione zdolności i determinacja tego drugiego do jej realizacji ataku odwetowego) oraz (3) komunikacja – groźba musi być w pełni zrozumiana przez przeciwnika i być postrzegana jako realna[507].

Ponadto, w wyniku badań stwierdzono korzystne działanie wzmacniające potencjał obronny w wyniku zastosowania modelu rozszerzonego odstraszania, w którym mocarstwo broni sojusznika poprzez odstraszanie jego wroga. Ten model, jak przypomina Avner Golov,

[505] M. Rühle, *Odstraszanie: co może sprawić, a czego nie,* Przegląd NATO 20 kwietnia 2015 https://www.nato.int/docu/review/pl/articles/2015/04/20/odstraszanie-co-moze-sprawic-a-czego-nie/index.html [dostęp:7.12.2022].

[506] Y. Baidatz, D. Adamsky, *Not Just Deterrence*, Israel Defense 4/03/2015, https://israeldefense.co.il/en/content/not-just-deterrence [7.12.2022].

[507] Tamże.

był powszechne stosowany podczas zimnej wojny, kiedy Stany Zjednoczone starały się zniechęcić Związek Sowiecki do ataku na jego europejskich sojuszników. W tej koncepcji, jego zdaniem, „kluczowym wyzwaniem dla strony broniącej (odstraszającej) było przekonać drugą stronę, iż przesłanie odstraszania było wiarygodne (gotowość działania zgodnie z groźbą użycia siły). Przede wszystkim, obrońca musiał przekonać atakującego (stronę, którą próbuje odstraszyć), że jest przygotowany na eskalację w ich stosunkach (…)[508].”

Jeśli chodzi o odstraszanie nuklearne można mówić o przynajmniej dwóch istotnych jego typach. Jednym jest, występujące podczas zimnowojennej konfrontacji USA z ZSRR, koncepcja MAD (ang. *mutually assured destruction*), która zakładała rozbudowę sił nuklearnych w takim stopniu, aby atak na dany kraj wiązał się z zagładą jądrową. Drugim typem jest odstraszanie minimalne polegające na posiadaniu przez dane państwo tylko takich obronnych zdolności nuklearnych, jakie wystarczą dla skutecznego odstraszenia jego wrogów od wyprowadzenia ataku. Jest to najbardziej rozpowszechniona dziś forma podejścia do kwestii odstraszania na świecie, którą stosują kraje posiadające broń jądrową. Trzeba jednak dodać, że zimnowojenne mocarstwa, cały czas utrzymują arsenał jądrowy, którego użycie wywołałoby destrukcję nie tylko tych państw, ale także – w skali globalnej.

W toku badań sposobów przeciwdziałania zagrożeniom hybrydowym Izraela stwierdzono, że kluczowe znaczenie dla skuteczności jego polityki odstraszania miały nie tylko zdolności konwencjonalne, ale także niekonwencjonalne. Ujawniono także poglądy krytyczne względem zdolności Izraela do obrony siłami konwencjonalnymi, co wskazuje na kluczowe znaczenie dwóch elementów: zwiększonego wsparcia sojuszniczego dla rozwoju konwencjonalnych dolności bojowych oraz utrzymania i rozwoju izraelskich sił nuklearnych dla polityki odstraszania tego kraju. Zdolności obronne Izraela od powstania tego kraju były wyjątkowo wysokie, jednak z czasem, jak dowodził Stanisław Lewicki, coraz bardziej widoczna była konieczność reform, modernizacji armii i wsparcia amerykańskiego dla utrzymania niepodległości tego kraju. Podczas wojny o niepodległość (1948-1949), świeżo utworzone państwo izraelskie „starło się z siłami zbrojnymi wszystkich swoich sąsiadów: Egiptu, Transjordanii, Syrii i Libanu, które wspomagane były także przez siły ekspedycyjne z innych krajów arabskich. Nie mając oficjalnego wsparcia od żadnego sojusznika, za

[508] A. Golov, *Israeli Deterrence in the 21st Century,* Memorandum No. 155, Tel Aviv: Institute for National Security Studies, June 2016, https://www.inss.org.il/wp-content/uploads/systemfiles/INSSMemo155.03.1.Golov.ENG.pdf [dostęp: 6.12.2022].

wyjątkiem dostaw broni z Czechosłowacji, Izrael pokonał zdecydowanie siły zbrojne tych wszystkich arabskich krajów[509].” Z kolei, w wojnie sześciodniowej w 1967 r., „Izrael pokonał siły trzech pogranicznych państw: Egiptu, Syrii i Jordanii, także wspomagane przez kontyngenty innych krajów. W działaniach nie wziął już udziału Liban. W roku 1973 miała miejsce wojna Jom Kipur, gdzie Izrael starł się z siłami zbrojnymi już tylko dwóch państw, czyli Egiptu i Syrii. Na granicy z Jordanią i Libanem starć wojennych nie było. W wyniku tej wojny, siły zbrojne Izraela poniosły ciężkie straty i były w stanie przejść do kontrofensywy tylko dzięki masowym dostawom broni z USA zrealizowanym za pomocą mostu powietrznego. Jak wielu uważa, ta interwencja USA uratowała wtedy Izrael[510].

W ciągu tych kolejnych wojen, jak zauważył S. Lewicki, Izrael „walczył z coraz mniejszą liczbą swoich arabskich przeciwników, zaś wynik tych starć był coraz mniej korzystny dla Izraela, a w wojnie Jom Kipur było już konieczne masowe wsparcie ze strony USA by Izrael mógł zapewnić sobie pożądany wynik. To przesądziło, że ostatecznie Izrael zdecydował się oddać półwysep Synaj dla Egiptu i zawrzeć, za pośrednictwem USA, pokój z tym państwem, gdyż zdał sobie sprawę, że nie ma już dostatecznych sił by dalej konfrontować się z Egiptem i Syrią jednocześnie. Taka tendencja, pokazująca względne słabnięcie Izraela, także i dalej mogła być obserwowana. W roku 1982 doszło do tzw. wojny libańskiej. Izrael wtargnął do Libanu by wyrzucić stamtąd siły wierne Arafatowi. Tym razem Izrael skonfrontował się tylko z siłami Organizacji Wyzwolenia Palestyny oraz wojskiem syryjskim. Wynik tej, toczonej w kilku fazach, wojny jest niejednoznaczny; co prawda Organizacja Wyzwolenia Palestyny została usunięta z Libanu, ale wojska syryjskie tam pozostały, a na dodatek pojawił się Hezbollah, który okazał się o wiele groźniejszym przeciwnikiem niż organizacja podległa Arafatowi[511].”

Jak pokazały wyniki badań, z kwestią odstraszania atomowego związane jest ryzyko rozpowszechnienia się środków jądrowych w takim stopniu, że ich użycie może być dokonywane w sposób pochopny i w sytuacjach, w których można było zastosować innego rodzaju środki obronne (np. siły konwencjonalne, wsparcie sojuszników, presja sankcjami na arenie międzynarodowej). Ryzyko to jest tym większe im bardziej niestabilna władza

[509] S. Lewicki, *Jak silny jest Izrael?,* Portal Myśli Konserwatywnej – Konserwatyzm.pl, 4 września 2021, https://konserwatyzm.pl/lewicki-jak-silny-jest-izrael/ [dostęp:7.12.2022].
[510] Tamże.
[511] Tamże.

panuje w krajach posiadających bron jądrową. Z pozoru wydaje się, że odstraszanie to „stosunkowo prosta idea: jeden podmiot przekonuje drugi – potencjalnego agresora – że agresja pociągnęłaby za sobą koszty, być może w formie strat niemożliwych do zaakceptowania, które zdecydowanie przewyższyłyby potencjalne zyski, zarówno w wymiarze materialnym, jak i politycznym[512].” Jednakże, zaangażowanie przynajmniej dwu podmiotów, jak dowodzi Kęstutis Paulauskas, sprawia, że „odstraszanie jest skomplikowaną interakcją społeczną. Ma bardzo wiele wspólnego z ludzką naturą, psychologią i podstawowymi ludzkimi emocjami: strachem, odwagą oraz żądzą władzy – i zemsty. Przenieśmy to na płaszczyznę podmiotów politycznych, ze wszystkimi zawiłościami związanymi z państwowością i dojrzałością mężów stanu, dodajmy, że stawką jest przetrwanie narodu, wmieszajmy w to broń jądrową – wnet odstraszanie staje się pojęciem nad wyraz skomplikowanym, zmiennym, nieuchwytnym, ale także potencjalnie wybuchowym[513].”

Z przeprowadzonych badań wynika, że zarówno poszczególne państwa, jak i ich organizacje (m.in. NATO) wykorzystują wszystkie będące w ich dyspozycji narzędzia do budowania wiarygodnej postawy odstraszania potencjalnych agresorów. Instrumenty te są bardzo szerokie: od konwencjonalnych narodowych sił zbrojnych, przez system służb mundurowych, wywiadowczych i sił specjalnych, wspieranych przez obronę powietrzną, cyberobronę i wreszcie – odstraszanie nuklearne (w przypadku krajów oficjalnie lub nieoficjalnie dysponujących taką bronią).

Stosując taktykę odstraszania przez odmowę (w tym ujęciu to nie jest kontratak, ale obrona), państwo broniące się utrudnia przeciwnikowi osiągnięcie pożądanego celu. Warunkiem wstępnym odstraszania konwencjonalnego jest zrozumienie intencji i możliwych kierunków wrogich działań przeciwnika oraz ocena, w jakich scenariuszach groźba użycia siły powinna zostać uruchomiona. Z przeprowadzonych badań wynika, że odstraszanie przez odmowę bazuje na strachu i „ma na celu uczynienie agresji przeciwnika nieopłacalną poprzez utrudnienie osiągnięcia celu. Aby jego zdolności defensywne były wiarygodne, obrońca musi zaopatrzyć się w odpowiednie śmiercionośne zdolności (stosowane nie w kontrataku, ale dla obrony) zdolne do uruchomienia w prawdopodobnym

[512] K. Paulauskas, *Zagadnienie odstraszania*, *Przegląd NATO* 5 sierpnia 2016, https://www.nato.int/docu/review/pl/articles/2016/08/05/zagadnienie-odstraszania/index.html [7.12.2022].

[513] K. Paulauskas, op. cit.

miejscu agresji lub w jego pobliżu. Strategia odstraszania przez odmowę była preferowana przez małe państwa, ale może być również stosowana w rozszerzonej formie przez wielkie mocarstwa[514].”

Z kolei, aby odstraszenie przez karę było skuteczne, „groźba ze strony obrońcy musi być wiarygodna. Państwa powinny posiadać wystarczające śmiercionośne zdolności użycia siły, aby poradzić sobie z danym zagrożeniem. Broń w dyspozycji obrońcy musi posiadać zdolności rażenia celów, unikania lub pokonywania systemów obrony wroga i zniszczenia jego sił i/lub populacji kraju agresora (…). Musi być również jasno zakomunikowane, że obrońca jest głęboko przywiązany do obiektu, którego broni i jakie formy zachowania będą skłaniać do odwetu. Odstraszanie przez karę powinno być skierowane przeciwko najpoważniejszym zagrożeniom hybrydowym, jednocześnie przekazując przeciwnikowi wiadomość, że takie czyny wykraczają poza progi graniczne wyznaczone przez obrońcę (tzw. „czerwone linie”) i spotkają się z reakcją karną[515].”

W toku badań stwierdzono, że niezbędnym warunkiem skutecznego odstraszania jest wiarygodność kraju broniącego się takim podejściem. Dla przykładu, w NATO wiarygodność opiera się na trzech elementach: zdolnościach, spójności, i komunikacji (ang. capability cohesion, communication – 3 C)[516]. Wystarczy, że zabraknie jednego z tych elementów lub będzie on osłabiony, cała konstrukcja odstraszania staje się mniej efektywna lub w ogóle przestaje działać.

Pierwszy z elementów wiarygodnego odstraszania – zdolności (potencjał militarny) – jest najważniejszy. Bez niego, ani spójność ani komunikowanie woli użycia siły nie spełni swojego celu. Wróg, dysponując rozpoznaniem wywiadowczym, będzie miał świadomość ograniczeń potencjału obronnego danego państwa-ofiary i wykorzysta je planując i realizując dany atak hybrydowy. Jeśli chodzi o wojskowy potencjał odstraszania, przypadku Polski po 1989 r. następowało systematyczne zmniejszanie armii, która była w przeszłości drugą siłą Układu Warszawskiego. Mimo bezsprzecznych zalet modernizacji polskich sił zbrojnych oraz budowy profesjonalnych (choć zbyt małych) sił specjalnych, co dokonało się dzięki

[514] R. Abbasi, *New Warfare Domains and the Deterrence Theory Crisis*, E-International Relations, May 13 2020 https://www.e-ir.info/2020/05/13/new-warfare-domain-and-the-deterrence-theory-crisis/ [dostęp: 7.12.2022].

[515] Tamże.

[516] K. Paulauskas,

akcesji do struktur natowskich, wielkość oraz uzbrojenie, a także przemysł obronny kraju. Nieporozumienia polityczne, mające swe historyczne źródła, które zmaterializowały się w postaci licznych zmian i braku stabilności służb wywiadu i kontrwywiadu, a także służb mundurowych, także stanowiły czynnik osłabiający w średniej perspektywie czasowej potencjał odstraszania Polski. Problem ten dotyczył przez lata większości krajów NATO, które po pokonaniu ZSRR doprowadziły do zmniejszania liczebności swoich sił zbrojnych oraz cięć wydatków na obronę. Początki zmiany tego podejścia nastąpiły w wyniku wojny Rosji z Ukrainą w 2022 r., w którą wielu członków NATO włączyło się pośrednio wspierając – aspirujące do członkostwa w Sojuszu – władze w Kijowie.

Drugi z elementów wiarygodności, spójność w przypadku państwa oznacza zdolność wszystkich jego struktur do współdziałania w zakresie przeciwdziałania zagrożeniu. Chodzi tu zarówno o jednolity głos ze strony klasy politycznej (poważny mankament polskiej polityki), jak i zapewnienie wysokiego poziomu morale sił obronnych i społeczeństwa oraz wysoki poziom koordynacji działań różnych jednostek i instytucji w obliczu zagrożenia (wspólne ćwiczenia, system dowodzenia). Spójność, w rozumieniu zdolności do jedności i solidarnego działania w obronie wszystkich członków NATO jest najsłabszym z tych elementów. Chodzi zwłaszcza o różnice zdań w ramach europejskich członków tej organizacji. Mimo, że NATO wyszło zwycięsko z zimnowojennej konfrontacji z ZSRR, spójność Sojuszu nie była poważnie przetestowana, co miałoby miejsce w sytuacji np. konieczności obrony terytorium członka z Europy Zachodniej przed agresją radziecką[517]. Trudności w uzyskaniu wysokiej spójności w ramach NATO współcześnie pokazują napięcia polityczne między Polską i najważniejszymi krajami zarówno NATO, jak i UE, które nastąpiły w 2021 r. i 2022 r. Miało to miejsce w czasie ataków hybrydowych na Polskę ze strony Białorusi (migranci na granicy), a następnie, kiedy władze w Warszawie musiały samotnie mierzyć się z falą uchodźców ukraińskich, przy początkowo minimalnym lub nieistniejącym wsparciu systemowym (przyjęcie uchodźców na swoje terytorium) i finansowym ze strony państw partnerskich i sojuszniczych.

Trzecim elementem wiarygodności gwarantującej skuteczne odstraszanie jest komunikowanie, które oznacza mechanizmy skutecznego – zdecydowanego i jednoznacznego – przekazu skierowanego do potencjalnych agresorów. Taka komunikacja

[517] Por. K. Paulauskas, op. cit.

powinna być prezentowana przez najważniejszych przedstawicieli zarówno danego państwa, jak i organizacji obronnej państw (NATO). Komunikacja powinna dotyczyć także możliwości odstraszania nuklearnego – jeśli takie są w posiadaniu państwa lub paktu obronnego[518].

W kontekście debaty nad współczesnymi uwarunkowaniami skutecznego odstraszania w euroatlantyckiej strefie bezpieczeństwa (NATO), M. Rühle, uważa, że kluczowe znaczenie ma sygnał polityczny ze strony USA, że kraj ten postrzega bezpieczeństwo swoich Sojuszników, jako swój fundamentalny interes narodowy. Chodzi o wytworzenie wśród potencjalnych agresorów / wrogów świadomości, że Stany Zjednoczone zaryzykują interwencję siłami konwencjonalnymi, a nawet eskalację nuklearną, w celu obrony terytorium Sojuszu. Przykład USA jest tu zasadny z uwagi na najpotężniejszy potencjał militarny tego kraju. Niemniej jednak pozostałe państwa członkowskie Paktu Północnoatlantyckiego powinny wzmacniać swoje zdolności zbrojne (co do czasu wojny w 2022 r. na Ukrainie czyniły w marginalnym stopniu). Jednak, przesłanie odstraszające „będzie przekonujące jedynie wtedy, gdy Stany Zjednoczone będą militarnie obecne w tych regionach, których według zapewnień bronią. Gwarantuje to, że w przypadku konfliktu Waszyngton będzie zaangażowany od początku. Bez takiej obecności, ani Sojusznicy, ani przeciwnicy nie będą uważać tego nuklearnego zobowiązania za wiarygodne[519].” Na początku kryzysu krymskiego w 2014 r., jak wynika z badań, Stany Zjednoczone wzmocniły swoją obecność militarną w Europie Środkowej i Wschodniej. Wsparły tym samym swoje obietnice pomocy realnymi działaniami w postaci dostaw sprzętu wojskowego. Istotna jest w tym kontekście właśnie komunikacja determinacji Sojuszu do aktywnego odstraszania (zaangażowania się w konflikt zbrojny w razie takiej potrzeby). Gdyby Stany Zjednoczone, co zauważył M. Rühle, „straciły tę wolę – albo zdolność do jej wyrażania – inni szybko zaczęliby testować różne czerwone linie nakreślone przez Waszyngton. Pomimo debaty nad krajowymi priorytetami, Stany Zjednoczone zachowują wyraźną świadomość tego faktu[520].”

[518] Tamże.

[519] M. Rühle, *Odstraszanie: co może sprawić, a czego nie,* Przegląd NATO 20 kwietnia 2015, https://www.nato.int/docu/review/pl/articles/2015/04/20/odstraszanie-co-moze-sprawic-a-czego-nie/index.html [dostęp:7.12.2022].

[520] Tamże.

W wyniku przeprowadzonych badań stwierdzono, że strategia odstraszania, jako metoda przeciwdziałania zagrożeniom hybrydowym była wykorzystywana w NATO. Budowanie odporności, co ma miejsce w krajach natowskich, można rozpatrywać jako działanie mieszczące się w ramach „odstraszania przez odmowę". Ale członkowie Sojuszu byli świadomi, że należy również rozwijać zdolności „odstraszania przez karę", które mają na celu zniechęcenie do ataku potencjalnego agresora poprzez wpływanie na niekorzystny dla niego bilans kosztów i korzyści.

Na szczycie w Warszawie w 2016 r. przedstawiciele państw członkowskich NATO oświadczyli, że ataki hybrydowe niosące znaczące zagrożenie mogą w ostateczności spowodować uruchomienie artykułu 5 Traktatu Waszyngtońskiego. Zagrożenia o mniejszej randze mogą się spotkać z inną reakcją ze strony NATO: od sankcji po wydalenie dyplomatów. Mimo, że takie kroki pozostają wrażliwą międzynarodowo kwestią (sprawa suwerenności narodowej), w określonych sytuacjach sojusznicy, jak ocenili Michael Rühle i Clare Roberts, muszą wysłać komunikat, że działania hybrydowe mają swój koszt dla państwa agresora[521].

W wyniku badań stwierdzono, że rolę sił zbrojnych w odstraszaniu hybrydowych przeciwników oraz użycia siły militarnej analizowało także helsińskie centrum przeciwdziałania zagrożeniom hybrydowym Hybrid COE, którego eksperci doszli do wniosku, że „twarda siła jest nadal warunkiem sine qua non odstraszania[522]." Zgodzić należy się z twierdzeniem, że odpowiedni potencjał wojskowy konwencjonalnego odstraszania wpływa na zmniejszenie ryzyka zastosowania przez agresora hybrydowych środków ataku[523]. Zastanawiając się jak NATO może powstrzymać w przyszłości Rosję przed sprowokowaniem konfliktu zbrojnego, Wojciech Lorenz uznał, że w obliczu zdeterminowanego przeciwnika, Sojusz będzie musiał oprzeć swoje odstraszanie na zdolności do obrony swojego terytorium. Wymagać to będzie zdolności utrzymania spójności politycznej, właściwego reagowania na kolejne stadia eskalacji konfliktu oraz – w ostateczności – prowadzenia wojny konwencjonalnej na dużą skalę i o wysokiej

[521] Tamże.

[522] S. Monaghan, *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice,* Hybrid CoE Paper 12, March 2022, https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf [7.12.2022].

[523] Tamże.

intensywności. Pakt Północnoatlantycki będzie też „musiał być w stanie odstraszyć Rosję od używania broni jądrowej dla tzw. deeskalacji konfliktu konwencjonalnego, co będzie wymagać wiarygodnych zdolności do reagowania (po stronie NATO)[524].”

W świetle wyników przeprowadzonych badań stwierdzić należy, że ewoluujący i dynamiczny charakter zagrożeń hybrydowych w dobie intensyfikacji strategicznej rywalizacji mocarstw na arenie międzynarodowej przyczynia się do wzrostu ryzyka eskalacji wielu konfliktów. Chodzi o przekształcenie się ograniczonego konfliktu hybrydowego w działania z użyciem broni konwencjonalnej, a nawet nuklearnej (ang. wormhole escalation). Aby przeciwdziałać temu rodzajowi zagrożenia, odstraszanie nuklearne i konwencjonalne powinno być utrzymane tam, gdzie to możliwe poprzez przewagę siły i jasny przekaz skierowany do państwa agresora o zdecydowaniu do odegrania przez państwo-obrońcę dominującej roli w potencjalnym konflikcie. Rola tych czynników powinna być należycie uwzględniana w kontekście działań mających na celu uzyskanie skutecznego efektu odstraszania w zakresie agresji zbrojnej na dużą skalę (wojna), jak i znaczących zagrożeń hybrydowych[525].

Zgodzić należy się z M. Rühle, który skrytykował rekomendacje wycofania taktycznej broni nuklearnej stacjonującej w różnych państwach NATO, jakie pojawiały się po aneksji Krymu przez Rosję w 2014 r. Argument, że sojusznicza broń jądrowa nie powstrzymała rosyjskiej agresji na Ukrainę był, według tego autora, nietrafiony. Gdyby ta logika była słuszna, jak dowodzi M. Rühle, „należałoby także zlikwidować wszystkie narodowe siły zbrojne, a nawet NATO. Ponieważ żadna armia i żaden sojusz nie odstraszyły Rosji od aneksji Krymu i destabilizacji wschodniej Ukrainy. Bardziej realistyczna analiza sytuacji na Ukrainie będzie prowadzić do stwierdzenia, iż jest to nie tyle kwestia odstraszania, co geografii oraz interesów. Rosja jest gotowa zapobiegać integracji Ukrainy z Zachodem nawet za pomocą środków zbrojnych podczas, gdy Zachód nie jest skłonny ryzykować eskalacji zbrojnej na rzecz kraju, który nie należy do NATO. Innymi słowy, przykład Ukrainy nie nadaje się by potwierdzić lub zaprzeczyć działaniu odstraszania. Ewentualnie dowodzi, że kraj, który jest politycznie i wojskowo słaby jest łatwym łupem dla

[524] W. Lorenz, Deterrence in the Baltic Sea Region. A View from Poland, The Hague Centre for Strategic Studies January 2022, https://hcss.nl/wp-content/uploads/2021/12/04-Deterrence-in-the-Baltic-Sea-Region-HCSS-2022.pdf [dostęp: 7.12.2022].

[525] S. Monaghan, op. cit.

potężnego sąsiada[526].” Ocena ta, mimo upływu szeregu lat, wydaje się celna w pewnym sensie także w odniesieniu do agresji rosyjskiej na Ukrainie w 2022 r. Mimo największego w historii NATO wsparcia dla Ukrainy (uzbrojenie, pomoc wojskowa), Pakt nie zdecydował się bezpośrednio zaangażować w tę wojnę toczoną w bliskości, ale – mimo wszystko – poza obszar natowski zdefiniowany traktatem waszyngtońskim z 4 kwietnia 1949 r.

W wyniku przeprowadzonych badań stwierdzono, że posiadanie przez wszystkie strony konfliktu broni nuklearnej stanowi czynnik skłaniający państwa do wyznaczenia granic rywalizacji, w ramach których ryzyko eskalacji nuklearnej jest zminimalizowane. Jednak nie można zapominać, że użyta broń nuklearna (lub groźba jej użycia) może być również zastosowana w ramach agresji hybrydowej[527]. Ponadto, przewaga danego państwa w zakresie potencjału nuklearnego może stanowić czynnik przyczyniający się do zwiększonej swobody jego działań ofensywnych. Przykładem jest tu Rosja, której arsenał jądrowy o globalnym zasięgu i sile rażenia, niewątpliwie zwiększył swobodę działań Kremla w zakresie inwazji na Ukrainę, zarówno w 2014 – jak i w 2022 r.

Wśród przykładów zawodności odstraszania niektórzy badacze podawali wojnę o Falklandy w 1982 r., kiedy to Argentyna zakwestionowała władzę Wielkiej Brytanii nad tymi wyspami. Ku zaskoczeniu rządzącej wówczas Argentyną junty wojskowej, strona brytyjska wysłała swoją marynarkę wojenną i odzyskała kontrolę nad tym terytorium. Dowódca argentyński gen. Galtieri miał przyznać, iż „nigdy nie przypuszczał, że europejskie państwo będzie gotowe ponieść tak wysoką cenę za kilka nieznaczących wysp położonych tak daleko[528].” Różnica potencjałów wojskowych Wielkiej Brytanii i Argentyny bezsprzecznie przemawiała na korzyść tej pierwszej, mimo to odstraszanie nie zadziałało. Stało się tak po pierwsze dlatego, że po stronie argentyńskiej zabrakło świadomości nieuchronności reakcji brytyjskiej. Drugim czynnikiem, który dobrze scharakteryzował M. Rühle, był deficyt racjonalności obserwowany u władz argentyńskich. Z uwagi na presję polityczną w kraju (oraz wcześniej omówiony brak świadomości woli działania władz w Londynie) junta wojskowa w Argentynie starała się – poprzez zajęcie Falklandów – odwrócić uwagę obywateli od problemów wewnętrznych i skonsolidować swoją władzę. W kryzysowych sytuacjach, jak dowodzi autor, „ludzie mają tendencję do tego, aby kierować

[526] M. Rühle, op. cit.
[527] S. Monaghan, op. cit.
[528] M. Rühle, op. cit.

się inną logiką (…) ci, którzy obawiają się stracić coś cennego są gotowi podejmować większe ryzyko, niż ci, którzy mają nadzieję coś zyskać. W odniesieniu do wojny o Falklandy oznacza to, że dla junty, która była pod politycznym ostrzałem okupacja „Malwinów" (Falklandów) miała na celu nie tyle odniesienie korzyści, co uratowanie się przed utratą władzy. To skłoniło ich do podjęcia ryzyka, którego w innych okolicznościach nie odważyliby się podejmować. Zabrakło racjonalności, która jest wstępnym warunkiem stabilnego odstraszania[529]."

Kryterium racjonalności miało także zastosowanie do oceny działalności ugrupowań zbrojnych występujących przeciwko Izraelowi, takich jak Hamas czy Hezbollah. Odnotowując wsparcie jakie posiadają oni ze strony państw (np. Iranu) były to jednak struktury dysponujące znacznie mniejszą siłą militarną, niż armia izraelska. Mimo tego, kierując się motywacjami narodowowyzwoleńczymi i religijnymi, podejmowały one walkę z silniejszym przeciwnikiem (stosując często metody walki hybrydowej i asymetrycznej). Rząd niemiecki oferował znaczne sumy pieniędzy porywaczom olimpijczyków z Izraela w czasie wydarzeń określonych jako „Masakra w Monachium", ale terroryści z „Czarnego Września" odmówili twierdząc, że nie interesuje ich to, ponieważ kierują nimi motywy pozafinansowe (wiara w wartości i cele w życiu pozagrobowym). Takie nastawienie było charakterystyczną postawą fundamentalistów muzułmańskich. Fundamentalizm, jak podaje *Słownik języka polskiego,* to „bezwzględna wierność doktrynie, zasadom religii, rygorystyczne ich przestrzeganie. (…) Z punktu widzenia nieograniczonej tolerancji – każda wierność zasadom może się wydać fundamentalizmem, z punktu widzenia fundamentalizmu – każda tolerancyjność jest zbrodnią[530].

Przeciwdziałanie zagrożeniom hybrydowym, podobnie jak kształtowanie szerszej polityki bezpieczeństwa i obrony, powinno mieć racjonalne podstawy. Podając za *Słownikiem języka polskiego,* racjonalny to mający rozumowe podstawy, efektywny oraz przemyślany, logiczny i rozsądny[531]. Liczne przykłady działań polskich władz w przeszłości wskazują, że racjonalność nie zawsze była elementem planowania i realizacji działań z zakresu obronny i bezpieczeństwa państwa.

[529] Tamże.

[530] *Słownik języka polskiego*, Wydawnictwo Naukowe PWN 2022, https://sjp.pwn.pl [dostęp: 20.12.2022].

[531] Tamże.

W toku badań stwierdzono, że przeciwdziałanie zagrożeniom hybrydowym wymaga działań wykraczających poza samo odstraszanie. Odstraszanie jako strategia nie powinna występować samodzielnie, ale być zgodna z działaniami państwa i jego instytucji w zakresie polityki zagranicznej (zarządzania jego stosunkami zewnętrznymi). Istnieje konieczność podejmowania działań wykraczających poza odstraszanie. Efektywne podejście do przeciwdziałania zagrożeniom, w tym – hybrydowym, wymaga łączenia różnych strategii obronnych. Tak jak odporność (sama w sobie) nie jest wystarczającą strategią, zastosowanie wyłącznie odstraszania także nie przyniesie pozytywnego rezultatu. W przypadku, kiedy mamy już do czynienia z rozpoczętą kampanią ataków hybrydowych, należy stwierdzić, że system odstraszania państwa broniącego się w znacznym stopniu zawiódł[532].

Jak pokazały wyniki badań, sam potencjał wojskowy nie jest wystarczający do efektywności odstraszania. Jeśli chodzi o zalety odstraszana, musi ono by poparte przekonaniem przeciwnika o nieuchronności, skuteczności i sile odwetu. Tylko w ten sposób podejście to spełni swoje zadanie. Jest mało prawdopodobne, jak pisze Wojciech Lorenz, aby „wzmocnione odstraszanie konwencjonalne i nuklearne powstrzymało Rosję od próby wykorzystania słabości politycznych w państwach członkowskich i w całym Sojuszu. (…) Konflikt hybrydowy poniżej progu otwartej wojny będzie postrzegany przez Rosję jako opłacalny instrument walki i wpływania na politykę członków NATO w celu komplikowania decyzji Sojuszu. Nawet jeśli członkowie NATO staną się mniej podatni na takie szkodliwe wpływy, nadal pozostaną słabe punkty społeczne i polityczne, które można wykorzystać do pogłębienia polaryzacji politycznej w państwach demokratycznych[533].” Niemniej jednak, podejście to nie wyklucza, że kraje takie jak Polska, w porozumieniu z sojusznikami, w tym z NATO, mogłyby realizować działania zniechęcające potencjalnych agresorów do stosowania broni hybrydowej. W takim wypadku, zagrożenie prezentowane przez sztucznie wywołany przez Białoruś – i niosący ryzyko groźnej eskalacji – kryzys graniczny z udziałem migrantów, zostałyby zniwelowane przez zastosowanie groźby lub działań prowadzonych metodami niejawnymi (np. za pomocą służb i /lub sił specjalnych np. na terytorium wroga lub w państwie trzecim uczestniczącym w procederze przerzutu migrantów). W przypadku zidentyfikowania zaangażowania w daną operację podmiotów pozapaństwowych,

[532] S. Monaghan, op. cit.
[533] W. Lorenz, op. cit.

działaniami odwetowymi należałoby również objąć taki podmiot. Warunkiem byłoby naturalnie posiadanie odpowiednich zdolności do działania tego typu przez Polskę, które obecnie są ograniczone.

Wiarygodność odstraszania, na co słusznie zwrócił uwagę Wojciech Lorenz, będzie ciągłym, dynamicznym procesem. Będzie to wymagało nie tylko usprawnienia gotowości sił NATO do zapewnienia wsparcia sojuszniczego, ale także długoterminowej modernizacji potencjału militarnego, co będzie niezbędne dla utrzymania przewagi militarnej i technologicznej nad Rosją[534].

Przeciwdziałanie zagrożeniom hybrydowym, a także metody ich usprawniania, należy rozpatrywać w kontekście priorytetów polskiej polityki bezpieczeństwa, do których od szeregu lat należą: członkostwo w NATO, współpraca z USA, członkostwo w UE oraz współpraca regionalna. W celu usprawnienia metod przeciwdziałania zagrożeniom hybrydowym w Polsce powinno się uwzględnić korzystne z polskiego punktu widzenia zalecenia UE oraz wytyczne NATO w tym obszarze. Ukierunkowanie Polski na kooperację w ramach tych form współpracy nie powinno jednak wyczerpywać działań mających na celu wzmocnienie polskich zdolności przeciwdziałania zagrożeniom hybrydowym.

W celu podniesienia efektywności przeciwdziałania zagrożeniom hybrydowym Polska i kraje zachodnie mogą podjąć szereg działań. W kontekście przeciwdziałania zagrożeniom hybrydowym względem Polski konieczne jest wzmocnienie zdolności odstraszania i obrony przede wszystkim Polski, a w drugiej kolejności także innych państw na wschodniej flance Sojuszu Północnoatlantyckiego, który dostarcza najważniejszego i najskuteczniejszego źródła gwarancji bezpieczeństwa w Europie.

Wzmocnienie konwencjonalnych i niekonwencjonalnych zdolności odstraszania danego państwa jest najlepszym sposobem obrony przed zagrożeniami hybrydowymi. Konieczność szybkiej i adekwatnej rozbudowy krajowych zdolności odstraszania wynika z faktu, że rozwiązania NATO w tym zakresie nie są wystarczające w aktualnej sytuacji bezpieczeństwa w otoczeniu Polski. Obecna polityka odstraszania Sojuszu w przypadku wojny hybrydowej opiera się głownie na szybkiej reakcji wojskowej. Słabość tego podejścia wynika z faktu, że nie ma pewności odnośnie porozumienia krajów członkowskich, co do źródła konfliktu oraz trafnego zidentyfikowania zagrożenia. Natura ataku hybrydowego

[534] Tamże.

(mogącego oznaczać początek wojny konwencjonalnej) utrudnia jego szybkie i prawidłowe rozpoznanie. Generuje to istotną barierę dla szybkiego podjęcia działań zbiorowych. Istnieją także ograniczenia dotyczące zakresu oraz szybkości udzielenia ewentualnego wsparcia. Jak dowodzi Peter Pindják, „niezależnie od tego, jak szybka może być reakcja, rozmieszczenie sił zbrojnych na obszarze ogarniętym wojną hybrydową okaże się [w większości przypadków] niedostateczne oraz spóźnione[535]". Ponadto, sojusznicy, nawet ci, którzy w czasach pokoju deklarują zdecydowane wsparcie w ramach NATO, mogą nie posiadać w określonym czasie wystarczających sił wojskowych i/lub woli, a także zdolności ich przemieszczenia w miejsce zagrożenia (np. na wschodnią granicę Polski).

Pozytywnie należy ocenić decyzję NATO na szczycie 25 lutego 2022 r. o wzmocnieniu wschodniej flanki NATO poprzez dodatkowe wsparcie wojskowe. W Polsce przebywało w 2022 r. kilkanaście tysięcy żołnierzy sił sojuszniczych, w zdecydowanej większości amerykańskich. Jednak realne gwarancje bezpieczeństwa powinny być uskutecznione w postaci możliwości szybkiego przerzucenia na teren Polski sił natowskich, co obecnie – w ocenie części ekspertów – może nastąpić najwcześniej ok. 6 miesięcy od początku agresji na Polskę. Jest to wysoce niezadowalająca perspektywa, która jest faktem mimo, że minęło ponad 20 lat od wejścia Polski do NATO.

W wyniku badań stwierdzono, że – mimo wzrostu wydatków na bezpieczeństwo i modernizacji sil zbrojnych – Polska powinna znacząco je zwiększyć, co odpowiadałoby realnie występującym zagrożeniom hybrydowym oraz konwencjonalnym w regionie Europy Środkowej i Wschodniej. W kontekście zaostrzającego się napięcia między państwami zachodnimi i Rosją oraz Chinami, a także wyzwań związanych z wojną na Ukrainie, nie można wykluczyć intensyfikacji ataków hybrydowych lub nawet rozszerzenia rosyjsko-ukraińskiego konfliktu także na inne kraje Europy Środkowej i Wschodniej, w tym – na Polskę. Badania polityki poszczególnych krajów względem konfliktu na Ukrainie, który bezpośrednio zagraża wschodniej flance NATO, pokazały, że wsparcie wielu państw NATO dla Polski, przynajmniej w początkowym etapie konfliktu, ograniczyłoby się do wysyłania uzbrojenia oraz amunicji, tak jak ma to miejsce w przypadku ukraińskim.

[535] P. Pindják, *Deterring hybrid warfare: a chance for NATO and the EU to work together?,* NATO Review, 18 November 2014, https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html [dostęp:7.12.2022].

Nakłady Polski na wydatki obronne niemal corocznie odnotowują wzrost, od 2012 r. wzrosły o 58%. Polska należy do grona krajów o najwyższych wydatkach obronnych na świecie – w rankingu SIPRI znalazła się w 2021 r. na 20. miejscu[536]. Państwa NATO i UE nadal zajmują wysokie miejsca w rankingu wydatków obronnych, jednak trwale rośnie rola państw z innych regionów. W tym kontekście, jak i wobec zagrożeń dla bezpieczeństwa międzynarodowego, ważne jest utrzymanie – pomimo ograniczeń i trudności związanych z pandemią – wzrostowego trendu wydatków obronnych w regionie europejskim, zgodnie ze zobowiązaniami ze szczytu NATO w Newport. W 2021 r. 8 z 26 europejskich państw NATO posiadających siły zbrojne wydało przynajmniej 2% PKB na obronność, co oznacza spadek w porównaniu do roku poprzedniego (wówczas 9 państw, aczkolwiek w 2014 r. – zaledwie dwa państwa). W odpowiedzi na rosyjską inwazję na Ukrainę w lutym 2022 r. kilka europejskich państw NATO (Polska, Belgia, Dania, Niemcy, Litwa, Holandia, Norwegia i Rumunia) ogłosiło plany zwiększenia budżetów obronnych w celu osiągnięcia lub przekroczenia zobowiązania z Newport dot. utrzymania wydatków obronnych na poziomie 2% PKB.

W wyniku przeprowadzonych badań stwierdzono, że znaczenie kwestii zwiększenia zdolności odstraszania potencjalnych agresorów przez dany kraj pokazuje aktualna sytuacja Ukrainy. Od 2014 r. Ukraina, orientując się na zachodni kierunek modernizacji armii, dokonała znaczących postępów w zakresie wzmocnienia swoich zdolności obronnych. Po aneksji Krymu, Federacja Rosyjska mogła zająć całą Ukrainę, ponieważ władze w Kijowie nie były przygotowane do skutecznej obrony, a zwłaszcza do konfrontacji z tak potężnym przeciwnikiem. W 2022 r. sytuacja się zmieniła, i – mimo iż Rosja nadal dysponowała ogromną przewagą militarną – Kremlowi nie udało się zrealizować planu błyskawicznego zajęcia ukraińskiej stolicy oraz opanowania Ukrainy w 10 dni oraz anektowania jej w ciągu kilku miesięcy (do sierpnia 2022 r.)[537]. Rosyjska inwazja na Ukrainę w 2022 r. zmieniła układ

[536] *Trends in world military expenditure 2021*, SIPRI 2022 https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf [dostęp: 10.12.2022].

[537] Na rok przed wybuchem wojny na Ukrainie w 2022 r. – jak oceniał Brian Mefford, założyciel firmy konsultingowej Wooden Horse Strategies z siedzibą w Kijowie, a wcześniej ekspert amerykańskiego International Republican Institute – długoterminowa trajektoria Ukrainy w kierunku integracji ze strukturami zachodnimi jest pewna. Jednak, krótkoterminowe perspektywy w tym zakresie jak dodał, pozostają niewiadomą. Na poziomie strategicznym cele Rosji wobec Ukrainy pozostawały niezmienne i zakładały niedopuszczenie do rozwoju tego państwa w kierunku integracji ze strukturami europejskimi i euroatlantyckimi (UE i NATO), co miało zagwarantować utrzymanie wpływów rosyjskich nad Dnieprem. B. Mefford, *Ukraine embraces openness with new report on Russian hybrid warfare challenges,* Atlantic

sił i uwarunkowania bezpieczeństwa w Europie. Jak wynika z badań, Rosja będzie kontynuowała dotychczasową politykę odbudowy stref buforowych oddzielających ją od – postrzeganych za zagrożenie – krajów zachodnich zgrupowanych w NATO – najpotężniejszym pod względem potencjału sił zbrojnych (defensywnym) bloku wojskowym.

W toku badań stwierdzono, że agresja Federacji Rosyjskiej na Ukrainę w 2022 r. odbyła się z wykorzystaniem metod hybrydowych (zwłaszcza dezinformacji), które zostały najbardziej intensywnie aktywowane na miesiące przed rozpoczęciem działań wojskowych. Celem rosyjskiej kampanii była nie tylko Ukraina, ale także państwa NATO oraz te spoza przestrzeni euroatlantyckiej, Propagowano zarzuty o rasizm, ambicje terytorialne Polski wobec Ukrainy, co trafiało do świadomości społeczeństw zwłaszcza w państwach Afryki czy Bliskiego Wschodu, ale także zachodnich. Ważnym celem, który Polska i inne – chcące pozostać niezależne – kraje regionu powinny osiągnąć, jest ograniczenie szkodliwego oddziaływania Federacji Rosyjskiej na instytucje UE oraz państwa członkowskie. Kreml był skuteczny jeśli chodzi o zbudowanie sieci wpływów w centrum europejskich elit politycznych i gospodarczych, co potwierdziła zgodna realizacja pierwszej oraz drugiej nitki osłabiającego bezpieczeństwo regionu Gazociągu Północnego.

Osią narracji hybrydowej Kremla była idea tzw. Ruskiego Miru, która zakłada zjednoczenie ludności rosyjskojęzycznej w jednym organizmie państwowym. W oparciu o tę koncepcję przez lata Federacji Rosyjskiej podważała ukraińską tożsamość narodową oraz prawo Ukrainy do istnienia. Podobne argumenty deprecjonujące pozycję międzynarodową były kierowane pod adresem Polski, co również udowadnia, że kraj nad Wisłą znalazł się na celowniku działań hybrydowych realizowanych przez Moskwę. Dla Rosji, Polska jest krajem dającym przykład pomyślnej transformacji i transformacji systemowej z ważnego dla Kremla państwa zależnego i drugiej pod względem liczebności armii Układu Warszawskiego, do członka UE i NATO.

W świetle wyników przeprowadzonych badań należy ocenić, że przeciwdziałanie zagrożeniom hybrydowym oraz innym wymaga planowego wzmacniania potencjału obronnego kraju, przewidywania ruchów przeciwników oraz scenariuszy zachowań

Council, February 1, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-embraces-openness-with-new-report-on-russian-hybrid-warfare-challenges/ [dostęp:28.11.2022].

sojuszników. Wybuch kolejnej odsłony wojny na Ukrainie w 2022 r. mógł zostać przewidziany w związku z rozwojem sytuacji bezpieczeństwa w regionie Europy Środkowej i Wschodniej. Dla decydentów politycznych aneksja Krymu i wojna w Donbasie od 2014 r. powinny być wystarczającym sygnałem ciągle występujących zagrożeń, niezależnie od pozornej stabilizacji międzynarodowej. Polska powinna w pierwszej kolejności dążyć do wzmocnienia swojego bezpieczeństwa oraz wypracowania możliwie najbardziej niezależnego przemysłu obronnego oraz odpowiedniego systemu szkolenia i patriotycznego wychowania młodych pokoleń. Co istotne, w sytuacji występowania zagrożeń egzystencjalnych, powinno się kształtować zdolność do długoterminowego myślenia o interesie państwa i narodu także w oparciu o wnioski płynące z historii. Rozwój patriotycznego ducha oraz dobre przygotowanie szkoleniowe, sprzętowe nie powinny być rozwijane bez kultywowania zdolności do samodzielnego myślenia. Jest to istotne w kontekście przeciwdziałania zagrożeniu w postaci sprowokowania przez silniejszego agresora konfrontacji, która będzie miała na celu zniszczenie sił państwa uważnego za wrogie. Krytyczny jest tu moment uderzenia – póki zdolności obronne kraju-ofiary znajdują się w fazie wzrostu. To podejście bazujące na zasadzie ucieczki do przodu jest często stosowane, aby zniszczyć rodzący się ruch oporu lub opozycję.

Zgodne z prawdą relacjonowanie przebiegu wojny jest rzadkością, ponieważ strony konfliktu (w przypadku działań hybrydowych – może być ich więcej niż dwie) stosują wybiórcze prezentowanie korzystnych ze swojego punktu widzenia informacji. Walka z fałszowaniem rzeczywistości przez aktorów państwowych, zwłaszcza tak potężnych jak Rosja, to często również wyścig z czasem. Wzmocnienie naszej odporności na dezinformację zależy od siły naszych agencji rządowych, realnego wsparcia ze strony sojuszników oraz sprawnego przepływu informacji i efektywnie działającego systemu monitorowania zagrożeń, które mogą uderzać w wizerunek lub zagrażać bezpieczeństwu Polski. Coraz bardziej nasilające się rosyjskie operacje dezinformacyjne, wycelowane zwłaszcza w kraje graniczne NATO, takie jak Polska czy Litwa, będą wymagały znalezienia skutecznych środków odpowiedzi, ale na pierwszym miejscu powinno znaleźć się jednak zapewnienie tzw. twardej obrony w przypadku przerodzenia się operacji hybrydowej w stricte militarną (odpowiednio liczne, patriotycznie wychowane oraz dobrze wyposażone i wytrenowane siły zbrojne). Przeciwdziałanie zagrożeniom hybrydowym wymaga podejścia obejmującego całe

społeczeństwo i całościowe zarządzanie (ang. *whole-of-society / whole-of-governance approach*).

W rezultacie badań stwierdzono, że działania hybrydowe są używane przez państwa jako niezależna taktyka, której najbardziej charakterystycznym i unikalnym wyróżnikiem jest fakt, iż jest ona stosowana metodami poniżej progu wojny. Mogą one stanowić wstęp do otwartych, jawnych działań zbrojnych, ale mogą także być realizowane autonomicznie już po rozpoczęciu wojny. Przykładem zastosowania tego podejścia była postawa Rosji, która – mimo rozpoczęcia inwazji na Ukrainie – nie zaprzestawała hybrydowych, skrytych działań przeciwko Ukrainie (cyberataki, marginalizacja na forach organizacji międzynarodowych), a także przeciwko wspierającym ją krajom zachodnim (dezinformacja, zastraszanie użyciem broni jądrowej)[538].

Potężne, doświadczone w boju siły zbrojne, jak wynika z badań, są istotnym elementem odstraszania potencjalnych agresorów także przed atakami hybrydowymi. Warunkiem realizacji jakiejkolwiek polityki państwa jest zabezpieczenie jego istnienia (niepodległości, suwerenności). „Trzeba „być", aby realizować jakąkolwiek politykę", jak zauważył prof. Przemysław Żurawski vel Grajewski w czasie konferencji Bezpieczeństwo wschodniej flanki NATO w Warszawie 19 października 2022 r.[539] W sytuacji geopolitycznej w jakiej znajduje się Polska, zwłaszcza w obliczu zagrożenia po inwazji Rosji na Ukrainę, wydatki obronne powinny być bezwzględnym priorytetem. II Rzeczpospolita, jak zaznaczył przedstawiciel Narodowej Rady Rozwoju przy Kancelarii Prezydenta RP (KPRP), miała zbilansowany budżet, ale nie pomogło to ochronić kraju przed przegraniem wojny obronnej w 1939 r. Najbardziej korzystną i dającą niezależność opcją, jak dodał, jest rozwijać swoje uzbrojenie w ramach krajowego przemysłu zbrojeniowego. Jednak wymaga to wielu lat inwestycji finansowych m.in. w badania i rozwój. Aby zapełnić luki w wyposażeniu sił zbrojnych, kraj znajdujący się w potrzebie powinien pozyskać odpowiedni sprzęt z zagranicy, ale jednocześnie zagwarantować transfer technologii (offset). W 1939 r. Polska zakupiła czołgi i samoloty od krajów sojuszniczych (m.in. Francji). Krajowy przemysł

[538] Rozmowa z prof. dr hab. Tomasz Grzegorz Grosse w czasie konferencji „Bezpieczeństwo wschodniej flanki NATO", Instytut Sobieskiego, Warszawa 19 października 2022 r.

[539] J. Borowski, *Przydacz: Sojusz postanowił wzmocnić wschodnią flankę, to zadanie dla dyplomatów i polityków*, Radio Opole 2022-10-19, https://radio.opole.pl/104,631182,przydacz-sojusz-postanowil-wzmocnic-wschodnia-fl [dostęp: 20.10.2022].

obronny (w tym Centralny Okręg Przemysłowy) nie był w stanie zapewnić adekwatnych do potrzeb dostaw uzbrojenia.

Niszczenie wiarygodności elit rządzących i autorytetów w państwie atakowanym hybrydowo jest istotnym celem wielu agresorów. Odpowiednikiem takiego działania hybrydowego w warunkach *stricte* wojennych, była fizyczna likwidacja elit przywódczych wielu podbitych państw w czasie II wojny światowej (zwłaszcza przez stronę rosyjską, oraz niemiecką). Polska i inne kraje leżące w tej części Europy, w ocenie P. Żurawskiego vel Grajewskiego, powinny antycypować, iż tego typu zagrożenie może się powtórzyć w przyszłości. Jeżeli założyć, że mogłyby one zostać dokonane skrytymi metodami, można mówić o potencjalnym zagrożeniu hybrydowym w tym obszarze. Tzw. „zhołowienie" (czyli pozbawianie głowy), było wstępnym warunkiem podporządkowania sobie narodu. Chodzi o uczynienie z niego bezwolnej masy ludzkiej pozbawionej kierownictwa w postaci elit: politycznych, kulturalnych, biznesowych. W odniesieniu do zbrodniczych działań strony radzieckiej w przeszłości, jak piszą Jerzy Gapys i Mariusz Nowak, zasadniczo represje były „wymierzone w osoby (niezależnie od narodowości) przynależne do elity społecznej i majątkowej Drugiej RP (tj. ziemiaństwo, inteligencja, duchowni, przedsiębiorcy) oraz polityczną (działacze polityczni i społeczni, urzędnicy, wojskowi, policjanci, itp.)[540]."

Przeciwdziałanie zagrożeniom hybrydowym należy postrzegać w kategoriach całościowej obrony narodowej, którą – jak słusznie zauważył prof. R. Jakubczak – należy budować od fundamentów. Jednym z dwóch podstawowych komponentów sił zbrojnych, obok wojsk operacyjnych, powinna być właśnie powszechna obrona terytorialna. W historii świata daje się zauważyć tendencję, że nikt na silnego nie napada, co odnotował prof. Jakubczak („nawet silni nie napadają na silnego"). Agresor najpierw osłabia dany podmiot państwowy różnymi sposobami – współcześnie wykosztuje do tego bardzo skutecznie różnorodne działania hybrydowe. Robi się to po to, aby państwo osłabione było łatwym łupem. Obronność państwa polskiego jest ciągle niedoinwestowana, a odporność strategiczna Polski może i powinna być pilnie zwiększona[541]. Cenne są tu wnioski z historii.

[540] J. Gapys, M. Nowak, *Polityka niemieckich i radzieckich okupantów wobec polskiego ziemiaństwa w latach II wojny światowej*, Przegląd Wschodnioeuropejski 2, 2011, s. 93-108.

[541] R. Jakubczak, *Obronę trzeba budować od fundamentów*, wywiad w ramach Forum Strategicznego Defence24.pl i Fundacji Instytut Bezpieczeństwa i Strategii (FIBiS) 11.11.2020, https://defence24.pl/polityka-obronna/prof-jakubczak-obrone-trzeba-budowac-od-fundamentow [dostęp: 9.03.2022].

Przywództwo państwowe Polski zgodziło się na rozbiory uznając, że wróg jest silniejszy (z wyjątkiem konfederatów barskich, którzy próbowali walczyć). Był to błąd, jak zauważył prof. R. Jakubczak. Efekty były dalekosiężne w negatywnych skutkach,. Zlikwidowano państwowość (instytucje, urzędy), podniesiono podatki (30 krotnie w stosunku do okresu przedrozbiorowego), unicestwiono szkolnictwo wojskowe i niszczono dobra kultury. Wywożono zasoby narodowe oraz Polaków na zsyłki. Zaborcy bardzo sprawnie uzupełniali swoje szeregi wojsk rekrutami z terenów polskich. Po zakończeniu I wojny światowej do Polski przybyło 1 mln 350 tys. dobrze uzbrojonych Polaków (tyle służyło wówczas w obcych armiach), co pokazuje skalę tego zjawiska[542].

Jeśli dany kraj nie będzie się przygotowywać do skutecznej obrony, a będzie polegać wyłącznie na sojuszach, jak dowodzi R. Jakubczak, ryzykuje stanie się kolonią, gdzie można rozgrywać wojny zastępcze (sytuacja np. na terenie Afganistanu). W Afganistanie od wieków wojny prowadziły mocarstwa, które wykorzystywali miejscowych jedynie do swoich interesów. Jeśli dany kraj jest wystarczająco silny militarnie to żadne państwo trzecie nie rozgrywa na jego terenie wojen zastępczych. Polska była w obecnym miejscu Afganistanu przez 123 lata zaborów, ponieważ nie miała silnej państwowości w znaczeniu zbrojnym – obronności. Powodem była słabość polskich sił zbrojnych, mizeria zdolności odstraszania[543].

Aby istnieć jako podmiot międzynarodowy, trzeba mieć zdolności i wolę. Jeśli dany kraj nie ma chęci aktywnego udziału we własnej obronie to najlepszy sojusznik nie pomoże, nie będzie w stanie lub nie będzie chciał obronić danego kraju partnerskiego. Sojusz należy traktować jako środek wzmocnienia posiadanych zdolności obronnych. Ale nigdy nie powinien to być środek zastępczy[544]. W historii Polski warte odnotowania jest zastąpienie obrony powszechnej (tzw. piastowskiej) wynajętymi wojskami obcymi (Sasów, Rosjan i Szwedów). W rezultacie Polska dała sygnał tym krajom, w tym Rosji, że sama nie jest

[542] Tamże.
[543] Tamże.
[544] Stacjonowanie wojsk rosyjskich na Białorusi, co nastąpiło w wyniku kryzysu reżimu Łukaszenki w związku z zakwestionowaniem wyborów przez Zachód, oznaczało de facto utratę nie zależności przez Mińsk. W sytuacji Polski, a także każdego innego kraju, optymalna obrona kraju także przeciw zagrożeniom hybrydowym, powinna być skonstruowana przede wszystkim na siłach własnych. Każde stacjonowanie wojsk na terytorium danego kraju, nawet w ramach doraźnego wsparcia sojuszniczego – w celu obrony przed silniejszym przeciwnikiem – może zostać wykorzystane do uzyskania określonego poziomu kontroli nad krajem stacjonowania.

w stanie się obronić, co rozpoczęło pewien proces zmian strategii państw ościennych i w efekcie zachęciło do realizacji planów rozbiorów. Elity na Kremlu doszły do (słusznego z ich punktu wodzenia) wniosku, że po co chronić państwo, które nie chce się samo chronić tylko wynajmuje zewnętrze siły. Zajęto 2/3 terytorium Polski i przekształcono nasze zdolności do obrony imperiów rozbiorowych – w tym rosyjskiego. Sojusz może być uzupełnieniem, ale potrzebna jest w pierwszym rzędzie własna gotowość do obrony[545].

R. Jakubczak postuluje zorganizowanie obrony powszechnej – na wzór szwajcarski – ze znacznie bardziej licznymi wojskami niż obecny system obrony terytorialnej w Polsce. Wojska operacyjne, które ma Polska są w stanie bronić terenu państwa tylko w niewielkiej części. Natomiast agresor może zawsze skutecznie zaskoczyć dany kraj, omijając wojska operacyjne. Skuteczna obrona narodowa musi polegać na obronie powszechnej / terytorialnej, która zagospodarowuje wszystkie możliwości obronne celem wypełnienia zadań niedostępnych dla wojsk operacyjnych (których zawsze jest za mało). Ważne, aby panować nad przestrzenią terytorialną państwa, co jest bardzo ważne[546]. Obrona terytorialna daje gwarancję panowania kinetycznego nad przestrzenią. W przypadku obecnej sytuacji w Polsce należy uznać, jak przekonuje R. Jakubczak, że około 50 tys. kontyngent lekkiej piechoty (docelowe siły Wojsk Obrony Terytorialnej) nie może zapanować nad obecnym terytorium Polski. Kontyngent ten można określić mianem „kieszonkowych" wojsk obrony terytorialnej. Natomiast, właściwe siły obrony terytorialnej powinny być tworzone przez nawet ponad milion (przeszkolonych i uzbrojonych) osób zdolnych do operowania w ciągu 2-3h od zagrożenia. W obecnej Polsce nie ma zdolności panowania nad przestrzenią i nikt generalnie, w ocenie R. Jakubczaka – niestety się tym nie zajmuje. Kluczowe jest, aby przywódcy państwa potrafili wykorzystać zgodność interesu obronnego obywateli z interesem obronnym państwa. W Polsce tego nie ma. Kolejni rządzący starają się zapewnić skuteczną obronę kraju bez aktywnego udziału ludności, co musi być skazane na porażkę[547].

[545] Tamże.

[546] Zapomnieli o tym m.in. Niemcy w czasie próby agresji na Rosję w czasie II wojny światowej i ponieśli porażkę.

[547] Obrona w czasach piastowskich była skuteczna, ponieważ używano jej elastycznie (nie wszystkich na raz). W okresie wczesnopiastowskim istniała drużyna książęca ok. 3000 drużynników. Ale w grodzie było 2-3 drużynników, jako kadra dowódcza. W przypadku zagrożenia na danym terenie (grodzie), wszyscy mężczyźni otrzymywali włócznię, tarczę i topór i stawali się tzw. tarczownikami, którymi kierowali drużynnicy. Tarczownicy chętnie i z determinacją szli do walki, ponieważ nie bronili króla, ale swoich domostw (przysłowiowej – własnej zagrody). R. Jakubczak, *Obronę trzeba budować od fundamentów…*

Wojska Obrony Terytorialnej w ich zasadniczym charakterze, jak zauważył R. Jakubczak, powinny w Polsce wynosić minimum 700 tys. osób zdolnych do walki w pierwszych godzinach oraz posiadać w rezerwie co najmniej kolejne 700 tys. przeszkolonych wojskowo ludzi. Wojska te „są zawsze pochodną systemu obrony terytorialnej, którego w Polsce nie ma, a obecne wojska budowane pod tą nazwą mają wybitnie charakter wojsk wewnętrznych. (…) System obrony terytorialnej i tym samym jego wojska, tworzy się na zasadzie powszechnej służby wojskowej (wyjątkowo krótkiego przeszkolenia wojskowego i dopasowanego do możliwości odbywania tej służby przez obywateli w sposób elastyczny), a nie ochotniczego (w dodatku „sztywnego" – mało wygodnego dla żołnierzy-obywateli) zaciągu na służbę półzawodową/kontraktową, gdzie zdecydowana większość obecnych żołnierzy obrony terytorialnej widzi w takiej służbie drogę do kariery w wojskach operacyjnych, a nie długotrwałej „służbie obywatelskiej" w formacjach obrony terytorialnej[548]." Sprawdzonych rozwiązań w zakresie obrony terytorialnej (systemu dowodzenia i funkcjonowania) dostarcza m.in. podejście zachodnioniemieckie z czasów Zimnej Wojny, kiedy to Niemcy dostrzegły potrzebę powszechnego zaangażowania ludności do obrony zamieszkiwanego przez nią terytorium.

Kluczowymi warunkami budowania odporności państwa w oparciu o obronę terytorialną – stanowiącą jednocześnie istotny komponent krajowych sił przeciwhybrydowych – R. Jakubczak uznał także powszechny dostęp społeczeństwa do broni i posiadanie broni w domu przez żołnierzy struktur obrony terytorialnej[549] oraz uczynienie samorządu zasadniczą strukturą obronną powszechnej obrony terytorialnej (wojska obrony terytorialnej mają współdziałać z – ale nie mogą podlegać – dowództwu wojsk operacyjnych)[550]. Ponadto, w szkoleniu w kwestiach powszechnej obrony terytorialnej

[548] R. Jakubczak, *Budujemy wojska wewnętrzne czy Obronę Terytorialną?,* Instytut Bezpieczeństwa i Rozwoju Międzynarodowego, 17.08.2018, https://instytutbirm.pl/budujemy-wojska-wewnetrzne-czy-obrone-terytorialna/ [dostęp: 6.03.2023].

[549] Podstawową strukturę militarną w powszechnej obronie terytorialnej musi stanowić „powiatowy batalion obrony terytorialnej funkcjonujący w podporzadkowaniu powiatowego dowództwa obrony terytorialnej. Brygada obrony terytorialnej może jedynie być strukturą szkoleniową i bazować na specjalistycznych obiektach szkolenia poligonowego, a nie koszarach i „wędrówkach" żołnierzy do niej z całego województwa. Jej specjalistyczne zasoby szkoleniowe mają przybywać do powiatów i tam szkolić żołnierzy obrony terytorialnej, a nie ci zmuszani są do niej „pielgrzymować". To jest kosztowne i mało wydajne szkoleniowo. Tamże.

[550] W celu doprowadzenia do sytuacji, w której powszechna obrona terytorialna mogłaby właściwie funkcjonować jako „równoważny wojskom operacyjnym komponent, konieczny jest system obrony terytorialnej, gdzie podstawowym i niezbędnym jego elementem są terytorialne organy dowodzenia (lokalne i

powinni uczestniczyć „wszyscy zajmujący się funkcjonowaniem administracyjnym państwa – od sołtysa (jak za Kazimierza Wielkiego) i nauczyciela po ministra oraz profesora wraz z jego studentami. A także wszyscy wybierani – zarówno samorządowcy, jak i inni ubiegający się o zaufanie publiczne oraz także kierownicza kadra przedsiębiorstw gospodarczych, które prowadzą działalność na terytorium RP[551].”

W obecnym kształcie systemu organizacji wojsk obrony terytorialnej ich zdolności obronne mogą zostać łatwo zneutralizowane przez hybrydowego przeciwnika. Kadra wojsk operacyjnych, jak dowodził R. Jakubczak, posiada „sprzęt bojowy, w tym broń osobistą i zespołową, w miejscu pełnienia służby – czyli w koszarach – tj. średnio w odległości 20-100 m od miejsca przebywania żołnierza, a w działaniach bojowych „przy sobie”. A ich gotowość bojowa liczy się przecież w tygodniach i miesiącach. Tymczasem żołnierze Wojsk Obrony Terytorialnej już od początku szkolenia są zatruci/„obsobaczeni” tym, że pomimo tego, iż mają w pierwszej kolejności (niemal natychmiastowo) podjąć walkę zbrojną w wypadku nawet niespodziewanego ataku/agresji, to ich broń osobista i zespołowa zdeponowana jest dziesiątki, a nawet setki kilometrów (nie „metrów”) od nich. W magazynach, które dywersyjnie (przez potencjalnego agresora) mogą być (i z pewnością w znacznym stopniu będą) zniszczone – nie mówiąc o samym sposobie dotarcia do niej w sytuacji rozwijającego się zagrożenia, np. hybrydowego[552].”

Wyzwanie w zakresie zapewnienia skutecznej obrony w warunkach państwa demokratycznego ukazał m.in. John Slessor, urodzony w 1897 r. dowódca Brytyjskich Sił Powietrznych, który stał na stanowisku, że „w krajach demokratycznych ubolewa się zwykle

regionalne oraz okręgowe i centralne dowództwa obrony terytorialnej). One, oprócz dowodzenia Wojskami Obrony Terytorialnej w „powiatowym”/stałym rejonie odpowiedzialności, stanowią niezbędny łącznik funkcjonalny (o strategicznym znaczeniu dla funkcjonowania obronności państwa) między tymi Wojskami a administracją powiatową (gminną, regionalną, okręgową) oraz organizacjami proobronnymi, towarzystwami kurkowymi, leśnikami, strażami, myśliwymi i całą masą struktur włączanych do kształtowania społeczeństwa na rzecz skutecznej obrony narodowej oraz ją tworzących w swoich kompetencjach”. Tamże.

[551] Tamże.

[552] R. Jakubczak odniósł tę kwestię do zidentyfikowanych przez siebie mankamentów obrony narodowej stwierdzając co następuje. „Czy to nie kuriozum zakrawające na dywersję strategiczną planowaną przez polskich sztabowców, na bazie prawa niesprzyjającego skutecznej obronie narodowej. Aż się prosi o nazwiska autorów takich „cennych” rozwiązań „strategicznych”. Tworzymy zastępy żołnierzy o „gotowości godzinowej bez broni”. Przecież tego absurdu doświadczyliśmy podczas rozpoczynania Powstania Warszawskiego, kiedy kilku potencjalnych powstańców przyporządkowanych było do jednego egzemplarza broni lub jej posiadacz miał kilaka pocisków do niej albo jedynie 2-3 granaty. Czy my czasem nie jesteśmy mistrzami walki zbrojnej bez broni, która jest przecież jej atrybutem? Czy my właściwie rozumiemy strategię w kontekście sztuki wojennej i jej znaczenie dla istnienia państwa? A może bawimy się w państwo i jego atrybuty, gdzie właściwe siły zbrojne są jednym z najważniejszych?” Tamże.

nad wydatkami na zbrojenia, gdyż kolidują one z budżetem świadczeń społecznych. Istnieje tendencja do zapominania, że najważniejszym świadczeniem społecznym rządu wobec społeczeństwa jest zachowanie mu życia i wolności[553].” R. Jakubczak ocenił, że “podejście do budowy skutecznej obrony państwa z gremialnym angażowaniem społeczeństwa w ramach struktur powszechnej Obrony Terytorialnej na rzecz skutecznej obrony narodowej jest widocznym miernikiem intencji przywództwa państwa, co do rzeczywistej chęci posiadania państwa niepodległego, które chce wykorzystać właściwe środki obrony państwa na rzecz własnej niepodległości[554].”

Jeśli Polska ma trwać jako naród zwarty, a jej przywódcy mają kontynuować zapoczątkowany na tych ziemiach ponad 1000 lat temu wysiłek budowania niezależnej, suwerennej państwowości, to – w ocenie R. Jakubczaka – powinno się wzmocnić obronę terytorialną, bo ona jest fundamentem skutecznej strategii obronnej. A potencjał do zbudowania skutecznej obrony istnieje. Jak wynika z badań portalu Defence24.pl, Polacy, na tle innych narodów europejskich, wykazują wysoką zdolność do obrony swojego kraju[555].

Tradycja obrony terytorialnej w Polsce sięga pospolitego ruszenia w czasach I Rzeczpospolitej. Przykłady licznych konfliktów zbrojnych a także działań zwiększających bezpieczeństwo poszczególnych państw ukazują istotne znaczenie praktyczne obrony terytorialnej. Obrona terytorialna, jak zauważył M. Jakubowski, „w dużej mierze bazuje na znajomości żołnierzy miejsca swoich lokalizacji czyli swojego zamieszkania – słusznie, więc też jest określana czasem rodzajem armii obywatelskiej, czy gwardii narodowej. (…) Pięciomilionowa Finlandia ma siły zbrojne składające się z 60 tys. żołnierzy zawodowych i 230 tys. ochotników wojsk obrony terytorialnej (stosunek 1 do 4). W podobny sposób funkcjonują armie Szwajcarii, Niemiec, Izraela, Norwegii. Najbardziej znaną na świecie armię ochotniczą mają Stany Zjednoczone – Gwardię Narodową. W czasie pokoju służy w niej ok. 360 tys. osób. (…)[556].”

Polska skorzystałaby ponadto na zastosowaniu niektórych rozwiązań szwedzkich. Koncepcja systemu obronnego Szwecji zakładała pierwotnie funkcjonowanie w czasie

[553] Tamże.
[554] Tamże.
[555] R. Jakubczak, *Obronę trzeba budować od fundamentów…*
[556] M. Jakubowski, *Gwardia Narodowa – Natychmiast Cz. II,* Polityka Polska. Wolny narodów – w silnym państwie, nr 2(10) luty 2016 r., s. 79.

pokoju i wojny rozbudowanej liczebnie „Gwardii Krajowej" (Hemvarnet) obejmującej 42 tys. żołnierzy skupionych w 70 batalionach 300 kompaniach (tj. jednej kompanii na gminę). Polska mogłaby skorzystać z doświadczeń szwedzkich w zakresie wkomponowania patriotycznych organizacji proobronnych w system obrony terytorialnej oraz objęcia żołnierzy obrony terytorialnej „specjalnie zbudowanym dla nich systemem świadczeń: m.in. diety, wynagrodzenia i dodatki funkcyjne, premie roczne, świadczenia dodatkowe, w tym objęcie żołnierzy przepisami o państwowych odszkodowaniach[557]." Część z tych rozwiązań jest wdrażana w ostatnich latach w Polsce jednak wyzwaniem nadal pozostaje nadanie wojskom obrony terytorialnej właściwego im charakteru (wyraźne rozdzielnie od wojsk operacyjnych) oraz zagwarantowanie społecznego prestiżu przyciągającego rekrutów.

W wyniku przeprowadzonych badań stwierdzić należy, że w przeszłości, Polska wielokrotnie stawała wobec zagrożeń hybrydowych. Były one tym silniejsze, że pochodziły od kilku potężnych państw w regionie które często koordynowały ataki wymierzone w Polskę, co ostatecznie doprowadziło do jej rozbiorów i utraty niepodległości na 123 lata.

Polska była najsilniejsza za czasów zdecydowanej przewagi władzy scentralizowanej mającej oparcie w religii katolickiej, a okres osłabiania się siły państwa został zapoczątkowany wraz z rosnącymi przywilejami szlachty, co odbywało się kosztem prerogatyw królewskich. Władza monarchy została ograniczona w myśl zasady „król panuje, ale nie rządzi". Do tego procesu przyczyniły się także porażki Polski w wojnach obronnych (np. potop szwedzki), co było przyczyną zniszczenia majątków elity kraju. Wraz z postępującą pauperyzacją środowisk szlacheckich, które były odpowiedzialne za obronę kraju (pospolite ruszenie), wzrosła wywiadowcza penetracja tych środowisk ze strony obcych służb specjalnych. Rozwiązania blokujące prace nad usprawnieniem I Rzeczpospolitej takie jak liberum veto, przy pozostawaniu przez wielu przedstawicieli magnaterii i szlachty (decydentów-delegatów na Sejm) na usługach obcych mocarstw, były źródłem rozkładu państwa. Rezultatem słabości I Rzeczpospolitej był wzrost potęgi sąsiadów, którzy umiejętnie i – niejednokrotnie w porozumieniu ze sobą – ingerowali w wewnętrzne sprawy polskie przyczyniając się do stopniowej dezintegracji kraju. Efektem końcowym były rozbiory Polski dokonane przez Imperium Rosyjskie, Królestwo Prus i Austrię.

[557] Tamże, s. 80.

Jedną z ostatnich i znaczących prób obrony przed zagrożeniami hybrydowymi ze strony mocarstw ościennych była Konstytucja 3. maja, która w jednym z głównych punktów zakładała przywrócenie i ugruntowanie w Polsce monarchii dziedzicznej z silną władzą centralną. Taka formuła zarzadzania krajem, także w obszarze bezpieczeństwa narodowego, była najbardziej skuteczna. Dzięki tej formie rządów, królom polskim udało się zjednoczyć poszczególne ziemie oraz położyć podwaliny pod mocarstwowość państwa, która objawiła się w okresie świetności Rzeczpospolitej Obojga Narodów. Polska była w tamtym czasie jedną z potęg regionalnych w Europie, a – z uwagi na brak zaawansowanych w rozwoju cywilizacji na innych kontynentach – także na świecie. Państwa sąsiednie, które wszystkie, bez wyjątku, posiadały silnie scentralizowany, autokratyczny system rządów monarchicznych, doprowadziły do unicestwienia I Rzeczpospolitej, w której usilnie popierały wpływy określonych stronnictw skorumpowanej przez siebie magnaterii oraz szlachty. Ponadto, Ustawa Rządowa uchwalona 3 maja 1791 r. regulująca ustrój prawny Rzeczypospolitej Obojga Narodów miała na celu wzmocnienie państwa poprzez odebranie decyzyjności szlachcie nieposiadającej ziemi (tzw. gołocie). Formalnie zniesiono liberum veto, które często było wykorzystywane do obstrukcji prac usprawniających państwo. Zjednoczeniu narodu wokół silnej państwowości miało ponadto sprzyjać częściowe zrównanie praw mieszczan i szlachty oraz zabezpieczenie podstawowych interesów chłopów (redukcja pańszczyzny).

Konstytucja 3. Maja obowiązywała niewiele ponad rok, zanim została zniesiona przez armię Rosji współdziałającą z Polakami-zdrajcami. Zrealizowało się to w wyniku konfederacji targowickiej – spisku magnackiego zawiązanego w kwietniu 1792 r. w Petersburgu, w którym główną rolę odgrywała cesarzowa Rosji Katarzyna II. Działania te były wymierzone w reformy Sejmu Czteroletniego i Konstytucji 3 maja. Polska w 1918 r. odrodziła się, jednak nastąpiło to nie w najbardziej skutecznej formie rządów, którą postulowała Konstytucja 3. maja – monarchii dziedzicznej. Wprowadzono ustrój demokratyczny, zbliżony do demokracji szlacheckiej, która była jedną z przyczyn wcześniejszego upadku państwa zakończonego rozbiorami.

Jak wykazały wyniki badań, podobnego typu działania hybrydowe jak przed rozbiorami Polski – w zmodernizowanej formie – Rosja stosowała także w stosunku do Ukrainy osłabiając ten kraj na długo przed dokonaniem na niego zbrojnej inwazji w 2014 r.

Poprzez powstrzymywanie reform, Moskwa dążyła do wytworzenia i zachowania na Ukrainie korupcyjnego sytemu gospodarczego i politycznego (oligarchowie), za pomocą którego była w stanie wpływać na politykę władz w Kijowie.

Jak pokazały badania, w późniejszym okresie koncepcje mocarstwowości, jako instrumentu gwarantującego bezpieczeństwo Polski, były wysuwane przez różnych przedstawicieli elity inteligenckiej kraju. Warto odnotować w tym miejscu rekomendacje premiera rządu Rzeczypospolitej Polskiej na uchodźstwie w latach 1954–1955 Stanisława Cata-Mackiewicza, który opowiadał się za budowaniem potęgi Polski na monarchicznym, a nie republikańskim systemie rządów. W jego ocenie, Polska niepodległa po 1918 r. powinna powstać, jako kontynuacja państwowości z czasów świetności Rzeczpospolitej. Jednocześnie, polityk ten był w opozycji do narodowej demokracji, jeśli chodzi o stosunek do mniejszości narodowych. Uważał, że Polska ma szansę zachować bezpieczeństwo tylko jako wielokulturowe imperium, co było warunkiem koniecznym do panowania nad znaczącym terytorium, znacznie większym niż to które powstało w wyniku postanowień kończących I wojnę światową. Tylko w takiej postaci, w jego ocenie, możliwe było zapewnienie bezpieczeństwa w sytuacji położenia Polski pomiędzy potęgami w postaci państwa niemieckiego i Rosji.

Konflikt hybrydowy, jak wykazały wyniki badań, stanowi wyzwanie dla każdego państwa o statusie mocarstwa, ponieważ nie istnieją środki pozwalające na całkowitą ochronę danego terytorium przed wtargnięciem osób postronnych. Ponadto, realizacja ataku hybrydowego może mieć miejsce nawet bez fizycznego wtargnięcia na teren danego państwa – na przykład w formie rozprzestrzeniania w mediach zagranicznych dezinformacji o danym kraju lub tez przez cyberataki. Zagrożenia hybrydowe są jeszcze poważniejszym problemem dla średnich i małych krajów nie będących mocarstwami[558].

W świetle wyników przeprowadzonych badań należy stwierdzić, że – mimo iż część środowiska eksperckiego krajów zachodnich uważa, że nie można iść na kompromis z agresorem w sprawie fundamentalnych wartości, które wymagają ochrony po stronie

[558] A. Karolewski, M. Rejman-Karolewska, *Konflikt hybrydowy zagrożeniem dla bezpieczeństwa granic Rzeczpospolitej Polskiej* [w:] Przegląd Naukowo-Metodyczny Edukacja Dla Bezpieczeństwa, Rok XI Numer 3/2018 (40), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2018, http://www.przeglad.wsb.net.pl/uploads/1/0/3/7/10371016/pnm_3_2018_ca%C5%81o%C5%9A%C4%86_-_druk_ostateczny.pdf [dostęp: 29.11.2022], s. 94.

państwa broniącego się, atak hybrydowy należy zawsze postrzegać w charakterze działania natury wojennej. W interesie państwa powinno być posiadanie silnych zdolności obronnych, ale unikanie konfrontacji hybrydowej czy militarnej, a jeśli to jest niemożliwe – z uwagi na zagrożenie żywotnych, strategicznych interesów i bezpieczeństwa – zawsze wejście do wojny na jej późniejszym (najlepiej końcowym) etapie, nie na początkowym. Analiza faktów historycznych, takich jak wydarzenia podczas II wojny światowej wskazuje, że największe korzyści przyniosło zastosowanie opisanego podejścia. Wszelkie sojusze, które dany kraj posiada, nie powinny zwalniać rządzących z priorytetu, jakim jest dbanie o bezpieczeństwo własnego kraju. Kwestia ta jest także zauważana przez polityków NATO, którzy wskazują na przykład, że ok. 6 miesięczny okres oczekiwania na wsparcie sojusznicze wymaga znacznego usprawnienia (szybsza pomoc wojskowa napadniętemu).

Organizacja systemu obrony Polski powinna mieć charakter powszechny, jak zauważył gen. dyw. w st. spocz. Leon Komornicki. Dodał on, że należy w większym stopniu patrzeć na odpowiednie przygotowania kraju oraz budowanie odporności państwa na wypadek kryzysu. Były zastępca Szefa Sztabu Generalnego zaznaczył tę potrzebę w odniesieniu do sfery militarnej, ale także cywilnej. Strategicznym celem bezpieczeństwa państwa jest to, aby nie doszło do konfliktu zbrojnego na jego terytorium. Generał Komornicki, zauważył, że Polska posiada niezbędny zasób, który umożliwia stworzenie skutecznej obrony narodowej. Całe terytorium państwa, w ocenie generała, powinno zostać objęte obroną, co wymaga efektywnej realizacji przygotowań ogólnopaństwowych.

Generał odniósł się również do zaprezentowanych w 2020 r. przez Defence24 i IBRiS wyników badania "Bezpieczeństwo 2020", zgodnie z którym 49 proc. polskich respondentów stwierdziła, że obrona powinna być zadaniem wszystkich mężczyzn w wieku 18-60 lat po uprzednim przeszkoleniu. Najmniej zwolenników takiego rozwiązania było w Niemczech (18 proc.), a najwięcej w Estonii (56 proc.). Oprócz Polski, badanie przeprowadzono również w Niemczech, w Czechach, na Słowacji, na Litwie, na Łotwie i w Estonii. Wyniki dotyczące polskich respondentów, jak zaznaczył L. Komorniki, wskazywały na wysoki poziom zrozumienia problematyki bezpieczeństwa narodowego w społeczeństwie oraz na determinację znacznej części obywateli do obronny swojego kraju.

W świetle wyników przeprowadzonych badań należy stwierdzić, że istotna jest szybkość działania i adaptacji kluczowych dla bezpieczeństwa państwa dokumentów, która powinna być wyrazem świadomości decydentów oraz społeczeństwa o nowych uwarunkowaniach bezpieczeństwa. SBN z 2014 r. została zaktualizowana dopiero w 2020 r. mimo, że zaszły w międzyczasie poważne zmiany uwarunkowań otoczenia Polski. Ważną zmianą było pojawienie się w strategii dwóch istotnych zapisów, które mówią o tym, że obrona państwa i – szerzej – bezpieczeństwo mają mieć charakter powszechny. Wszystkie zasoby kraju, materialne i niematerialne, jego wielowymiarowe bogactwo (zasoby, infrastruktura, potencjał ludzki, terytorium) trzeba przygotować do zadań obronnych. Potencjał ten musi być prawnie ulokowany w odpowiednich strukturach, aby był właściwie wykorzystany. Powinno to zostać zrealizowane bez względu na sojusze i być wprowadzane w życie tak jakby Polska była pozbawiona wsparcia sojuszniczego. Sojusze, zdaniem L. Komornickiego, należy bowiem postrzegać w kategoriach wartości oddanej i ich obecność nie może zwalniać, a tym bardziej usprawiedliwiać zaniechań w przygotowaniach obronnych kraju[559].

W kontekście przeciwdziałania zagrożeniom, także hybrydowym, Polska powinna podjąć działania mające na celu korektę podejścia do swojego bezpieczeństwa i obronności. W kontekście przyjętej w 2020 r. Strategii Bezpieczeństwa Narodowego, w ocenie L. Komornickiego, diametralnie przedefiniowana powinna zostać strategia obronny militarnej. Władze Polski, jak stwierdził, muszą wyzbyć się kompleksów, przewartościować swoje podejście w omawianym zakresie, oraz przekonać do niego swoich sojuszników. Głównym, nowym założeniem, w ocenie generała w stanie spoczynku, powinno być niedopuszczenie do sytuacji, aby ewentualna wojna kinetyczna w obronie Polski toczyła się, rozstrzygała się na jej terytorium. Trzeba uprzedzić przeciwnika tworząc taki system powszechnej i wojskowej obrony państwa, który by pozwalał uzyskać siłom zbrojnym poprzez określoną technikę, uzbrojenie – rażenia przeciwnika na jego terytorium. Kluczowe jest tu pozbawienie agresora zdolności ofensywnych tak aby nie był on w stanie wtargnąć na terytorium Polski. Jest to kwestia o fundamentalnym znaczeniu, a poświęca się jej bardzo mało uwagi w obecnej debacie nad priorytetami bezpieczeństwa narodowego Polski. Chodzi

[559] L. Komornicki: *Obrona państwa powinna mieć charakter powszechny*, wywiad dla Defence24.pl 28.08.2020, https://defence24.pl/sily-zbrojne/gen-komornicki-obrona-panstwa-powinna-miec-charakter-powszechny [dostęp:11.03.2022].

o niedopuszczenie do wyniszczającej państwo i jego obywateli wojny lądowej, której doświadczyła Ukraina w 2022 r. Oprócz nieuniknionych strat ludzkich, taka sytuacja powoduje zawsze cofnięcie danego kraju o dekady w rozwoju gospodarczym, politycznym i społecznym przez utratę dorobku wielu pokoleń. Polska doświadczyła tego chociażby podczas 2 wojny światowej. Cześć działań w tym słusznym kierunku jest już widoczna, o czym świadczą – zdaniem L. Komornickiego – zdolności bojowe pozyskiwanego przez Polskę sprzętu. Chodzi tu o samoloty F16 i F35 oraz o wyrzutnie HIMARS. Samoloty F16 uzyskały, jak wynika z informacji generała, rakiety średniego (370 km) i dalekiego (1000 km) zasięgu, co oznacza parametry umożliwiające sięgania ofensywnego w głębię strategiczną Rosji. Tu bardzo ważny jest także element odstraszania polegający na budowaniu tego typu zdolności ofensywnych Wojska Polskiego[560]. Oddzielną kategorią jest konieczność wzmocnienia obrony powietrznej nad Polską, co od wielu lat pozostaje istotnym wyzwaniem.

W świetle wyników przeprowadzonych badań należy stwierdzić, że działania należące do metod hybrydowych mogą być stosowane także jako plan obrony. Tajwańskie założenia wojny asymetrycznej, określane jako „strategia jeżozwierza"; ang. *porcupine strategy*), są tego dobrym przykładem. Samo pojęcie tej strategii zostało zaproponowane w 2008 r. przez amerykańskiego profesora US Naval War College, Williama S. Murraya. Jej istotą jest wzmacnianie obronności słabszego państwa, aby atak na niego oznaczał ogromne straty dla każdego potencjalnego najeźdźcy. W tym ujęciu, zakała się, że Tajwan może zostać zaatakowany, ale nie da się go pokonać bez niedopuszczalnie wysokich kosztów takiej agresji. Władze w Tajpej, kierując się tą strategią wyposażają siły zbrojne w duże ilości przeciwokrętowych pocisków kierowanych, dronów, min, przenośnych systemów rakietowych Javelin oraz Stinger, moździerzy, a także prowadzą znaczącą rozbudowę zdolności odparcia inwazji drogą morską – umocniona linia obrony wybrzeża.

Jak wykazały wyniki badań, kraje znajdujące się w niestabilnym międzynarodowym otoczeniu bezpieczeństwa powinny przedsięwziąć adekwatne działania w celu poprawy swojego potencjału odstraszania. Dobrym przykładem takich działań posłużył Tajwan. Biorąc pod uwagę grożące wojną napięcia z Chinami, prezydent Tajwanu ogłosiła w grudniu

[560] L Komornicki, *Rosja nie skończy wojny! Zmuszą Putina do pokoju?* Gen., wywiad w programie Express Biedrzyckiej, Super Express 8.11.2022, https://www.youtube.com/watch?v=NJq19RA2ogg [dostęp: 14.11.2022].

2022 r. plan przedłużenia obligatoryjnej służby wojskowej z czterech miesięcy do roku. Nastąpi to od 2024 r. Rząd w Tajpej postanowił ponadto o ponad czterokrotnym zwiększeniu żołdu poborowych oraz zreformowaniu programu szkolenia żołnierzy z poboru, którzy urodzi lisie po styczniu 2005 r.

Opracowując i wdrażając plany usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym, Polska musi brać pod uwagę szereg czynników uprawdopodabniających sukces danej operacji, w tym zwłaszcza skuteczność odstraszania nuklearnego (w kontekście zablokowania przyjścia z pomocą określonemu państwu), układ strategiczny sił w regionie i otoczenie międzynarodowe, ofensywne i defensywne zdolności propagandowe / dezinformacyjne (swoje i wroga / koalicji), konieczność zapewnienia efektywnej logistyki przy działaniach daleko od własnego terytorium. W tym kontekście, w przypadku ataku hybrydowego, bądź konwencjonalnego na terytorium Polski pozostające granicą zewnętrzną NATO, skuteczne wsparcie sojuszników mogłoby pojawić się z dużym opóźnieniem (w ocenie niektórych ekspertów nawet dopiero pół roku po rozpoczęciu agresji). Skalę wyzwań i zagrożeń tego typu pokazuje sztucznie wywołany kryzys graniczny między Polską i wspieraną przez Rosję Białorusią w 2021 r. oraz międzynarodowe osamotnienie naszego kraju (ataki zachodnich mediów na politykę Warszawy względem imigrantów).

Dążenie do rozbudowy polskich sil zbrojnych oraz trwałego zwiększenia sojuszniczej obecności wojskowej na wschodniej flance powinno zostać zrealizowane wiele lat przed wojną na Ukrainie w 2022 r. i było postulowane przez niektórych ekspertów z doświadczeniem pełnienia najwyższych stanowisk rządowych w Polsce w obszarze bezpieczeństwa narodowego.

Odstraszanie można także rozpatrywać w kategoriach spójnej, długoterminowej polityki bezpieczeństwa i obrony, która wynika ze stałych priorytetów władz (racja stanu). Warto zauważyć, że najpotężniejsze państwa na świecie, w sensie gospodarczym, militarnym i politycznym, cechuje wysoka spójność, stabilność i wieloletnia strategia kształtowania interesów narodowych. Przykładem są tu m.in. Niemcy, które były w stanie rozpocząć projekt Gazociągu Północnego przez socjaldemokratów Gerharda Schrödera i ukończyć go za rządów chrześcijańsko-demokratycznej CDU. Ponadto, zostało to dokonane w sytuacji silnego, publicznie wyrażanego sprzeciwu międzynarodowego w tym czołowych partnerów

gospodarczych i wojskowych z UE i NATO – np. Polski. Różnice nawet pomiędzy ugrupowaniami politycznymi deklarującymi publicznie skrajnie odmienne światopoglądy w najsilniejszych demokracjach (typu kraje G7) nie stoją, więc generalnie na przeszkodzie w realizacji długoterminowych interesów tych państw o znaczeniu strategicznym.

Cennych wskazówek dla usprawnienia krajowych zdolności przeciwdziałania zagrożeniom hybrydowym dostarcza analiza rozwiązań wskazywanych w kontekście polityki USA i ich sojuszników. Największym zagrożeniem bezpośrednim zarówno w optyce Polski, Waszyngtonu, jak i większości innych państw NATO jest agresywna polityka Rosji. Z tego powodu badania możliwości przeciwdziałania zagrożeniom hybrydowym skoncentrowano na bieżącym i potencjalnej ataku tego typu ze strony tego kraju. Natomiast, warto w tym miejscu zauważyć, że źródłem zagrożeń hybrydowych mogą być dla Polski potencjalnie także inne kraje. Rozwiniecie możliwości przeciwdziałania zagrożeniom hybrydowym bazując na przygotowaniu do odparcia agresji ze strony Kremla, przy zachowaniu roztropności decydentów – wzmocni też odporność Polski na podobne działania generowane w przyszłości także przez inne podmioty.

W celu skutecznego przeciwdziałania atakom hybrydowym ze strony Rosji, jak zauważa Mason Clark, Stany Zjednoczone i ich sojusznicy muszą zrozumieć istotę prowadzenia przez stronę rosyjską wojen hybrydowych (i konwencjonalnych) na warunkach Kremla, bo takie były i będą podejmowane przez to państwo w przyszłości.

Rosja wzmacnia nie tylko zdolności konwencjonalne, ale równolegle – także hybrydowe. Wśród zidentyfikowanych obszarów tych adaptacji M. Clark, wymienia:

a) centralizację wszystkich instytucji i centrów decyzyjnych (cywilnych, wojskowych, gospodarczych i środków masowego przekazu) w celu koordynacji działań rządu;

b) dostosowanie tradycyjnych wojskowych doktryn, aby umożliwić przeprowadzanie operacji hybrydowych, jako jednego z głównych zadań sił zbrojnych;

c) realizacja ogólnokrajowych kampanii informacyjnych, aby wzmocnić świadomość patriotyczną, którą Moskwa postrzega, jako niezbędny warunek wojen hybrydowych;

d) zwiększenie zdolności adaptacyjnych i mocy odziaływania rosyjskich kampanii informacyjnych w celu pomyślnego przeprowadzania działań hybrydowych w przyszłości;

e) poprawa zdolności konwencjonalnych ekspedycyjnych rosyjskiej armii (usprawnienie jej możliwości operowania za granicą w celu wsparcia operacji hybrydowych);

f) zwiększenie możliwości użycia przez Federację Rosyjską prywatnych firm wojskowych lub innych pośredników (*deniable proxy forces*);

g) podporządkowanie operacji kinetycznych operacjom informacyjnym, które według władz na Kremlu, mają być podstawą fundamentalnej zmiany w charakterze przyszłej wojny[561].

Jeśli chodzi o ten ostatni punkt, rosyjska inwazja na Ukrainie w 2022 r. pokazała, że działania hybrydowe są traktowane przez Federację Rosyjską, jako element wstępny, przygotowujący grunt pod ostateczne rozwiązanie sporu z danym krajem lub ich grupą zagrażającego – w percepcji Moskwy – jej bezpieczeństwu narodowemu. Za takie Rosja uznała zarówno możliwość obalenia przez tłumy demonstrantów reżimu prezydenta Assada w Syrii, jak i postępujące coraz szybciej od Pomarańczowej Rewolucji zbliżenie między Ukrainą, a zachodnimi strukturami bezpieczeństwa.

Użycie przez Rosję taktyk hybrydowych przeciwko Ukrainie, zwłaszcza od czasu aneksji Krymu w 2014 r., było w rzeczywistości wstępem do wojny na pełną skalę co pokazała rosyjska inwazja w 2022 r. Ataki hybrydowe, takie jak dezinformacja, cyberataki i przymus energetyczny (energy coercion) były stosowane także przeciwko państwom zachodnim przez Rosję i Białoruś, co nasiliło się od czasu kryzysu granicznego z Polską w 2021 r. Polska, wraz z innymi sojusznikami, powinna więc inicjować i wspierać korzystne dla swojego bezpieczeństwa projekty wzmacniające reakcję NATO na zagrożenia hybrydowe.

[561] M. Clark, *Russian Hybrid Warfare*, Military Learning and the Future of War, Institute for the Study of War – ISW September 2020, https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf [dostęp: 12.04.2022].

Przez miesiące poprzedzające inwazję Rosja inicjowała różnorodne działania informacyjne przeciwko Ukrainie (demonizowanie nacjonalizmu i rzekomych pronazistowskich nastrojów Ukraińców). Po rozpoczęciu wojny w 2022 r. Kreml oskarżał stronę ukraińską o blokowanie korytarzy humanitarnych i stosowanie „żywych tarcz" i przedstawiał swoją militarną agresję, jako misję „pokojową". Na wiosnę 2022 r. pojawiły się raporty o rzekomej broni biologicznej na Ukrainie, a także o rzekomo przygotowywanych przez Kijów atakach z użyciem „brudnych bomb". Zarzuty te wzmacniano środkami narzędzi dezinformacyjnych, które pozostają w dyspozycji Moskwy: rosyjskimi ambasadami oraz aparatem państwowym, kontrolowanymi przez rząd mediami, rosyjskimi „korespondentami wojennymi" i aktywami w mediach społecznościowych (tzw. influencerzy).

Analizując tego typu działania hybrydowe strona polska powinna zachować czujność względem narracji Rosji i stosować pogłębione sprawdzanie źródeł. Jednym z kroków może być także wypracowanie metod bardziej proaktywnego przeciwdziałania kampaniom dezinformacyjnym, zwłaszcza w obszarach o podwyższonej wrażliwości (historyczne konflikty między Polakami i mieszkańcami Ukrainy – zwłaszcza w czasie II Wojny Światowej).

5.2. Usprawnienie systemów reagowania na zagrożenia hybrydowe oraz intensyfikacja współpracy międzynarodowej

Oprócz wzmocnienia zdolności odstraszania potencjalnych agresorów, ważnymi obszarami wymagającymi udoskonalenia przeciwdziałania zagrożeniom hybrydowym jest udoskonalenie systemów reagowania na zagrożenia hybrydowe, wzmocnienie zdolności do obrony przed dezinformacją oraz kooperacja międzynarodowa z sojusznikami (wymiana informacji). W kontekście przeciwdziałania zagrożeniom hybrydowym, odstraszanie, jak dowodził M. Rühle, szef sekcji NATO do spraw bezpieczeństwa energetycznego „musi także obejmować aspekty cywilne. Na Ukrainie Rosja zastosowała podręcznikowy przykład wojny hybrydowej: szybka koncentracja regularnych sił zbrojnych przy granicy z Ukrainą, wzrost ceny gazu oraz masywna kampania propagandowa, której celem było zaciemnienie obrazu wydarzeń na tym terenie. (…) Odstraszanie w odniesieniu do wojny hybrydowej wymaga innych środków takich, jak zwiększenie wytrzymałości sieci cybernetycznych, dywersyfikacja dostaw energii oraz strategiczna komunikacja, która mogłaby szybko korygować fałszywe informacje rozpowszechniane przez przeciwnika. Zamiast karać

agresora odwetem zbrojnym, „odstraszanie przez wytrzymałość" stara się odwieść go od zamiarów poprzez wykazanie nieskuteczności jego podejścia[562]." W wyniku przeprowadzonych badań stwierdzono, że wzmacnianie odporności, powinno stanowić jednak element uzupełniający, a nie – jak to ma miejsce obecnie w przypadku wielu krajów w tym Polski – podstawowy środek przeciwdziałania zagrożeniom hybrydowym i innym sytuacjom kryzysowym, z wojną włącznie. Podstawową powinnością władz państwa jest bowiem zagwarantowanie adekwatnych do zagrożeń ofensywnych i defensywnych krajowych zdolności wojskowych wspartych sojuszami. To one są podstawą odstraszania, a w przypadku konieczności – na przykład próby przetestowania przez agresora determinacji obrońcy – powinny zostać użyte.

Jeśli chodzi o przeciwdziałanie zagrożeniom hybrydowym, państwo chcące skutecznie przeciwdziałać im powinno zabezpieczyć możliwości przejęcia lub uzyskania choćby nawet częściowej kontroli nad firmami działającymi na rynku medialnym, włączając w to źródła internetowe (głownie media społecznościowe). Można tu mówić zarówno o próbach przejęcia danego podmiotu przez kapitał zagraniczny, jak i krajowy (związany z agresorem hybrydowym). W obu przypadkach mogą to być powiązania narażające dany kraj na niebezpieczeństwo nierzetelnego (korzystnego dla agresora) przedstawiania wydarzeń, a w efekcie – wpływu na politykę atakowanego kraju i postaw jego polityków. Wpływ ten może być widoczny także w innych sferach funkcjonowania państwa i społeczeństwa takich jak zaopatrzenie w żywność, energię, rynek medyczny i ochrony zdrowia.

Przeciwdziałanie zagrożeniom hybrydowym wymaga przewidzenia możliwego ataku i dostosowanie obrony do nowych uwarunkowań, które może on wywołać. Często wymaga to zupełnie odmiennego, nieszablonowego spojrzenia (ang. out of the box) na możliwe scenariusze. Funkcjonowanie współczesnych państw, w tym – działanie ich sił zbrojnych, opiera się na narzędziach cyfrowych i sieciach internetowych. W przypadku ich zniszczenia lub uszkodzenia, drastycznej zmianie ulegają warunki i zdolności obrony danego kraju. Do potencjalnych sytuacji tego typu można zaliczyć m.in. atak na infrastrukturę satelitarną umożliwiającą lokalizację GPS, zakłócenie komunikacji teleinformatycznej i komórkową na dużą skalę czy uszkodzenie elektroniki w sprzęcie wojskowym przeciwnika za pomocą

[562] M. Rühle, op. cit.

nowych borni (wykorzystujących np. sztucznie wygenerowany, odpowiednio silny impuls elektromagnetyczny). Przykład wojny na Ukrainie w 2022 r. pokazał jednak, że sama wiedza o zagrożeniu nie jest w stanie stanowić wystarczającej obrony przed nim.

W kontekście przeciwdziałania zagrożeniom hybrydowym, ze względu na ich charakter konieczne jest podejście obejmujące całe społeczeństwo i wszystkie instytucje rządowe (ang. *whole-of-society, whole-of-government approaches*). Kluczowa jest w tym zakresie kompetencja krajowa państw członkowskich. UE prowadzi działania uzupełniające wysiłki państw członkowskich inicjatywami politycznymi, najlepszymi praktykami oraz ułatwianiem koordynacji między państwami. UE stara się wypracowywać wspólną odpowiedź na podobne lub takie same wyzwania w zakresie bezpieczeństwa dotykające wiele krajów członkowskich. Ustalanie norm na forach międzynarodowych ma istotne znaczenie dla promowania porządku światowego opartego na zasadach. Podkreślenia wymaga także duże znaczenie podobnie myślących partnerów UE na arenie międzynarodowej (kraje partnerskie)[563].

Ponadto, Polska w coraz większym stopniu buduje swoje bezpieczeństwo energetyczne na dostawach surowców drogą morską, dlatego wzmocnienia wymagać będzie także zdolność do wykrywania zagrożeń i ochrony infrastruktury krytycznej od strony morza. Może to oznaczać nasilenie się działań hybrydowych poniżej progu otwartej wojny i rozszerzenie ich na przykład o ataki na infrastrukturę krytyczną zamachy terrorystyczne (włącznie z użyciem broni masowego rażenia na dużą skalę, ładunkami taktycznymi i/lub przeciwko pojedynczym celom ludzkim)[564].

W wyniku przeprowadzonych badań stwierdzono, że wyzwaniem dla UE jest to, że nie wszystkie kraje zgadzają się z identyfikacją określonego kraju, jako agresora. Podejście takie utrudnia działania w zakresie przeciwdziałania zagrożeniom hybrydowym. Jednak wynika to z istoty funkcjonowania UE zakładającej znaczący zakres działań bazujących na konsensusie. Pokazała to wojna na Ukrainie i problem ze skoordynowaniem unijnych sankcji[565]. Brak porozumienia w szerszym gronie państw osłabiał w wielu przypadkach (ostatnio – w czasie wojny na Ukrainie w 2022 r. skuteczną reakcję w zakresie

[563] *Countering Hybrid Threats and enhancing resilience*…

[564] *Ataki cybernetyczne, zamachy terrorystyczne*, Polska Agencja Prasowa, 3.10.2022, https://www.pap.pl/aktualnosci/news%2C1441577%2Cataki-cybernetyczne-zamachy-terrorystyczne-putin-chce-calkowita-zmiane-w [dostęp: 11.10.2022].

[565] *Countering Hybrid Threats and enhancing resilience*…

przeciwdziałania zagrożeniom hybrydowym. Istnieje potrzeba usprawnienia zasad bezpieczeństwa dla systemów informatycznych różnych podmiotów instytucjonalnych UE podczas prowadzenia operacji i misji zagranicznych[566]. Mając na względzie konieczność przeciwdziałania zagrożeniom hybrydowym, korzystne dla UE byłoby zapewnienie stabilizacji w krajach ościennych wspierając procesy zabezpieczające przez wpływem hybrydowym (np. Rosji w krajach sąsiadujących z UE). Relacje UE z NATO w zakresie przeciwdziałania zagrożeniom hybrydowym są bardzo istotne. W wymiarze zewnętrznym odbywa się to w ramach dialogu Unia-NATO. UE bada doświadczenia instytucjonalne NATO starając się wdrożyć korzystne dla siebie rozwiązania. Instytucje Sojuszu Północnoatlantyckiego są bardziej zaawanasowane w zakresie wdrażania rozwiązań zwiększających bezpieczeństwo, także w obszarze hybrydowym. Kluczowa jest kwestia zaufania wewnątrz UE i NATO, aby skutecznie współpracować w zakresie odparcia zagrożeń hybrydowych, w tym transnarodowych ataków cybernetycznych. Musimy zbudować zaufanie w gronie krajów partnerskich. Były przypadki wspólnych, skoordynowanych działań UE, NATO oraz USA w zakresie odparcia cyberataków, ale na tym polu wile pozostaje do zrobienia. Kluczowe w tym zakresie jest uzyskanie zgody, co do zidentyfikowania agresora.

Wyzwania hybrydowe to zagrożenie horyzontalne i wymaga horyzontalnej odpowiedzi i dostosowana odpowiednich środków przeciwdziałania. Komicja Europejska oraz Europejska Służba Działań Zewnętrznych wspierają narodowe wysiłki państw członkowskich i ułatwiają koordynację. Ma to na celu wypracowanie holistycznego podejścia w coraz większej liczbie obszarów polityki, obejmujących świadomość sytuacyjną, budowanie odporności, reagowanie i współpracę międzynarodową. Działania w zakresie przeciwdziałania zagrożeniom hybrydowym takie jak zamrożenie aktywów czy zakaz podróżowania, choć nie są jeszcze w pełni skuteczne, pokazują czerwone linie, które UE wyznacza dla agresorów. To pokazuje unijną aktywność w kierunku proaktywnych działań w zakresie przeciwdziałania zagrożeniom hybrydowym. Uzupełnieniem jest przeciwdziałanie dezinformacji oraz przedstawianie wiarygodnych faktów w jej miejsce. Ograniczeniem UE i innych demokracji są instytucje oparte na gruncie prawa. Kwestią, którą

[566] Prace nad poprawą zdolności UE w zakresie cyberobrony na szczeblu UE prowadzi Sztab Wojskowy UE (EUMS) i Europejska Agencja Obrony. Od 2016 r. w celu zacieśnienia współpracy organizacje na szczeblu UE – w tym EDA, ENISA, Europejskie Centrum ds. Walki z Cyberprzestępczością Europolu (EC 3) i CERT UE – współpracują ze sobą w obszarze cyberbezpieczeństwa i obrony.

decydenci powinni mieć stale na uwadze jest zagwarantowanie, aby kraje UE mogły zachować swoje wartości i skutecznie walczyć z nowego typu wyzwaniami takimi jak zagrożenia hybrydowe[567].

W wyniku przeprowadzonych badań stwierdzono, że istotne znaczenie ma przeciwdziałanie zagrożeniom hybrydowym w kontekście kontroli nad szlakami logistycznymi oraz przepływami informacyjnymi. Mimo obecnie obserwowanego wzrostu znaczenia siły militarnej (rosyjska agresja na Ukrainie w 2022 r.), ciężar konfrontacji globalnej między mocarstwami przesuwa się ze sfery wojskowej coraz bardziej w stronę dążeń do dominacji technologicznej i gospodarczej. Zjawisko to dotyczy także otoczenia bezpieczeństwa krajów małych i średnich. Od ich poziomu zaawansowania technologicznego będzie zależała odporność a także zdolności odstraszające w zakresie obrony przed zagrożeniami hybrydowymi.

W kontekście usprawnienia metod przeciwdziałania zagrożeniom hybrydowym w Polsce przed zagrożeniami z kierunku wschodniego, M. Wojnowski, zauważył, że „rosyjskie rozumienie przyczyn, przebiegu oraz skutków konfliktów ma charakter geopolityczny, czyli przestrzenny. Oznacza to, że według Rosjan działania są prowadzone w przestrzeni geograficznej, ekonomicznej, informacyjno-cybernetycznej oraz informacyjno-psychologicznej danego państwa." W związku z tym, z punktu widzenia bezpieczeństwa Polski, jak dodaje, konieczne jest „stworzenie doktryny bezpieczeństwa informacyjnego RP, uwzględniającej rosyjską specyfikę działań. Stanowiłaby ona punkt odniesienia dla działalności legislacyjnej, precyzyjnie definiując zagrożenia i ich skutki. Państwo polskie nie dysponuje potencjałem materialnym, technologicznym i finansowym, aby przygotować symetryczną odpowiedź na rosyjskie formy oddziaływania informacyjnego. Pewną próbą udzielenia takiej odpowiedzi może być jednak prowadzenie szerokiej akcji informacyjnej i edukacyjnej w społeczeństwie oraz pogłębianie specjalistycznych studiów nad rosyjską myślą wojskową, strategią i historią rosyjskiej wojskowości, bez zamykania się tylko i wyłącznie w kręgu zachodniej sztuki wojennej[568]".

Ponadto, w wyniku przeprowadzonych badań stwierdzono, że istotne jest udoskonalanie mechanizmów reakcji na przypadki dezinformacji. Bardzo często przypisanie

[567] *Countering Hybrid Threats and enhancing resilience*…
[568] M. Wojnowski, *Mit „wojny hybrydowej"…*

winy konkretnym podmiotom państwowym lub prywatnym jest utrudnione, ale atrybucja polityczna jest możliwa. W takim przypadku ujawniana jest publicznie informacja o przesłankach wskazujących, że za konkretnym atakiem może stać dany kraj (na przykład Federacja Rosyjska lub Chiny). Pomocna w walce z dezinformacją będzie niewątpliwie wzmocniona komunikacja strategiczna, która powinna mieć za zadanie informowanie obywateli o ich zakresie odpowiedzialności oraz o zmianach w zakresie przeciwdziałania zagrożeniom hybrydowym w kontekście wprowadzania nowych regulacji prawnych. Aby skutecznie zmieniać podejście adaptując je do nowych wyzwań potrzeba skutecznej komunikacji ze społeczeństwem odnośnie prawodawstwa i zmienionego podejścia do określonych kwestii bezpieczeństwa. Jednostki do spraw komunikacji strategicznej mają na celu spowodować zmianę schematów zachowań w kierunku wzrostu odporności na zagrożenia hybrydowe (spójność społeczna, czujność i determinacja do ochrony wartości społeczności lokalnych). Komunikacja Strategiczna ma za zadanie również promowanie międzynarodowej współpracy i wartości politycznych korzystnych dla bezpieczeństwa danego kraju. Odpowiada też ona, w ocenie przedstawicieli Wielkiej Brytanii, na potrzeby informacyjne obywateli w zakresie wiedzy o kluczowych usługach związanych z szeroko pojętym bezpieczeństwem (na przykład szczepienia przeciwko groźnym chorobom zakaźnym takim jak COVID-19)[569].

Inicjatywy takie jak przeciwdziałanie dezinformacji w ramach serwisów informacyjnych Polskiej Agencji Prasowej (FakeHunter) powinien być wdrożony także do innych środków masowego przekazu, także tych prywatnych. FakeHunter to projekt weryfikacji treści publikowanych w Internecie, który został uruchomiony przez Polską Agencję Prasową wspólnie z GovTech Polska i ma na celu demaskowanie nieprawdziwych wiadomości.

W świetle wyników przeprowadzonych badań stwierdzono, iż rosnące prawdopodobieństwo, że wojna hybrydowa stanie się formą walki częściej wykorzystywaną między państwami (nawet jeśli będzie ona mogącym trwać latami wstępem do konwencyjnych działań zbrojnych) wymaga wprowadzenia adaptacji w zachodnich stylach prowadzenia wojny. Wartych uwagi odniesień do istoty zagrożeń hybrydowych dokonał

[569] Prezentacja o przeciwdziałaniu dezinformacji w Wielkiej Brytanii w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), *MSZ, 21 kwietnia 2022*.

William J. Nemeth w pracy na temat wojny w Czeczenii, w której wprowadza on kategorię społeczeństw hybrydowych (hybrid societies). Na przykładzie Czeczenii, która stawiała zaciekły, opór siłom rosyjskim wykorzystując hybrydowe metody walki (wojna partyzancka), doszedł on do wniosku, że organizacja militarna takich społeczeństw nie odpowiada zachodnim koncepcjom wojskowości. Mocnymi stronami grup hybrydowych są następujące elementy: ideowość, charyzmatyczny lider, silna wiara i determinacja, duża odporność na straty własne, zdecentralizowana taktyka. Tego typu wyznaczniki sprawiają, że społeczności takie jak Czeczeni z powodzeniem stosują taktyki walki hybrydowej, którym zbiurokratyzowane struktury agresora nie są w stanie łatwo sprostać. Jednocześnie, tego typu grupy społeczne mogą skutecznie włączyć zaawansowane technologicznie systemy w ich struktury działania i strategię, a także wykorzystywać te systemy w niekonwencjonalny sposób. Przykład czeczeński pokazał możliwości wykorzystania m.in. nowoczesnych mediów do rozpowszechniania dezinformacji lub propagandy[570]. W szczególności, co doradzał W. J. Nemeth, należy wprowadzić zmiany w amerykańskiej doktrynie wojskowej, szkoleniu i organizacji sił zbrojnych oraz w całym systemie bezpieczeństwa państwa, które będą miały na celu przeciwdziałanie zagrożeniom hybrydowym. Chodzi m.in. o spłaszczenie szczebli dowodzenia na poziomie brygady w oparciu o wykorzystanie przewagi Stanów Zjednoczonych i państw zachodnich w dziedzinie informatyki, technologii komunikacyjnych i zarządzania informacjami. Wyeliminowane w ten sposób zostaną zbędne poziomy dowodzenia, co zwiększy skuteczność mniejszych sił zbrojnych Stanów Zjednoczonych[571].

Przytaczając rekomendacje amerykańskiego wojskowego sprzed ponad 20 lat trzeba stwierdzić, że kluczowe jest stałe wzmacnianie systemu bezpieczeństwa i obrony państwa z naciskiem na przeciwdziałanie tak zagrożeniom konwencjonalnym, jak i niekonwencjonalnym (hybrydowym). W 2002 r. zagrożenie krajów Europy Środkowej i Wschodniej przez Rosję zostało określone przez W. J. Nemetha jako niewystępujące *(„the non-existent Soviet threat to Central Europe").* Zagrożenie to tymczasem cały czas występowało, tylko w formie nieaktywnej, co wynikało z ówczesnej słabości Rosji oraz aktualności porozumień między NATO i Rosją. Wojna na Ukrainie w 2022 r. pokazała, że

[570] W. J. Nemeth, *Future war and Chechnya: a case for hybrid warfare*, Naval Postgraduate School, Monterey, California, June 2002, https://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1 [dostęp:12.08.2022].

[571] Tamże.

otwarte użycie siły w relacjach międzynarodowych jest zawsze możliwe, wbrew rozpowszechnianym w danych okresach trendom ideowym przez Nemetha i innych autorów lub całe środowiska zawodowe. W tym sensie, niewątpliwym błędem, z punktu widzenia długoterminowego bezpieczeństwa narodowego, było odejście od zasadniczej służby wojskowej po symbolicznym odzyskaniu przez Polskę suwerenności. Służbę tę należało zmodyfikować i dostosować do nowych realiów, ale powszechne przeszkolenie zdolnych do obrony kraju obywateli, jak pokazuje przykład m.in. Szwajcarii czy Izraela jest słusznym podejściem. Dotyczy to zawłaszcza krajów takich jak Polska, które są położone w regionach historycznie narażonych na działania zbrojne.

Struktura sił i doktryna muszą być na tyle elastyczne, aby – w sytuacji zagrożeń niekonwencjonalnych – były odpowiednie do skutecznej obrony przez wojną hybrydową. Wymaga to, aby w służbach odpowiedzialnych za bezpieczeństwo zwiększyć liczbę oficerów i personelu cywilnego z doświadczeniem w realizacji projektów, działań i operacji o charakterze międzyresortowym i międzyinstytucjonalnym[572].

Zaktualizowaną o zagrożenia hybrydowe doktrynę należy następnie wprowadzać w życie poprzez szkolenie. Obecny program szkoleniowy musi zostać zmodernizowany, aby był bardziej realistyczny i zróżnicowany. Przy zachowaniu operacji ukierunkowanych na odparcie tradycyjnego ataku, należy udoskonalać metody zdecentralizowanej walki w przypadku niekonwencjonalnego zagrożenia. Konieczny jest większy nacisk wspólne ćwiczenia i współdziałanie różnych służb i jednostek odpowiedzialnych za przeciwdziałanie zagrożeniom, w tym – hybrydowym. Przy szkoleniu istotne jest, aby używanie technologii miało miejsce jako uzupełnienie, a nie substytut wysokiej jakości sił obronnych państwa[573]. Aby zwiększyć efektywność szkoleń, należy ponadto uwzględnić zwiększony realizm (np. nacisk na ćwiczenia z użyciem ostrej amunicji także z udziałem jednostek Wojsk Obrony Terytorialnej po odpowiednim przeszkoleniu).

Prace nad włączeniem coraz bardziej realistycznych scenariuszy do ćwiczeń z zakresu przeciwdziałania zagrożeniom hybrydowym są krokiem w dobrym kierunku. Działania te polegają na trenowaniu sposobów odpowiedzi na wiele, zróżnicowanych i nie powiązanych ze sobą ataków. NATO rozważa zwiększanie przedstawicieli przemysłu

[572] Tamże.
[573] Tamże.

zaangażowanych w prace związane z przeciwdziałanianiem zagrożeniom hybrydowym. Podobnie, intensyfikuje się włączanie w tę problematykę naukowców i ekspertów pozarządowych.

Powinno się dążyć do wykształcenia kadry na różnych szczeblach hierarchii, która będzie zdolna do reagowania na zagrożenia w oparciu o pozyskaną wiedzę, umiejętności i niekonwencjonalny, ukierunkowany na cel (skuteczna obrona państwa) sposób myślenia. Osoby na kierowniczych stanowiskach (liderzy) muszą kształcić się w zakresie taktycznego podejmowania decyzji nie w oparciu o schematy i procedury, ale bazując na odpowiednim zestawie umiejętności dostosowanych do odpowiedniej sytuacji. Tego rodzaju spłaszczenie struktury dowodzenia będzie korzystne z punktu widzenia zagrożeń hybrydowych[574].

Jak wykazały wyniki badań, zagrożenia hybrydowe w cyberprzestrzeni mogą być skutecznie zwalczane tylko przy rozwoju nowoczesnych technologii przez broniące się państwo. Prace badawczo rozwojowe Polski w tym zakresie powinny być należycie finansowane, aby nie dopuścić do przewagi technologicznej adwersarzy. Wykrycie i zidentyfikowanie kraju pochodzenia ataku jest kluczowe dla zastosowania skutecznej odpowiedzi. Polska powinna korzystać w tym zakresie z możliwego wsparcia sojuszników, ale jednocześnie rozbudowywać własne zdolności. Atak cybernetyczny może być także używany jako forma obrony przed różnymi rodzajami zagrożeń, także – hybrydowymi. Siły zbrojne najpotężniejszych krajów na świecie rozwijają zdolności w zakresie defensywnych oraz ofensywnych działań w sferze cyber[575]. Potwierdza to przykład amerykański. W czerwcu 2022 r. po raz pierwszy publicznie poinformowano, że US Cyber Command przeprowadziło serię ofensywnych operacji wspierających Ukrainę[576].

W wyniku przeprowadzonych badań stwierdzono, że narzędzia cybernetyczne mogą stanowić także skuteczną obronę w określonych obszarach, jak utrzymanie kanałów komunikacji napadniętego kraju – wewnętrznych i zewnętrznych (ze światem). W klasycznych konfliktach zbrojnych, we wstępnych fazach konfliktu strona atakująca starała się zakłócić komunikację przeciwnika. Obecnie, jak pokazuje przykład wojny na Ukrainie w 2022 r. władze w Kijowie są w stanie podtrzymać system komunikacji, co wynika

[574] Tamże.

[575] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

[576] Tamże.

z zalet sieci cybernetycznych. Linia obrony w czasie konfliktu na Ukrainie wykorzystuje zdolności konwencjonalne. W przyszłości, dzięki rozwojowi zdolności ofensywnych w sferze cyber pojawić się może możliwość przeciwdziałania atakom konwencjonalnym przez paraliżujące uderzenie z wykorzystaniem arsenału cybernetycznego[577].

Wyzwaniem w zakresie przeciwdziałania zagrożeniom hybrydowym w Polsce (oraz innych państwach demokratycznych) pozostaje fakt, że tematy bezpieczeństwa narodowego przez wiele lat nie były nośne politycznie, a były wręcz ryzykowne dla rządzących. Kwestie przeciwdziałania zagrożeniom hybrydowym, oraz szerzej – przygotowania państwa do kryzysu – nie są popularnym tematem zainteresowania polityków. To raczej kwestie z zakresu tzw. szarej strefy. Przekonanie wśród decydentów politycznych i ich wyborców, że na wojnę trzeba się przygotowywać w czasach pokoju, jest coraz powszechniejsze, ale niestety wciąż niewystarczające. Trzeba jednak przyznać, że polsko-białoruski kryzys graniczny z wykorzystaniem migrantów w 2021 r. zapoczątkował zmianę w podejściu do zagrożeń hybrydowych. Konieczne są usprawnienia zarówno jeśli chodzi o rozszerzenie wiedzy o sposobach zachowania w przypadku kryzysu, jak i wypracowanie automatyzmu zachowań społecznych w takiej ewentualności[578].

Pandemia COVID -19 była testem dla państw zachodnich, który przygotował niejako je do poważniejszego kryzysu innego, ale różnie poważnego typu, jak Inwazja Rosji na Ukrainę w 2022 r. (np. większa odporność społeczeństwa w kontekście zjawiska zakupu na masową skalę produktów żywnościowych)[579].

W wyniku przeprowadzonych badań stwierdzono, że działania administracji rządowej, służb i formacji mundurowych w zakresie przeciwdziałania zagrożeniom hybrydowym powinny być wspierane i wdrażane przez całe społeczeństwo, przez oddolne ćwiczenia w zakresie przygotowania i wzrostu świadomości o zagrożeniach hybrydowych w ramach gospodarstw domowych. Znamienny jest przykład skutecznej obrony Finów przed agresją w czasie Drugiej Wojny Światowej i zestawienie tej sytuacji z załamaniem się obrony polskiej w 1939 r. Patrząc realistycznie Polska może i powinna zrobić więcej, aby

[577] Tamże.

[578] *Wzmacnianie odporności, jako kluczowa metoda przeciwdziałania zagrożeniom hybrydowym – odporność w NATO, UE i lessons learned z wybranych państw,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

[579] Tamże.

przygotować efektywną obronę przeciwko zagrożeniom hybrydowym (oraz w ujęciu odparcia potencjalnego ataku konwencjonalnego). Wejście do NATO w 1999 r. było wielkim osiągnięciem w zakresie wzmocnienia polskiego bezpieczeństwa w kontekście zagrożeń wojennych, które regularnie dotykały regionu Europy Środkowej w minionych dekadach, a wcześniej – stuleciach.

Ponadto, w planowaniu sposobów przeciwdziałania zagrożeniom hybrydowym należy uwzględnić wykorzystanie zamachów jako narzędzia wojny hybrydowej na terytorium Rzeczpospolitej Polskiej. Istnieje zatem konieczność stałego uwzględniania zagrożeń o charakterze terrorystycznym w działaniach na rzecz wzmacniania odporności na zagrożenia hybrydowe. W celu skutecznej odpowiedzi, istotne jest zaplanowanie i dokonanie „hybrydowej reakcji na tego rodzaju zagrożenia. Oprócz samych działań antyterrorystycznych i kontrterrorystycznych niezbędne będzie prowadzenie innych działań, w tym z zakresu przeciwdziałania dezinformacji i walki informacyjnej[580].” Istnieje w tym zakresie dużo do zrobienia jeśli chodzi m.in. o świadomość w tej tematyce (gdzie się spotykamy – punkt zbiorczy), jakie posiadamy metody awaryjnego zachowania na wypadek nie tylko ataków hybrydowych, ale i kryzysów, które mogą być ich skutkiem (np. odcięcie prądu lub wyłączenie telefonii komórkowej w wyniku ataku). Po inwazji rosyjskiej na Ukrainę w 2022 r. w Polsce też rozpoczęto prace udoskonalające rozwiązania na wypadek zagrożeń hybrydowych i innych sytuacji kryzysowych (np. obowiązek budowy schronów dla deweloperów – charakterystyczna cecha systemu fińskiego), ale powinny one mieć charakter systemowy i uprzedzający zagrożenie, a nie reaktywny[581].

W wyniku przeprowadzonych badań stwierdzono, że państwa zachodnie, w tym Polska, przeciwdziałając zagrożeniom hybrydowym muszą uwzględniać swoją aktywność we wszystkich istotnych dla bezpieczeństwa narodowego dziedzinach. Następuje przesunięcie ze sfery wojskowej dominacji do gospodarczej i technologicznej. Trwa walka o to, kto będzie kontrolował przepływ informacji czy szlaki logistyczne. Zamieniające się uwarunkowania międzynarodowe i rywalizacja krajów demokratycznych z autokratycznymi

[580] M. Piekarski *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych*, „Terroryzm – studia, analizy, prewencja” 2022, s. 89-90.

[581] *Wzmacnianie odporności, jako kluczowa metoda przeciwdziałania zagrożeniom hybrydowym – odporność w NATO, UE i lessons learned z wybranych państw,* prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), *MSZ, 21 kwietnia 2022.*

dostarczają nowych wyzwań w zakresie przeciwdziałania zagrożeniom hybrydowym. Zagrożenia hybrydowe obecnie wynikają ze zmieniającej się sytuacji globalnej i politycznych uwarunkowań. Wzrost potęgi Chin jest jedną z nich. Pekin nie chce być już numerem 2 czy trzy na arenie międzynarodowej, ale zając pozycje lidera. Wzrost znaczenia potęg regionalnych (Iran, Korea Północna) oraz aktorów pozapaństwowych (np. ISIS), które wykorzystują wszystkie dostępne im środki walki. Kolejnym powodem jest zmieniające się środowisko bezpieczeństwa. Ciekawym przykładem jest tu Państwo Islamskie, którego aktywność posiada wiele cech pozapaństwowego aktora hybrydowego (co nie oznacza, że nie ma on związków z zainteresowanymi taką formą destabilizacji aktorami państwowymi). Przeciwdziałanie zagrożeniom hybrydowym musi być prowadzone we wszystkich domenach, gdzie występuje to ryzyko (m.in. sfery: wojskowa, cyber, informacyjna, wywiadowcza, gospodarcza, kulturalna), co nadaje tym wysiłkom horyzontalny charakter[582]. Zadanie to musi być realizowane przede wszystkim przez państwa, przy wykorzystaniu wsparcia instytucji unijnych i/lub natowskich[583].

Dla skutecznego przeciwdziałania zagrożeniom hybrydowym konieczna jest dokładna wiedza o działalności na terenie kraju-obrońcy podmiotów, które mogą być wykorzystane do ataku. Zwiększeniu powinny ulec m.in. zdolności wpływu instytucji państwowych na zarejestrowane lub funkcjonujące w nich powiązane z zagranicą przedsiębiorstwa i inne podmioty. Przykładem służą inne kraje, w których osiąga się to m.in. przez stosowanie polityki fiskalnej i regulacyjnej w celu skłonienia firm do określonych zachowań. Mogą to być zachęty lub rozwiązania penalizujące. Przykładem są tu działania USA w zakresie ograniczenia inwestycji firm amerykańskich w Chinach oraz zablokowania dostępu tego kraju do półprzewodników i innych nowoczesnych technologii pozyskiwanych od prywatnych spółek (powodem – bezpieczeństwo narodowe).

Jak wykazały wyniki badań, od czasu aneksji Krymu w 2014 r. podjęto wiele inicjatyw – także w sferze informacyjnej – aby wzmocnić odporność Polski, oraz innych krajów UE i NATO na zagrożenia hybrydowe. Trudno nie zgodzić się z A. Olechem, iż należy docenić te wysiłki i utrzymać tempo i intensywność procesów usprawniających przeciwdziałanie

[582] Zob. *The Landscape of Hybrid Threats: A Conceptual Model. Public Version*, European Union / Hybrid CoE, 2021 https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf [dostęp: 4.10.2022].

[583] *Countering Hybrid Threats and enhancing resilience*…

zagrożeniom hybrydowym[584]. Jednak, ze względu na zmieniający się charakter zagrożeń hybrydowych konieczne jest stałe monitorowanie rozwoju sytuacji bezpieczeństwa oraz przygotowania danego kraju do zwalczania tych zagrożeń. Potrzebne jest strategiczne podejście do przeciwdziałania zagrożeniom hybrydowym, które obejmie przede wszystkim nowe rozwiązania w państwach narodowych, ale także współpracę na poziomie międzynarodowym, włączając w to kraje pozaeuropejskie. Zrozumienie wszystkich stron konfliktu oraz uzyskanie informacji o ich motywach i stosowanych przez nich działaniach jest kluczowe dla budowania potencjału bezpieczeństwa i obronny kraju położonego w danym regionie (także – w kontekście przed rozmaitych zagrożeń hybrydowych). Zrozumienie przesłanek jakimi kierują się światowi przywódcy krajów, których polityka bezpieczeństwa może stanowić zagrożenie, zwiększy wiedzę NATO i UE odnośnie do możliwych przyszłych działań tych państw. Skutkiem tego będzie wzmocnienie systemów zwalczania zagrożeń hybrydowych w krajach członkowskich tych struktur[585].

Z perspektywy Polski, należy w pierwszej kolejności skoncentrować się na wyzwaniach w Europie Środkowo-Wschodniej, zwłaszcza po wybuchu wojny rosyjsko-ukraińskiej w 2022 r. Kluczowa do tego jest znajomość celów polityki Federacji Rosyjskiej oraz realnych (nie deklaratywnych) relacji tego mocarstwa nuklearnego nie tylko z krajami go wspierającymi (jak pośrednio czynią Chiny i Iran), ale także z innymi czołowymi aktorami w globalnej polityce bezpieczeństwa w postaci przede wszystkim USA, a także innych członków Rady Bezpieczeństwa ONZ (Wielkiej Brytanii, Francji) i krajów do niej aspirujących (m.in. Niemcy, Indie), bądź posiadających znaczące zdolności wpływania na politykę bezpieczeństwa na świecie (np. Izrael).

Jednym z narzędzi przeciwdziałania zagrożeniom hybrydowym, które powinno być intensywniej wykorzystywane przez Polskę, są społeczne kampanie informacyjne uświadamiające o zagrożeniach oraz przeciwdziałające dezinformacji w mediach społecznościowych. W odróżnieniu od prób czysto eksperckiego informowania o zagrożeniach hybrydowych, przekaz instytucji rządowych powinien być realizowany w większym stopniu za pomocą organizacji pozarządowych oraz wpływowych jednostek o autorytecie w określonej dziedzinie lub środowisku (np. przedstawicieli świata naukowego,

[584] A. Olech, op. cit.
[585] Tamże.

ale także szeroko rozumianej sfery kultury, mediów, sportu a nawet rozrywki – włączając w to źródła internetowe i elektroniczne). Ukierunkowanie działań informacyjnych w ten sposób pomoże zapewnić maksymalnie skuteczne dotarcie z komunikatem o zagrożeniach hybrydowych do znaczącej części społeczeństwa podnosząc jego świadomość o zagrożeniach. Władze powinny podjąć intensywniejsze działania na rzecz budowania i umacniania umiejętności polskiego społeczeństwa do umiejętnej – mającej na względzie długoterminowe bezpieczeństwo państwa – oceny informacji (także – decyzji polityków) biorąc pod uwagę kryterium zapewniania bezpieczeństwa państwa w długim okresie. Chodzi zwłaszcza o umiejętności pozyskiwania, weryfikacji i analizy informacji. Przekaz mający za zadanie przeciwdziałać dezinformacji (programy, audycje, wywiady) powinien być także cyklicznie wprowadzany do oferty programowej publicznej telewizji i stacji radiowych, a także – innych rozgłośni (za pośrednictwem Krajowej Rady Radiofonii i Telewizji). Analogiczne rozwiązanie powinno się zastosować w odniesieniu do prasy, Internetu oraz innych mediów elektronicznych (kanały filmowe typu Netflix).

Jak wynika z badań, polskie władze powinny organizować cykliczne kampanie medialne, które miałyby na celu uświadomienie obywateli odnośnie ryzyka dotyczącego agitacji, propagandy i dezinformacji. Działania informacyjne winny być nasilone w okresach przedwyborczych, w tym – przed istotnymi referendami i innymi głosowaniami, które są charakterystyczne dla obecnych uwarunkowań demokratycznych w Polsce. Inicjatywy tego typu nie mogą być jednak incydentalne, ale powinny być starannie zaplanowane i profesjonalnie oraz systematycznie wdrażane. Tego rodzaju kampanie zorganizowano w latach 2018-2019 r. np. w Australii (pt.: „Zatrzymaj się i rozważ", ang. *Stop and Consider Campaign*). Australia wprowadziła także wydzielony, dostępny publicznie przez Internet Rejestr dezinformacji (ang. *Disinformation register*), do którego wprowadzano się na bieżąco przypadki fałszywych lub błędnych informacji wraz z ich korektą.

Skuteczne przeciwdziałanie zagrożeniom hybrydowym nie jest możliwe bez wielosektorowej współpracy między instytucjami państwowymi, mediami, biznesem oraz społeczeństwem obywatelskim. W Australii w 2018 r. cztery instytucje rządowe utworzyły Zespół Zadaniowy ds. Integralności Wyborów, który został powołany w celu zidentyfikowania potencjalnych ataków cybernetycznych i wywierania wpływu na proces

wyborczy z zagranicy. Kierownictwo prac zespołu powierzono Departamentowi Spraw Wewnętrznych.

W kontekście obserwowanego przeciwdziałania narracji prorosyjskiej w czasie wojny na Ukrainie w 2022 r., podkreślić należy, iż wrogi przekaz może mieć subtelny charakter i być dozowany w trudno wykrywalny sposób. Nie muszą to być treści jawnie opowiadające się za daną stroną konfliktu (np. Rosją), ale mogą one wzbudzać nieufność do obecnych sojuszników czy świata wartości (np. zachodnich) i w tą drogą osłabiać pozycję danego kraju. Społeczeństwo powinno być zatem uwrażliwione na zagadnienia wywierania wpływu na wartości, odczucia i emocje. Kampanie informacyjne i uświadamiające powinny być realizowane przy poszanowaniu wolności słowa i praw obywatelskich. Tego rodzaju ofertę należy także przygotować dla zamieszkujących na terenie Polski mniejszości narodowych i etnicznych ze szczególnym uwzględnieniem Białorusinów i Ukraińców.

W świetle wyników przeprowadzonych badań stwierdzono, że korzystne dla usprawnienia możliwości przeciwdziałania zagrożeniom hybrydowym przyniosłoby rozpoznanie możliwości wykorzystania sieci komórkowych w sposób zbliżony do działań Rządowego Centrum Bezpieczeństwa, które przekazuje obywatelom ostrzeżenia dotyczące warunków atmosferycznych i klęsk żywiołowych. Wiadomości SMS z ostrzeżeniami odnośnie przypadków znaczącej dezinformacji oraz fałszywych treści rozpowszechnianych w mediach, które zarażają bezpieczeństwu państwa lub porządkowi publicznemu. Komunikowanie się tą drogą instytucji państwowych z obywatelem, powinno jednak uzyskać uprzednio jego akceptację. Jest to istotne zwłaszcza jeśli chodzi o wykorzystanie prywatnych środków obywateli w postaci telefonu i abonamentu (obecnie jest to wprowadzone bez uzyskania autoryzacji). Podobnej zgody obywatela powinno wymagać używanie przez instytucje państwowe do komunikacji aplikacji na prywatnych telefonach komórkowych (i samo instalowanie ich). Kampanie informujące powinny zwiększyć świadomość celowości takiego rozwiązania i powinno się wycofać z obecnie przyjętej drogi wprowadzania go odgórnie. Nie powinno ono także być nadużywane do przekazywania informacji mało istotnych lub z wysoką częstotliwością, co ma miejsce obecnie w przypadku informacji pogodowych.

Skalę wyzwań w zakresie stworzenia skutecznego systemu przeciwdziałania zagrożeniom hybrydowym pokazuje obszar informacyjny. Edukacja o źródłach

dezinformacji i propagandy stanowiących zagrożenie dla bezpieczeństwa Polski powinna być włączana do programów szkolnych, co najmniej na poziomie szkół średnich i w szkolnictwie wyższym. Chodziłoby w tym przypadku o kształtowanie umiejętności krytycznego myślenia, kwestionowanie niewiarygodnych źródeł informacji i ich umiejętne odczytywanie/interpretowanie. W kontekście bezpieczeństwa Polski, jak trafnie zauważyła Agnieszka Rogozińska, niezbędne jest „stworzenie doktryny bezpieczeństwa informacyjnego uwzględniającej rosyjską specyfikę działań hybrydowych, która stanowiłaby punkt odniesienia dla działalności legislacyjnej, precyzyjnie definiując zagrożenia wynikające z nowych działań wojennych i ich skutki, szczególnie w sytuacji, kiedy Polska nie dysponuje odpowiednim zapleczem ekonomicznym, materialnym i technologicznym, aby odpowiednio zabezpieczyć się przed rosyjskimi formami oddziaływań informacyjnych[586].”

W świetle wyników przeprowadzonych badań stwierdzono, że ważnym elementem przeciwdziałania zagrożeniom hybrydowym jest tworzenie wyspecjalizowanych struktur instytucjonalnych do tego celu. Krokiem w dobrym kierunku jest powoływanie międzyresortowych zespołów ds. przeciwdziałania dezinformacji, w którego skład wchodzą najczęściej m.in. przedstawiciele resortu spraw zagranicznych (przykład Danii). Lepszym rozwiązaniem byłoby jednak powoływanie komórek wyspecjalizowanych tylko w analizie i przeciwdziałaniu dezinformacji. Powinno się także intensyfikować działania monitoringowe w związku z ważnymi wydarzeniami zaplanowanymi w danym kraju, zwłaszcza kampaniami wyborczymi oraz samymi wyborami. W takich sytuacjach zagrożenie obcej ingerencji w przebieg kampanii może być wysokie.

Ponadto, jak wykazały wyniki badań, eksperci do spraw przeciwdziałania dezinformacji powinni skupiać się nie tylko na śledzeniu wrogich narracji dotyczących bieżących wydarzeń (np. n a Ukrainie), ale przede wszystkim tych wymierzonych w kierunku Polski, a w dalszej kolejności wobec Zachodu. Rolą komórek przeciwdziałających dezinformacji w ministerstwach spraw zagranicznych jest przeważnie przegląd i monitoring aktywności w mediach oraz zarysowywanie szerszej perspektywy. Natomiast, cywilne

[586] A. Rogozińska, *Niemilitarne zagrożenia dla Ukrainy w kontekście działań hybrydowych prowadzonych przez Federację Rosyjską*, INE 24 listopada, 2019, http://ine.org.pl/wp-content/uploads/2020/02/INE.niemilitarnezagrozeniadlaukrainywkontekstiedzialanhybrydowych.pdf [dostęp: 11.06.2022].

i wojskowe służby specjalne odpowiedzialne są za śledzenie zewnętrznych i wewnętrznych zagrożeń (np. potencjalnych cyberataków). Ponadto, kraje sojusznicze mogą także, przy okazji swoich działań kompetencyjnych, na bieżąco monitorować wątki dotyczące Polski pojawiające się w mediach krajów mogących mieć wrogie zamiary i przekazywać nam te informacje. Praktyka ta powinna wiązać się z wzajemnością ze strony polskich instytucji.

Jak wykazały wyniki badań, uwzględniając sytuację geopolityczną i wyzwania w zakresie przeciwdziałania informacyjnym zagrożeniom hybrydowym przed jakimi stoi Polska, konieczne jest stworzenie strategii (doktryny) bezpieczeństwa informacyjnego RP. Zasadne jest dokonanie przeglądu istniejących regulacji prawnych w kontekście uzupełnienia ich o zakres BI. Pilnych działań wymaga problem propagandy i dezinformacji ze strony aktorów stosunków międzynarodowych. Należy wskazać, że regulacje dotyczące dezinformacji w polskim prawie nie istnieją w ogóle. Natomiast problem fałszywych wiadomości (ang. *fake news*) uregulowany jest w ograniczonym wymiarze (kwestie dostępu do informacji, jej rozpowszechniania i prawdziwości są rozproszone). Co zdumiewające, żadna z partii politycznych nie artykułuje wyraźnie kwestii dezinformacji (brak w programach wyborczych i w działaniach). Celem strategii bezpieczeństwa informacyjnego RP, która podlegałaby okresowej ewaluacji, powinno być m.in.:

a) określenie interesów narodowych w sferze bezpieczeństwa informacyjnego (BI) i sposobów ich zabezpieczania (w polityce wewnętrznej, zagranicznej);

b) zdefiniowanie rodzajów zagrożeń bezpieczeństwa informacyjnego oraz źródeł tych zagrożeń (w tym – stworzenie siatki pojęciowej z obszaru bezpieczeństwa informacyjnego oraz jej aktualizowanie i wprowadzanie do aktów prawnych);

c) określenie stanu BI w różnych dziedzinach życia publicznego i głównych wyzwań w tej dziedzinie;

d) wprowadzenie regulacji prawnych dotyczących obszarów mających bezpośredni wpływ na BI (m.in. w zakresie repolonizacji mediów, penalizacji dezinformacji oraz transparentności finansowania organizacji pozarządowych);

e) określenie ram i sposobów współpracy międzynarodowej w odniesieniu do BI;

f) wskazanie źródeł i sposobów finasowania projektów wzmocnienia BI.

Co więcej, w toku badań stwierdzono, że do priorytetów w zakresie przeciwdziałania zagrożeniom hybrydowym w sferze informacyjnej (głownie z kierunku wschodniego), należy wprowadzenie ustawy repolonizacyjnej. Wynika to z faktu, iż zagraniczny kapitał posiada większość udziałów w kilku segmentach rynku medialnego w Polsce: prasowym, radiowym i internetowym. Polski kapitał pozostaje jeszcze przeważający tylko na rynkach: telewizyjnym i ogólnokrajowym tygodników. Sytuacja taka, która nie powtarza się w innych krajach UE, stanowi źródło zagrożenia dla bezpieczeństwa informacyjnego państwa. Liczne przypadki wykupywania mediów w Europie przez podmioty związane z rosyjskimi służbami specjalnymi potwierdzają to ryzyko. Korzystny model organizacji sektora medialnego pokazują przykłady i rozwiązania przyjęte np. w Niemczech i we Francji.

W wyniku przeprowadzonych badań stwierdzono, że w celu ochrony bezpieczeństwa informacyjnego należałoby także wprowadzić penalizację dezinformacji. Jednak, z uwagi na wrażliwy społecznie charakter kwestii wolności słowa i wprowadzenia cenzury, wprowadzenie regulacji penalizujących wrogą propagandę należałoby poprzedzić merytoryczną kampanią edukacyjną i konsultacjami m.in. z przedstawicielami środowisk naukowych, dziennikarskich organizacjami pozarządowymi. Wyzwaniem w zakresie przeciwdziałania zagrożeniom hybrydowym jest kwestia legalności dezinformacji. Dezinformacja – jak wynika z przygotowanego dla Komisji Europejskiej raportu o nieprawdziwych informacjach w sferze online – niekoniecznie jest „niezgodna z prawem, ale może być szkodliwa dla obywateli i ogółu społeczeństwa. Ryzyko szkody obejmuje zagrożenia dla demokratycznych procesów politycznych i wartości demokratycznych, które kształtują politykę publiczną w różnych sektorach, takich jak zdrowie, nauka, edukacja, finanse i inne. Ryzyko szkód wywołanych przez dezinformację jest potęgowane przez produkcję i promocję tego typu treści dla korzyści ekonomicznych, celów politycznych lub ideologicznych i może być zwielokrotnione w wyniku sposobów, w jaki różni odbiorcy i społeczności otrzymują, angażują się i wzmacniają przekaz dezinformacyjny[587].” W Europie i na świecie istnieją kraje posiadające przepisy penalizujące dezinformację. Najbardziej restrykcyjne prawodawstwo w tym zakresie obowiązuje w Singapurze (od 2019

[587] *A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation*, European Commission – Directorate-General for Communication Networks, Content and Technology, March 2018 , https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1 [dostęp: 29.11.2022].

r.), Na mocy ustawy o ochronie przed fałszerstwami i manipulacją w Internecie zdelegalizowano rozpowszechnianie fałszywych stwierdzeń, które zagrażają bezpieczeństwu publicznemu i stosunkom Singapuru z innymi państwami. Za tego typu praktyki grozi kara grzywny w wysokości do 37 tys. USD lub pięć lat więzienia. W przypadku, gdy takie informacje zostały rozpowszechnione za pomocą nieautentycznego konta internetowego lub automatu (tzw. bota), kary wzrastają dwukrotnie. Ponadto, platformy internetowe (m.in. Twitter, YouTube, Facebook), mogą zostać ukarane grzywną w wysokości nawet do 740 tys. USD, a ich lokalne kierownictwo – karą więzienia do 10 lat. Singapur prowadził także prace nad mechanizmami prawnymi i procedurami, które miały na celu powstrzymanie rozprzestrzeniania dezinformacji w krótkim czasie (do kilku godzin). Jak wykazały wyniki badań, podobne przepisy oraz sankcje karne (grzywny lub więzienia) stosuje się m.in. w Niemczech (ustawa Netzwerkdurchsetzungsgesetz, NetzDG – zwana także ustawą facebookową), Izraelu, Włoszech, Brazylii, Chile, Chorwacji i Irlandii. Z kolei we Francji, przyjęte w grudniu 2018 regulacje ustawowe zawierają pierwszą w Europie prawną definicję „fałszywych informacji" (ang. *fake news*). Daje ona władzom prawo do usuwania fałszywych treści, a nawet blokowania witryn.

W wyniku przeprowadzonych badań stwierdzono, że istotnym czynnikiem wywierającym wpływ na przeciwdziałanie zagrożeniom hybrydowym jest dokonanie zmian w prawie dotyczącym funkcjonowania organizacji pozarządowych pod kątem zwiększenia dostępu do informacji o finansowaniu tego rodzaju struktur. Interesującym przykładem takiego rozwiązania jest węgierska ustawa z czerwca 2017 r., zgodnie z którą każda organizacja pozarządowa, która w ciągu roku otrzymała równowartość co najmniej 23 tys. euro wsparcia z zagranicy, musi w ciągu 15 dni zadeklarować i upublicznić zagraniczne finansowanie (przez zgłoszenie w sądzie i opublikowanie na własnej stronie Internetowej oraz na wszystkich wydawanych przez siebie materiałach).

Multiplikowaniu dezinformacji i propagandy sprzyja również powszechny poziom tabloidyzacji mediów, dziennikarstwa, a w efekcie – społeczeństwa, a nawet kręgów rządzących. Zjawisko łączenia informacji z rozrywką (ang. *infotainment*), w nienaturalny sposób stymuluje zainteresowanie odbiorcy. Jego szkodliwość wynika z zalewu rynku medialnego (i generalnie zdecydowanej większości publicznej przestrzeni informacyjnej) materiałami, które mają jednocześnie pełnić funkcję rozrywkową i informacyjną (dominują

informacje o płytkim charakterze, połączone ze zdjęciami, mającymi przyciągnąć uwagę – afery, plotki i skandale, tematyka seksualna, pieniądze, władza). Ważna jest przy tym świadomość, że wrogie ośrodki propagandowe wykorzystują każdą wypowiedź lub incydent z udziałem polskich obywateli do uwiarygodnienia własnych narracji. Ryzyko takiego zamanipulowania niosą zwłaszcza kontrowersyjne wypowiedzi osób publicznych.

Jak wykazały wyniki przeprowadzonych badań stwierdzono, w kontekście usprawnienia metod przeciwdziałania zagrożeniom hybrydowym Polska powinna wzmocnić korzystne dla siebie wymiary kooperacji z USA celem budowania niezależnego, krajowego potencjału w tym obszarze. W ostatnich latach sytuacja bezpieczeństwa w otoczeniu Polski ulega pogorszeniu. Tradycyjne zagrożenia dla bezpieczeństwa narodowego nie maleją za sprawą m.in. aktywności wojskowej Rosji na wschodzie Europy, a równolegle narastają zagrożenia hybrydowe. Jeśli o sytuację bezpieczeństwa w sąsiedztwie Polski, politycy europejscy dostrzegli zagrożenia hybrydowe w 2014 r., kiedy nastąpiła błyskawiczna operacja zajęcia Krymu z użyciem tych metod[588]. Cześć ekspertów wskazywała, że to swoiste przebudzenie powinno nastąpić znacznie wcześniej. Przesłanek do takich działań osłonowych dostarczyła m.in. wojna w Gruzji (hybrydowe ataki Rosji wsparciem działań konwencjonalnych) czy cyberataki na Estonię w 2007 r.[589] USA uzupełniają systemy zaprojektowane z myślą o konfliktach XX w. o nowe, asymetryczne zdolności obrony i ataku. Stany Zjednoczone, których strategicznym imperatywem jest utrzymanie dominacji wojskowej na świecie, przyjęły podejście określane mianem „zintegrowanego odstraszania". Obejmuje ono zaangażowanie sojuszników i partnerów oraz własnych sił konwencjonalnych i niekonwencjonalnych (nuklearnych, kosmicznych, informacyjnych). Bazą do tego jest potencjał gospodarczo-technologiczny i wykorzystanie instrumentów amerykańskiej dyplomacji. Obok zwalczania agresywnych działań Rosji w Europie, USA rozwijają także wojskowy potencjał w celu stawienia czoła Chinom, które Waszyngton uznaje za wzrastające wyzwanie („*pacing challenge*").

Jak wykazały wyniki badań, Polska powinna – zgodnie z interesem narodowym – czerpać z doświadczeń wybranych krajów, które dokonały usprawnień systemu przeciwdziałania zagrożeniom hybrydowym. Państwa członkowskie UE są obecnie zgodne,

[588] Rosja używała przeciwko Ukrainie kampanii dezinformacyjnych, cyberataków oraz uderzeń na infrastrukturę krytyczną na miesiące przed zajęciem Krymu.

[589] *Countering Hybrid Threats and enhancing resilience*…

co do potrzeby skoordynowanego przeciwdziałania narastającemu problemowi związanemu z zagrożeniami hybrydowymi, konieczności adaptacji UE do zmieniających się uwarunkowań, a także wzmocnienia regulacji dotyczących przestrzeni informacyjnej, cyberprzestrzeni, infrastruktury (zwłaszcza energetycznej i transportowej). W szczegółowych sprawach widoczne są jednak różnice stanowisk. Kwestie takie jak różne priorytety geograficzne państw wymagają stałej aktywności strony polskiej w celu utrzymania uwagi swoich sojuszników z UE, NATO oraz pozostałych regionów na zagrożeniach na naszych wschodnich granicach (generowanych głownie przez Rosję, a także Białoruś). Percepcja bezpieczeństwa narodowego krajów w Europie zmieniła się w ostatnich latach, co obrazowało podejmowanie licznych działań zaradczych przez poszczególne państwa (np. powołanie przez Niemcy specjalnego zespołu ds. ingerencji w proces wyborczy, powołanie przez Francję agencji Viginum ds. ingerencji cyfrowych, czy ustanowienie Agencji Obrony Psychologicznej przez Szwecję). Wskazuje to na wzrost świadomości zagrożeń. Zagrożenia hybrydowe stały się „nową normalnością", do której państwa muszą się dostosować. Potrzeba tworzenia w warunkach krajowych odrębnej agencji, której rolą byłoby zwiększanie odporności społeczeństwa na dezinformację jest różnie postrzegana w Europie. Cześć państw, jak Dania nie widzi takiej konieczności pozostawiając tę domenę odpowiednio wzmocnionej kadrowo, finansowo i organizacji dyplomacji (centrum monitorowania dezinformacji) oraz służbom specjalnym. Inne kraje, jak np., Szwecja utworzyły specjalne struktury służące przeciwdziałaniu zagrożeniom hybrydowym (Agencja Obrony Psychologicznej).

W świetle wyników przeprowadzonych badań, strategia przeciwdziałania zagrożeniom hybrydowym ze strony Rosji powinna uwzględniać specyficzny charakter i nastawianie do walki rosyjskiego narodu. Wskazują na to uwagę liczni autorzy, w ocenie których Rosja powinna być uważana za społeczeństwo hybrydowe[590]. Aby odnieść sukces w

[590] Rosyjskie działania hybrydowe nie są czymś wyjątkowym, natomiast nowość polega na ich połączeniu – jak zauważył pułkownik amerykańskiej piechoty morskiej i badacz problematyki wojny hybrydowej w Czeczenii W. J. Nemeth – „ze społeczno-kulturowo-polityczną konstrukcją kleptokracji i państwa bezpieczeństwa, które Putin stworzył w Rosji". Co więcej, przywódca Federacji Rosyjskiej: „dokonał syntezy istniejącej taktyki wojskowej i elementów rosyjskiej kultury z hybrydową naturą obecnego państwa i społeczeństwa rosyjskiego, tworząc hybrydową strategię (…). Ponadto, Putin wykorzystał zalety nowoczesnej technologii i środków komunikacji, które nie tylko wzmacniają stosowaną taktykę hybrydową, ale operacjonalizują ją w całej Rosji, wzmacniając hybrydowy charakter rosyjskiego państwa i społeczeństwa, a także eksportując tę taktykę na zewnątrz przeciwko państwom zachodnim w ogóle, a NATO w

przeciwdziałaniu zarówno taktyce, jak i ewolucji rosyjskiego modelu wojny hybrydowej, jak dowodzi Nemeth, kraje zachodnie muszą: „(…) opracować – oprócz środków przeciwdziałających aspektom taktycznym – kompleksową reakcję, która odnosi się do hybrydowej natury państwa rosyjskiego. Skupienie się wyłącznie na przeciwstawianiu się rosyjskiej taktyce nie przyniesie pożądanego efektu końcowego, ponieważ utrzyma to kraje zachodnie w ciągłym cyklu wymagającym przeciwdziałania kolejnym odsłonom [rosyjskiego] państwa hybrydowego bez zajmowania się fundamentalną przyczyną i skutecznego przeciwdziałania odradzaniu się Rosji i jej antypatii względem Zachodu[591].”

Dla zrozumienia pełnego obrazu zagrożeń hybrydowych generowanych przez Federację Rosyjską konieczne jest przyjrzenie się relacjom Kremla z Chinami. Ukraina, w ocenie części ekspertów, jest częścią większej rozgrywki między USA i Chinami o dominację na arenie międzynarodowej. USA, traktują Europę Środkową i Wschodnią, jako część swojej strefy wpływów, co zostało potwierdzone przyjęciem m.in. państw tego regionu do NATO (uchroniło to te kraje przed powrotem do rosyjskiej strefy wpływów). Armia rosyjska jest obecnie silniejsza niż ta, która jest w dyspozycji władz Chin. W kontekście Ukrainy, Pekin mógłby zatem wesprzeć Federację Rosyjską kontyngentem nawet kilkusettysięcznym celem zabezpieczenia dla przykładu rosyjskiej Syberii i zluzowaniem tamtejszych sił rosyjskich, które mogłyby wesprzeć tzw. „specjalną operację wojskową”. Jednak Federacja Rosyjska nie jest tym zainteresowana z uwagi na ryzyko, że takie obce wojska prawdopodobnie nie opuściłyby już terytorium rosyjskiego.

Odkąd termin zagrożeń i wojny hybrydowej został wprowadzony państwa zachodnie były w stanie zmienić postrzeganie działań Rosji (główny – obok Chin – agresor hybrydowy, a od 2022 r. – także kinetyczny). Z drugiej jednak strony, w obecnej sytuacji wielu przywódców krytykuje określanie przez Federację Rosyjską agresywnych działań zbrojnych na Ukrainie mianem operacji specjalnej. W tym kontekście używanie nadal określenia wojna hybrydowa powoduje rozmycie sytuacji i może utrudnić ewentualne roszczenia prawne o odszkodowania.

szczególności.” W. J. Nemeth, *Russia’s State-centric Hybrid Warfare,* ICDS Diplomaatia magazine, APRIL 17, 2015, https://icds.ee/en/russias-state-centric-hybrid-warfare/ , [dostęp:13.08.2022].

[591] W. J. Nemeth, *Russia’s State-centric Hybrid Warfare*, ICDS Diplomaatia magazine, APRIL 17, 2015, https://icds.ee/en/russias-state-centric-hybrid-warfare/ [dostęp:13.08.2022].

W czasie wojny na Ukrainie użycie prorosyjskich zasobów dezinformacji (proxy) wzrosło znacząco w krajach zachodnich (prorosyjska narracja była nadawana z adresów IP zlokalizowanych poza Rosją właśnie w krajach NATO i UE. Wcześniej nie było to odnotowywane na taką skalę. Taka sytuacja wymaga od krajów zachodnich prac nad wypracowaniem protokołu zachowań i środków w zakresie cyberobrony, który będzie respektowany przez wszystkie kraje tej wspólnoty bezpieczeństwa.

W wyniku badań stwierdzono, że w planowaniu działań zmierzających do poprawy systemu przeciwdziałania zagrożeniom hybrydowym ważne miejsce powinno mieć uwzględnienie polityki Chin. Wsparcie władz w Pekinie dla Rosji (deklaracje polityczne) może poważnie wpłynąć na determinujący polskie bezpieczeństwo dalszy rozwój wypadków w Europie Środkowej. Cenna dla analizy postrzegania zagrożeń międzynarodowych przez kraje, z którymi Zachód pozostaje w konflikcie jest ocena ich oficjalnych stanowisk i konfrontowanie tego z realnymi działaniami. Analiza poglądów polityków chińskich była istotna w kontekście bliskiej współpracy tego kraju z Federacją Rosyjską. W wypowiedziach przedstawicieli ChRL systematycznie pojawiały się (zwłaszcza od czasu agresji Rosji na Ukrainę w 2022 r.) następujące argumenty lub twierdzenia:

a) podkreślanie, że kraje zachodnie powinny spoglądać na Chiny jak na szansę, a nie zagrożenie. Pekin był zdania, że zawsze prowadził politykę pokojowego rozwoju (nie tworzył bloków wojskowych, nie prowadził wojen przez pośredników);

b) sprzeciw wobec prowokacyjnej retoryki NATO (Chiny są zagrożeniem) oraz konieczność zaprzestania przez państwa zachodnie wysyłania okrętów i samolotów w bezpośrednie sąsiedztwo Chin oraz budowy wrogich Pekinowi nowych bloków (z Australią, Japonią i Koreą Południową);

c) utrzymywanie, że polityka nuklearna Chin jest realizowana w wymiarze minimum koniecznym dla zapewnienia bezpieczeństwa narodowego (zasada „no first use").

Deklaracje strony chińskiej nie pokrywają się jednak z szerokim zakresem pośredniego wsparcia udzielanego przez Chiny Rosji. Brak jasnego potępienia przez Pekin rosyjskich działań na Ukrainie od lutego 2022 r. pokazuje, że większość z argumentów prezentowanych przeze ChRL publicznie nie ma pokrycia w rzeczywistych działaniach.

Pekin, podobnie, jak Rosja, bardzo intensywnie rozbudowuje swoje konwencjonalne oraz niekonwencjonalne zdolności bojowe – w tym hybrydowe (np. cybernetyczne). Z każdego konfliktu z elementami walki hybrydowej wnioski wyciągają nie tylko strony tego sporu, ale także kraje bezpośrednio niezaangażowane. Warto zauważyć, że agresja Rosji na Ukrainę w 2022 r. może posłużyć dla przykładu Chinom do aktualizacji planów ewentualnego zajęcia Tajwanu.

Ponadto, jak wykazały wyniki badań, świadomość sytuacyjna jest kluczowa dla przeciwdziałania zagrożeniom hybrydowym nie tylko w odniesieniu do sfery rządowej, ale także – sektora prywatnego (banki, firmy transportowe, porty lotnicze i morskie, producenci i dystrybutorzy żywności). Przeciwdziałanie zagrożeniom w tym ujęciu wymaga zadbania o zabezpieczanie całej tkanki społeczeństwa i wszystkich instytucji działających na jego rzecz. To bardzo istotne, aby firmy z sektorów kluczowych dla bezpieczeństwa miały świadomość i instrumenty w zakresie przeciwdziałania zagrożeniom hybrydowym, w tym w cybersferze[592].

Przeciwdziałanie zagrożeniom hybrydowym – podobnie jak praca nad poprawą bezpieczeństwa państwa – ma swoje początki w edukacji. Wychowywanie młodych pokoleń w poszanowaniu zarówno instytucji rządowych oraz służb, jak i ich personelu jest warunkiem koniecznym budowania świadomości społecznej w tym zakresie. Aby to mogło być możliwe działalność tych instytucji musi jednoznacznie być oceniana pozytywnie przez społeczeństwo. W tym znaczeniu istotne jest odpowiedzialne zachowanie mediów, które – po pojawieniu się określonych wątpliwości czy zarzutów – nie powinny wysuwać przedwczesnych oskarżeń wobec przedstawicieli instytucji bezpieczeństwa, jak to ma miejsce w wielu przypadkach obecnie. Jest to także istotne w kontekście przeciwdziałania celowej manipulacji o naturze hybrydowej w takich przypadkach. Czwarta władza powinna być ponadto finansowana z środków pochodzących z kapitału krajowego, nie zagranicznego, co jest nieodzownym warunkiem przeciwdziałania dezinformacji ze strony obcych państw.

Ponadto, usprawnień wymaga system działania administracji państwowej odpowiedzialnej za bezpieczeństwo narodowe, w tym przeciwdziałanie zagrożeniom hybrydowym. Kraje, które posiadają najlepiej rozwinięte siły zbrojne oraz skuteczną politykę

[592] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

bezpieczeństwa (zdolną zapewnić bezpieczny rozwój kraju w dłużej lub średniej perspektywie), co stanowi element odstraszania także potencjalnych agresorów hybrydowych, charakteryzują się silną władzą wykonawczą lub wysokim poziomem centralizacji władzy[593].

W kontekście przeciwdziałania zagrożeniom hybrydowym pojawiają się wyzwania dotyczące kwestii przekonania opinii publicznej o istniejącym zagrożeniu, sposobu odpowiedzi bez podważania demokratycznego ustroju państwowego oraz radzenia sobie z wieloma aktorami hybrydowymi zarówno państwami jak u podmiotami niepaństwowymi, o zróżnicowanej specyfice (samodzielnie oraz wraz z sojusznikami). Wybuch wojny na Ukrainie w 2022 r. spowodował, że wzrosła świadomość opinii publicznej w Polsce zagrożeniami hybrydowymi oraz konwencjonalnymi ze strony Rosji. Jednak w przypadku wyczulenia społeczeństwa na zagrożenia hybrydowe ze strony państw trzecich poza Federacją Rosyjską, świadomość ta nie jest wystarczająca.

W kontekście przejścia od zagrożeń do wojny hybrydowej warto prowadzić dalsze prace mające na celu doprecyzowanie typu zagrożeń i ich dynamiki. Wojna na Ukrainie w 2022 r. dokonała przewartościowań sytuacji w zakresie zagrożeń pozakinetycznych. Państwa zachodnie, które nie są postrzegane jako aktor hybrydowy, jeśli spojrzeć na to co dzieje się na Ukrainie (aktywność grupy hackerskiej Anonymus, ochotnicy z krajów zachodnich walczący po stronie Ukrainy, sankcje – rekwirowanie jachtów i kont bankowych osób prywatnych i prawnych) stwarza wiele nowych uwarunkowań prawno-międzynarodowych. Po zakończeniu działań zbrojnych na Ukrainie te nowe aspekty prawne mogą rodzić konsekwencje dla państw zachodnich używających po raz pierwszy wiele z opisanych rodzajów uzbrojenia, które można określić jako defensywną broń hybrydową. Reszta świata obserwuje uważnie rozwój sytuacji związanej z wojną na Ukrainie i działaniami zachodnimi.

[593] Jest tak w przypadku m.in. Stanów Zjednoczonych (kluczowa rola urzędu prezydenta), Francji (silna rola prezydenta; do roku 2000 kadencja wynosiła aż 7 lat), Rosji (minister spraw zagranicznych Siergiej Ławrow pełni obowiązki nieprzerwanie od ponad 15 lat) oraz Chin (konsolidacja władzy w ręku prezydenta Xi Jinpinga w 2022 r.). Zakładając, że osoba sprawująca władzę jest patriotycznie nastawiona, i faktycznie ma na względzie dobro rządzonych przez siebie obywateli, przedłużenie kadencji jest zaletą w kontekście planowania skutecznej obrony kraju, w tym – przeciwdziałaniu zagrożeniom hybrydowym, nie w średniej i krótkiej, ale w dłuższej perspektywie.

Casus ukraiński w postaci wojen z Rosją w 2014 r. i 2022 r. jeszcze raz udowodnił, że w przypadku nieporozumień w polityce międzynarodowej, wojna jest niestety jej przedłużeniem i spory te dany kraj (zwykle silniejszy) przy założeniu determinacji jego przywódcy – może zdecydować się rozwiązać, jak od wieków – siłowo, tzw. mieczem. Dlatego kluczowym instrumentem przeciwdziałania zagrożeniom hybrydowym powinna być wiarygodna polityka odstraszania, którą można zapewnić przez wzmocnienie potencjału obronnego państwa. Jak wykazały wyniki badań, wojna Rosji z Ukrainą w 2022 r. ukazała, że zagrożenia hybrydowe nie były największym wyzwaniem dla władz w Kijowie. Natomiast stanowiły one ważny element osłabiania przeciwnika przed atakiem rosyjskim. W tym kontekście, przeciwdziałanie zagrożeniom hybrydowym powinno dotyczyć przede wszystkim wzmacniania potencjału obronnego państwa, którego siła będzie miała działanie odstraszające. Natomiast w przypadku gdyby doszło jednak do konfliktu, potencjał obronny państwa jest jedynym pewnym zabezpieczeniem, które może zostać zastosowane (ze wsparciem wystarczających i odpowiednio wcześnie wysłanej pomocy sojuszników lub bez niej). Działania mające na celu zbudowanie odporności społeczeństwa i instytucji państwa na różnego typu działania hybrydowe (cyberataki, dezinformacja, działania grup dywersyjnych, sabotaże), powinny być realizowane, ale ze świadomością, iż są one uzupełnieniem. Podstawowym podejściem strategicznym do przeciwdziałania zagrożeniom hybrydowym powinno być bowiem odstraszanie na bazie potencjału obronnego państwa: konwencjonalnego i niekonwencjonalnego.

Zasadna jest intensyfikacja roboczych kontaktów między polskimi ekspertami do spraw dezinformacji i zagrożeń hybrydowych z przedstawicielami zagranicznych, sojuszniczych ośrodków analitycznych, m.in. Ośrodka Studiów Wschodnich czy Polskiego Instytutu Spraw Międzynarodowych. Polska powinna czynić wysiłki na rzecz zwiększenia stałego zatrudnienia polskich ekspertów w międzynarodowych instytucjach zajmujących się przeciwdziałaniem zagrożeniom hybrydowym takim jak np. Europejskie Centrum Doskonalenia w Zakresie Przeciwdziałania Zagrożeniom Hybrydowym w Helsinkach **(**Hybrid CoE**).** Ważny jest też dalszy rozwój współpracy na szczeblu eksperckim oraz pogłębianie wymiany wiedzy za pomocą m.in. wizyt studyjnych. W wyniku przeprowadzonych badań stwierdzono, że Hybrid CoE zajmuje się analizowaniem bieżących wyzwań, wśród których w 2022 r. zidentyfikowano m.in. kwestię instrumentalizacji

migracji, percepcje wojny na Ukrainie, możliwe scenariusze rozwoju sytuacji na wschodzie Europy, działania Rosji ukierunkowane na złamanie jedności UE oraz manipulacje informacjami i podatność społeczeństw na dezinformację. W 2022 r. w Hybrid CoE reprezentowanych było 31 państw członkowskich UE i NATO, które wnoszą roczną opłatę w wysokości 60 tys. euro. Resztę kosztów instytucji pokrywa rząd fiński. Centrum, którego budżet to prawie 4 miliony euro, zatrudniało 37 pracowników (15 osób wysłanych zostało przez państwa członkowskie w ramach oddelegowania). Polska była reprezentowana przez jednego eksperta. Jeśli chodzi o merytoryczne funkcjonowanie Centrum, działa ono w oparciu o trzy tzw. Wspólnoty Interesów (*Community of Interest* – COI). Zajmują się one badaniem wpływów hybrydowych, podatności i odporności oraz strategii i obrony. COI obejmują sieci ekspertów z państw uczestniczących, także z UE i NATO i zapewniają przestrzeń dla wielonarodowej i wielodyscyplinarnej wymiany najlepszych praktyk, doświadczeń i wiedzy specjalistycznej w taki sposób. Celem jest umożliwienie państwom i organizacjom uczestniczącym lepsze zrozumienie i przeciwdziałanie zagrożeniom hybrydowym. COI stanowią również przestrzeń do koordynacji działań. Ponadto, w ich ramach działają dwa zespoły ds. Badań i Analiz oraz Organizacji Szkoleń i Ćwiczeń. Jak wykazały wyniki badań, współpraca z Centrum powinna być jeszcze bardziej intensywnie rozwijana przez instytucje administracji rządowej RP oraz polskie *think-tanki*, które mogłyby wpływać na tematykę pogłębionych analiz opracowywanych przez Centrum w kierunku korzystnym dla poprawy systemu przeciwdziałania zagrożeniom hybrydowym w Polsce (badanie najważniejszych z punktu widzenia Polski kwestii).

5.3. Ekspercka ocena zaproponowanych rozwiązań w zakresie poprawy sposobów przeciwdziałania zagrożeniom hybrydowym

Realizując ekspercką ocenę zaproponowanych sposobów poprawy sposobów przeciwdziałania zagrożeniom hybrydowym do uczestniczących w sondażu ekspertów zwrócono się z następującymi pytaniami.

1. Czy zgodzi się Pan / Pani z tezą, że najlepszym sposobem przeciwdziałania zagrożeniom hybrydowym jest: (a) wzmacnianie zdolności odstraszania państwa w postaci rozbudowy jego konwencjonalnego potencjału obronnego (armia, służby i siły specjalne oraz inne formacje, obowiązkowe przeszkolenie i służba wojskowa, rozwój nowoczesnych systemów uzbrojenia –

głównie przez firmy krajowe), a także – (b) potencjału niekonwencjonalnego (pozyskanie defensywnych zdolności nuklearnych i/lub innej broni masowego rażenia) przy wytworzeniu mechanizmów sprzyjających uzyskiwaniu politycznego konsensusu w zakresie prowadzenia spójnej, długoterminowej i pozbawionej poważnych sporów wewnętrznych polityki zagranicznej oraz bezpieczeństwa i obrony (np. rozważenie wzmocnienia kompetencji i wydłużenia kadencyjności władzy wykonawczej)?

2. Czy w Pana / Pani ocenie aktywne przeciwdziałanie aktualnym oraz potencjalnym zagrożeniom hybrydowym powinno dotyczyć (a) udoskonalenia państwowych systemów reagowania na zagrożenia hybrydowe (lepsza koordynacja, efektywne zdolności przeciwdziałania atakom z użyciem migrantów, dezinformacji, jednoczące społeczeństwo kampanie informacyjne) oraz (b) zabezpieczenia trwałych partnerstw i sojuszy międzynarodowych dających realne gwarancje, a może istnieją też inne sposoby korzystne zwłaszcza z perspektywy krajów małych i średnich znajdujących się w otoczeniu międzynarodowym o wysokim ryzyku napięć miedzy krajami bądź ich blokami (jak w przypadku Polski – geograficznie położonej obecnie na linii konfrontacji ideologicznej i zbrojonej między Zachodem i Wschodem)?

Jak wykazały wyniki przeprowadzonych badań, zaproponowane sposoby poprawy sposobów przeciwdziałania zagrożeniom hybrydowym zostały w dużym zakresie pozytywnie ocenione przez ekspertów-praktyków.

W odpowiedzi na pierwsze pytanie, Ryszard Jakubczak, zgodził się z jego drugą częścią – wariantem „b" dotyczącym celowości przeciwdziałania zagrożeniom hybrydowym przez wzmocnienie potencjału niekonwencjonalnego (pozyskanie defensywnych zdolności nuklearnych i/lub innej broni masowego rażenia). Kiedy będą trudności międzynarodowe w zakresie pozyskania opisanych zdolności, co zwykle ma miejsce z bronią jądrową, to pierwszy wariant („a" – wzmacnianie zdolności odstraszania w postaci rozbudowy jego konwencjonalnego potencjału obronnego) jest wręcz obowiązkowy i powinien zostać wdrożony natychmiastowy – niezależnie co będzie można uczynić w kwestii pierwszego rozwiązania.

Jeśli chodzi o odpowiedź na drugie pytanie, R. Jakubczak ocenił, że – w przypadku Polski – celowym jest drugie z zaproponowanych w tym pytaniu rozwiązań (b) czyli zabezpieczenie trwałych partnerstw i sojuszy międzynarodowych dających realne gwarancje wsparcia w zakresie przeciwdziałania zagrożeniom hybrydowym. Należy je – jak ocenił ekspert – pogłębiać, gdyż jako państwo średniej wielkości, położone pośród dwu „gangsterów”[594], jedynie własnym potencjałem może nie sprostać potrzebom skutecznej obrony przed Niemcami i Rosjanami. Jednak wiedząc, że każdy sojusz może być zawodny – jak doświadczenie historyczne mieszkańców Polski „doświadczyło”, a i sztuka wojenna na to wskazuje (C. Clausewitz, *O wojnie*, Lublin 1995, *Księga VI*, rozdział VI: *Zakres środków obrony,* ss. 443-450 – należy mieć na względzie także rozwiązanie „a” (udoskonalenie państwowych systemów reagowania na zagrożenia hybrydowe).

Przedstawiona przez uczestniczącego w badaniu eksperta-praktyka konkluzja w kontekście obu pytań zadanych w kwestionariuszu jest następująca. Otóż one nie stanowią w cząstkowej wersji ich treści alternatywę względem siebie, czyli jeśli „a”, to już nie „b” – chociaż można i tak je traktować. Bowiem zarówno „a” jak i „b” są godne do podjęcia na rzecz wzmocnienia systemu bezpieczeństwa państwa. A nawet – w ocenie R. Jakubczaka – mogą być jednocześnie zasadne. Jednak na bazie propozycji zawartych w pytaniach można pokusić się na ustawienie ważności (wagi dla rozwiązania problemu) i możliwości podjęcia działań „przeciwhybrydowych” (przeciw działaniom hybrydowym potencjalnego agresora). Czyli co pierwsze ma być realizowane i dlaczego, a następnie też inne proponowane działanie też mieć na względzie w drugiej kolejności (dlaczego).

Realizując sugestie zawarte w odpowiedziach badanych ekspertów, w przypadku państw małych i średnich zasadne jest wskazanie priorytetów w zakresie doboru i harmonogramu wdrażania działań przeciwhybrydowych. Wejście do organizacji ochrony zbiorowej, takich jak NATO, jest na początku najważniejszym elementem wzmocnienia zdolności odstraszania danego kraju – zwłaszcza dysponującego ograniczonym potencjałem politycznym, gospodarczym i wojskowym. Ponadto, akcesja do sojuszu obronnego jest zasadna zwłaszcza w sytuacji państw graniczących lub znajdujących się w bliskości geograficznej potęg militarnych (Rosja) i/lub gospodarczo-technologiczno-politycznych –

[594] „Jest oczywistym faktem, że Polacy żyją otoczeni przez europejskich gangsterów, że aspołeczne posunięcia sąsiadów pozbawiły ich możliwości spokojnego niepodległego bytu”. N. Davis, *Boże igrzysko*, Kraków 1999, s. 1080.

które, przy sprzyjających okolicznościach zewnętrznych, mogą stosunkowo szybko przekształcić się ponownie w potęgi militarne, jak to już wielokrotnie miało miejsce w przeszłości (Niemcy). Po pomyślnym zakończeniu kwestii akcesji i staniu się pełnoprawnym członkiem danej organizacji obrony kolektywnej dane państwo powinno bezzwłocznie rozpocząć prace nad wzmocnieniem autonomicznego potencjału obronnego – najpierw konwencjonalnego, a później, jeśli faktywnie wzmocni to ich zdolności obronne – także niekonwencjonalnego. Wejście do sojuszu obronnego, zwłaszcza tak potężnego jak Pakt Północnoatlantycki, nie powinno jednak wstrzymywać procesów wzmacniania zdolności obronnych danego kraju, ale – wprost przeciwnie – przyspieszać je (skoro akcesja zakończyła się sukcesem – władze przerzucają zasoby i siły polityczne na usprawnieniu wewnętrznego potencjału obronnego). Kwestia ta dotyczy także rozbudowy własnego przemysłu obronnego, co – po ewentualnych zakupach sprzętu ad hoc od sojusznika wiodącego (najsilniejszy militarnie kraj danej organizacji) lub od kilku sojuszników – powinno stać się jednym z pilnych zadań. Tymczasem, w przypadku wielu krajów, po zabezpieczeniu akcesji do organizacji sojuszniczej, ich władze nie podejmują dodatkowych działań wzmacniających potencjał obronny, a często wręcz go osłabiają pozostając w mylnym przeświadczeniu o gwarancjach bezpieczeństwa zapewnianego przez deklarację wspólnej obrony sojuszniczej (taką deklaracją jest m.in. art. 5 Traktatu Waszyngtońskiego tworzącego NATO).

W odpowiedzi na pytanie pierwsze i zaproponowane rozwiązanie przeciwhybrydowe w postaci wzmacniania zdolności odstraszania państwa (rozbudowa jego potencjału konwencjonalnego i niekonwencjonalnego, Damian Szlachter uznał, że taki optymistyczny scenariusz jest możliwy tylko bardzo krótkofalowo. Jedynie europejskie państwa nordyckie, są w stanie wytworzyć konsensus polityczny wobec polityki bezpieczeństwa i polityki zagranicznej w perspektywie dłuższej niż jedną kadencję. Tylko tam, w jego ocenie, jest to możliwe z uwagi na dojrzałość tamtejszego społeczeństwa obywatelskiego, tradycji państwowości, czy choćby z powodu kodu kulturowego narodów północnej Europy.

Ponadto, jak zauważył ekspert, kraje prowadzące dziś międzynarodowe działania hybrydowe wobec państw Zachodu, czyli Rosja, Chiny czy Iran nie wstrzymują swoich operacji wobec m.in. USA, Francji czy Wielkiej Brytanii. Potencjał militarny nie odstrasza służb specjalnych, które są architektami współczesnych działań hybrydowych. W opinii

D. Szlachtera, tym co odstrasza przed konfrontacją na polu militarnym jest efekt synergii wymienionych w pytaniu pierwszym czynników połączonych ze sprawnym systemem zarządzania bezpieczeństwem państwa, posiadanym potencjałem gospodarczym, wielością źródeł pozyskiwania energii, elastycznością gospodarki, którą można łatwo przestawić na tryb wsparcia wojska. Ekspert zwrócił także uwagę, że nie jest należycie doceniana rola sprawnej legislacji w konstytucyjnym podziale władzy czy koordynacja na poziomie działań operacyjnych lub w łańcuchu dowodzenia w sytuacjach kryzysowych o charakterze narodowym. Jeśli zachowanie ciągłości działania państwowości i ciągłości dostarczania kluczowych dla bezpieczeństwa jego obywateli usług zależy od jednego obiektu znajdującego się w kwadracie 3 km^2 to realne zdolności odstraszania danego kraju są iluzoryczne.

W odpowiedzi na pytanie drugie, średniej wielkości podmioty państwowe, które chcą realnie zwiększyć swoją odporność na działania hybrydowe, powinny – w opinii D. Szlachtera – przestać liczyć i uzależniać się od wsparcia sojuszników, a tworzyć swoje zasoby do tego celu. Dla Polski takim ciekawym punktem odniesienia powinny być kraje nordycki. Skoro władze inwestują miliardy złotych w sprzęt wojskowy, który dotrze do nas częściowo w ciągu 3 do 5 lat to ten okres jest po to by tak zaprojektować system dowodzenia, zbudować system pozyskiwania danych poprzez rozpoznanie i działania służb specjalnych, przygotować całe wsparcie logistyczne i środowisko serwisowe, wdrożyć rozwiązania prawne które skracają czas na reagowanie kryzysowe i połączyć potencjał cywilny z militarnym.

Ponadto, trzeba będzie także wreszcie zmierzyć się z największym zaniechaniem po 1989 r. w zakresie bezpieczeństwa państwa, czyli zbudować wielowarstwowy i niejawny system łączności satelitarnej, komórkowej i radiowej na potrzeby administracji państwowej czy wojska. Radzimy sobie coraz lepiej z dezinformacją bo budujemy system od zera w którym uczestniczy administracja cywilna, wojskowa oraz prężne na tym polu ośrodki akademickie czy organizacji społecznych. W tym wypadku wykorzystujemy optymalnie posiadane zasoby, ale wciąż kulą u nogi jest legislacja – nieadekwatna do wyzwań współczesnych czasów. Polska powinna kierować się dewizą: „Chcesz zbudować silny opór na działania hybrydowe, najpierw zacznij od przygotowania systemu prawnego i ekosystemu oddolnych inicjatyw społecznych wspieranych przez środki z budżetu państwa (bez patologii

faworyzowania „swoich”).” Obecna sytuacja pozostawia wiele rozwiązań, które de facto nie sprzyjają wzmocnieniu przeciwdziałania zagrożeniom hybrydowym, np. w postaci penetracji polskiego życia politycznego, gospodarczego i naukowo-badawczego przez obce służby specjalne. Jakiego kraju boi się „nielegał”, który za działania szpiegowskie na terenie danego kraju ryzykuje wyrok skazujący zaledwie w wysokości maksymalnie od 5 do 7 lat więzienia? Władze Polski mogą kupować uzbrojenie (m.in. Kraby, Langusty, Leopardy itd.), ale to nie da państwu przewagi jeśli w sytuacji kryzysowej nie będzie dla tego sprzętu paliwa, części zamiennych, informacji o sabotażu dróg i mostów którymi będą transportowane, a przede wszystkim – jeśli nie będzie z nimi łączności i szansy na przekazanie ich załogom rozkazów.

W odpowiedzi na pierwsze pytanie, dr Jarosław Cymerski zauważył, że współczesny świat nacechowany jest szeregiem zagrożeń bezpieczeństwa zarówno w aspekcie zewnętrznym (międzynarodowym) i wewnętrznym (krajowym), militarnym i pozamilitarnym. Powstają one na płaszczyznach wielu dziedzin życia. Istotny wpływ na kształtowanie środowiska bezpieczeństwa ma postępująca globalizacja doprowadzając do daleko idących przemian społecznych, wzrostu rozwoju technologicznego, zmian kulturowych. Prowadząc ludzkość w kierunku kolejnych etapów rozwoju cywilizacyjnego, w ocenie eksperta, wprowadza nas jednocześnie w nowe odsłony form zagrożeń. W postępujących przemianach należy dostrzegać wiele pozytywów, ponieważ zarówno przepływ myśli, rozwój ludzkiego kapitału, oraz współczesnej technologii w skali globalnej wpływają pozytywnie na wiele obszarów, czy też tych regionów świata, które w innych okolicznościach nie miałyby możliwości na przemiany i dalszy rozwój. Poza pozytywną jest – zdaniem J. Cymerskiego – jednak druga strona zjawiska. Przemiany doprowadzają też do rozprzestrzenienia się zjawisk negatywnych, takich jak kryzysy polityczne, gospodarcze, terroryzm, cyberzagrożenia, przestępczość zorganizowana, handel ludźmi, narkomania i rozprzestrzeniających się wprost proporcjonalnie rozwojem cywilizacyjnym. Niewątpliwie współcześnie zagrożenia hybrydowe stanowią wyzwanie dla podmiotów systemu bezpieczeństwa państwa funkcjonujących w wielu obszarach m.in. w obszarze bezpieczeństwa militarnego i bezpieczeństwa publicznego. Złożona konstrukcja systemu i zachodzące pomiędzy podmiotami zależności umożliwiają budowanie systemu bezpieczeństwa państwa charakteryzującego się następującymi zasadami:

- zasadą niepodzielności – polegającą na powiązaniu podmiotów systemu bezpieczeństwa państwa w procesie zapewnienia bezpieczeństwa;
- zasadą kompleksowości – bazującą na wszechstronności systemu bezpieczeństwa państwa;
- zasadą kooperatywności – opierającą się na wielostronnej współpracy krajowej i międzynarodowej.

System bezpieczeństwa państwa, jak wskazał J. Cymerski, należy postrzegać jako wytwór o charakterze organizacyjnym. Takie podejście pozwala na dostrzeżenie złożoności materii zjawiska, który należy traktować jako szczególny przedmiot będący realnym wytworem człowieka, którego celem jest realizacja określonych zamierzeń, przez uporządkowany zbiór elementów organizacyjnych. Zbudowany w oparciu o w/w zasady, daje rękojmie zachowania bezpieczeństwa państwa wobec dynamicznie zmieniających się zagrożeń – w tym hybrydowych. Ich specyfika łączy w sobie zagrożenia wywoływane wykorzystaniem broni konwencjonalnej i niekonwencjonalnej, dlatego też skuteczne im przeciwdziałanie i zwalczanie wymaga wielokierunkowych działań na poziomach strategicznym, operacyjnym i taktycznym o zasięgu krajowym i międzynarodowym. Opisane uwarunkowania mają tym większe znaczenie, że w działaniach hybrydowych za sprawą wykorzystania cyberprzestrzeni możliwym jest prowadzenie działań propagandowych, dezinformacyjnych oraz zbierania informacji nt. szeroko pojętych preferencji użytkowników infosfery. Dodatkowo z uwagi na rozwój współczesnych technologii zauważalne jest zjawisko wspierania działań hybrydowych narzędziami wykorzystującymi sztuczną inteligencję (Artificial Intelligence) stawiając tym samym kolejne wyzwania dla podmiotów tworzących system bezpieczeństwa.

Dlatego też biorąc pod uwagę zaprezentowany wcześniej charakter działań hybrydowych, trudno nie zgodzić się ze stwierdzeniem, że wzmacnianie zdolności odstraszania państwa w postaci rozbudowy jego konwencjonalnego potencjału obronnego jak i potencjału niekonwencjonalnego przy wytworzeniu mechanizmów sprzyjających uzyskiwaniu politycznego konsensusu w zakresie prowadzenia spójnej, długoterminowej i pozbawionej poważnych sporów wewnętrznych polityki zagranicznej oraz bezpieczeństwa i obrony (np. rozważenie wzmocnienia kompetencji i wydłużenia kadencyjności władzy wykonawczej) jest najlepszym sposobem na przeciwdziałanie zagrożeniom hybrydowym.

Zastrzec jednak należy, że zaproponowane sposoby zapewnienia sprawnego funkcjonowania mechanizmów politycznie wspierających długoterminową politykę zagraniczną oraz bezpieczeństwa i obrony takie jak wydłużenie kadencyjności władzy wykonawczej w krajach demokratycznych do których zaliczana jest Polska jest na obecną chwilę niemalże niemożliwe. Uzasadniając przedstawione stanowisko należy zaznaczyć, że przeczy to zapisom Konstytucji Rzeczpospolitej Polskiej a wprowadzenie jakichkolwiek zmiany w tym zakresie wymaga zmiany Ustawy Zasadniczej w trybie art. 235. Warto również zauważyć, że sama zmiana środowiska zagrożeń bezpieczeństwa państwa nie może stanowić podstawy do wprowadzania zmian w kadencyjności sprawowania władzy, ponieważ czym innym są przyjęte zasady funkcjonowania państwa demokratycznego a czym innym środowisko zagrożeń jego bezpieczeństwa. Oczywiście zachodzi związek pomiędzy sprawowaniem władzy i środowiskiem zagrożeń bezpieczeństwa państwa jednak ogranicza się on wyłącznie do odpowiedzialności politycznej za brak zapewnienia bezpieczeństwa państwa a co za tym idzie i jego obywatelom bez względu na środowisko zagrożeń bezpieczeństwa, które jak to podniesiono jest zmienne.

Odpowiadając na pytanie drugie, J. Cymerski stwierdził, że biorąc pod uwagę dynamikę zmian współczesnego środowiska zagrożeń bezpieczeństwa państwa ze szczególnym ukierunkowaniem się na zakres i zmienność zagrożeń hybrydowych, należy mieć na uwadze działania, które będą adekwatne i proporcjonalne do mogących wystąpić zagrożeń. W przypadku omawianych zagrożeń w ramach, których wykorzystywane są działania o zróżnicowanej specyfice, wspomniana adekwatność i proporcjonalność działań będzie polegać m.in. doborze właściwych sił i środków umożliwiających optymalne im przeciwdziałanie i zwalczanie. Dążenie do optymalnego funkcjonowania systemu bezpieczeństwa państwa wobec zagrożeń hybrydowych wymaga co już podkreślono, aktywności na wielu płaszczyznach. Płaszczyzny te swym zakresem obejmują wskazane w zadanym pytaniu działania polegające na udoskonalaniu systemów reagowania na zagrożenia hybrydowe oraz zabezpieczaniu trwałych relacji międzynarodowych poprzez budowanie sojuszy międzynarodowych. Oczywistym jest, zdaniem J. Cymerskiego, że sojusze międzynarodowe nie dają pełnej gwarancji zachowania bezpieczeństwa, ponieważ głównym celem każdego uczestnika sojuszy z politycznego punku widzenia jest zabezpieczenie własnych interesów na każdej z płaszczyzn działań (militarnej, gospodarczej

i politycznej). Dlatego ważnym jest dysponowanie własnym potencjałem zdolnym do przeciwdziałania i zwalczania zagrożeń hybrydowych z założeniem podejmowania kolejnych inicjatyw, których celem jest nie tylko wzmacnianie własnego potencjału, ale i budowanie nowych sojuszy w myśl zasady minimalizowania ryzyka poprzez dywersyfikację pól oddziaływania na zagrożenia, w tym przypadku – hybrydowe. Zatem odpowiadając na pytanie, J. Cymerski uznał, że należy podkreślić, iż tylko aktywne działanie państwa na wielu płaszczyznach daje szansę na zwiększenie realnego potencjału zdolnego do przeciwdziałania i zwalczania zagrożeń hybrydowych, co więcej, stwarza również szansę na budowanie pozycji lidera w działaniach, a tym samym wpływa na budowanie pozycji państwa na arenie międzynarodowej.

Podsumowując omówioną w odpowiedziach na zadane pytanie tematykę J. Cymerski stwierdził, że należy uznać, iż optymalnym działaniem państwa, które poprzez system bezpieczeństwa wypełnia swój obowiązek reagowania na zagrożenia jest podejmowanie wielopłaszczyznowych działań w celu wzmacniania zdolności odstraszania na zagrożenia hybrydowe. Zaprezentowane podejście jest zgodne i wpisuje się w treść wyników badań uzyskanych w procesie badawczym zawartym w rozprawie mgr Tomasza Kijewskiego pt. „Przeciwdziałanie zagrożeniom hybrydowym" wyrażających opinię, że skuteczne przeciwdziałanie zagrożeniom hybrydowym wymaga ciągłego udoskonalenia. Należy tylko dodać, że przyczyną tego stanu rzeczy jest naturalna zmienność środowiska zagrożeń bezpieczeństwa państwa.

Odpowiadając na pierwsze pytanie, dr Krzysztof Malesa, ocenił, że teza jest sformułowana przekonująco, jednak zaznaczył, iż mogłaby ona zostać rozszerzona o co najmniej jeden element, warunkujący skuteczność funkcjonowania państwa w obliczu działań hybrydowych, mianowicie o jego odporność. Zgodnie z przyjętym uchwałą Rady Ministrów Krajowym Planem Zarządzania Kryzysowego, skuteczną odpowiedzią na zagrożenia spowodowane działaniami hybrydowymi – obok potencjału obronnego i ochronnego państwa – jest wzmocnienie odporności oraz budowa zdolności do wczesnego rozpoznania i szybkiego wdrożenia działań minimalizujących negatywne skutki, również jako element odstraszania skierowany do inicjatora (agresora) tych działań. W tym celu – według K. Malesy – niezbędne jest zrozumienie mechanizmów powstawania tego typu zagrożeń, monitorowanie działań i interesów inicjatora tego typu działań, aby

w konsekwencji ocenić ryzyka wystąpienia tych zagrożeń w warunkach normalnego funkcjonowania państwa, szczególnie w obszarze gospodarczego bezpieczeństwa państwa, obronności i świadczenia usług dla ludności. Takie komplementarne podejście do budowy systemu reagowania na działania hybrydowe pozwoli, w opinii eksperta, na szybkie i efektywne reagowanie ogniw militarnych oraz pozamilitarnych w sytuacji wystąpienia tego typu zagrożeń.

Mając na uwadze sytuację np. Polski lub państw bałtyckich, które bez wątpienia są aktualnie areną działań hybrydowych w wielu obszarach środowiska bezpieczeństwa (zgodnie z segmentacją PMESII zakładającą podział potencjalnych obszarów działań hybrydowych na polityczne, militarne, ekonomiczne, społeczne, infrastrukturalne i informacyjne), K. Malesa podkreśl, że Polsce jest daleko jeszcze do militarnych przejawów działań hybrydowych, przy dość intensywnym nasileniu działań w sferze informacyjnej, ekonomicznej czy społecznej. Stąd też ekspert uznał, że kwestia odporności nie powinna być w tym kontekście pomijana, również jeśli chodzi o odporność społeczną – dość nowe pojęcie na agendzie NATO.

Jeśli chodzi o odpowiedź na drugie pytanie zawarte w kwestionariuszu, w ocenie K. Malesy, należy przede wszystkim ponownie przeanalizować i wdrożyć rekomendacje z kilku ostatnich edycji ćwiczeń NATO-CMX, w których aspekt działań hybrydowych w kontekście odstraszania był istotnym elementem scenariusza. Należy również uwzględnić wnioski z kontroli NIK z 2018 r. obejmującej w szerokim aspekcie przygotowania obronne państwa. Niezależnie od opisanych wcześniej uwag dotyczących ćwiczeń CMX, K. Malesa zauważył, że wiele obszarów bezpieczeństwa, które mogą stać się polem działań hybrydowych, to obszary dotyczące całego regionu, a nie pojedynczych państw członkowskich NATO. Przykładem takiego obszaru jest energetyka. Działania Rosjan na Bałtyku mogą zdestabilizować łańcuch dostaw energii elektrycznej w całym regionie, więc małe kraje (trzy republiki bałtyckie – 3B) nie powinny wahać się przed korzystaniem z NATOwskich instrumentów wsparcia, takich jak Counter Hybrid Support Team, który nota bene na zapotrzebowanie Litwy został wykorzystany we wrześniu 2021 r. przy narastającym kryzysie uchodźczym na granicy z Białorusią. Ta sytuacja – w opinii eksperta – pokazała, że myślenie w kategoriach regionalnych i sojuszniczej współpracy

pozwalają na skuteczne zarządzanie ryzykiem i wzmacnianie odporności na działania hybrydowe.

Podsumowując, stosunek uczestniczących w badaniu ekspertów do wypracowanych propozycji sposobów przeciwdziałania zagrożeniom hybrydowym był zgodny z wynikami badań uzyskanymi w procesie badawczym zawartym w rozprawie. Eksperci zgodzili się z tezą zawartą w pytaniu pierwszym stwierdzając, że najlepszym sposobem przeciwdziałania zagrożeniom hybrydowym jest wzmacnianie zdolności odstraszania państwa w postaci rozbudowy jego konwencjonalnego potencjału obronnego oraz potencjału niekonwencjonalnego przy wytworzeniu mechanizmów sprzyjających uzyskiwaniu politycznego konsensusu w zakresie prowadzenia spójnej, długoterminowej i pozbawionej poważnych sporów wewnętrznych polityki zagranicznej oraz bezpieczeństwa i obrony.

Eksperci wskazali również inne elementy służące poprawie przeciwdziałania zagrożeniom hybrydowym, co można wykorzystać do wskazania kierunków przyszłych działań w opisywanym obszarze. J. Cymerski zaznaczył konieczność poszukiwania dodatkowych dróg wzmocnienia jednolitej polityki państwa w zakresie przeciwdziałania zagrożeniom hybrydowym (brak możliwości wydłużenia kadencyjności władz z uwagi na obecne ograniczenia demokratyczne). Ponadto, dr K. Malesa zaznaczył, że częścią polityki odstraszania mogłyby być wzmocnienie zdolności odporności państwa na zagrożenia hybrydowe. Za ważne w tym kontekście uznał on budowę zdolności do wczesnego rozpoznania i szybkiego wdrożenia działań minimalizujących negatywne skutki zagrożeń hybrydowych, co służyłoby również jako element odstraszania skierowany do inicjatora (agresora) tych działań.

W zakresie odpowiedzi na tezy zawarte w pytaniu numer dwa, eksperci zgodzili się, że aktywne przeciwdziałanie aktualnym oraz potencjalnym zagrożeniom hybrydowym powinno dotyczyć zarówno udoskonalenia państwowych systemów reagowania na zagrożenia hybrydowe, jak i zabezpieczenia trwałych partnerstw i sojuszy międzynarodowych. Wskazując na potrzebę priorytetyzowania skuteczności doboru sposobów przeciwdziałania zagrożeniom hybrydowym, prof. R. Jakubczak wskazał na większe znaczenie zbudowania skutecznych, pogłębionych sojuszy, gdyż jako państwo średniej wielkości, położone pośród dwóch potęg regionalnych, a nawet światowych

(Niemiec i Rosji), kraj – jedynie własnym potencjałem – nie sprosta potrzebom skutecznej obrony przed Niemcami i Rosjanami. Wszyscy uczestniczący w badaniu eksperci potwierdzili wnioski, jakie wyprowadzono na podstawie badań.

5.4. Wnioski

Polityka odstraszania połączona z rozbudową potencjału obronnego państwa jest najskuteczniejszą metodą przeciwdziałania zagrożeniom hybrydowym. Największą zaletą wiarygodnych zdolności odstraszania (potencjał sił i wola ich użycia) jest to, że stwarzają one środek pozwalający zapobiec konfliktom i wojnie, które zwłaszcza dla małych i średnich państw mogą być destrukcyjne w skutkach. Zniszczenia zasobów ludzkich (ofiary wśród elity przywódczej, żołnierzy i ludności cywilnej), infrastruktury, gospodarki, oraz straty finansowe, jakie obserwuje się w czasie konfliktów zbrojnych i wojen (przykład m.in. Polski w II wojnie świtowej, Ukrainy w 2014 r. i w 2022 r.) cofają dany kraj o dekady w rozwoju cywilizacyjnym i gospodarczym. Ponadto, osłabiają warunki do jego niezależnego funkcjonowania, co pokazał przypadek przekazania Polski do radzieckiej strefy wpływów po II wojnie światowej). Utrata wiarygodności państwa w oczach przede wszystkim swoich obywateli, ale także obniżenie pozycji na arenie międzynarodowej także są istotnymi czynnikami, które skłaniają do przeciwdziałania zagrożeniom tego typu.

Jeśli chodzi o sposoby przeciwdziałania zagrożeniom hybrydowym państwa współczesne takie jak Polska mogą podjąć szereg działań, w tym zwłaszcza rozbudować siły odstraszania. Jeśli chodzi o klasycznie pojmowane odstraszanie w ujęciu wojskowym jest ono związane przede wszystkim ze zdolnościami nuklearnymi danego kraju. Jednak w zakresie odstraszania przeciwdziałania atakom hybrydowym może być wykorzystany szereg działań natury gospodarczej (sankcje), dyplomatycznej, ale także kontrataków hybrydowych, którymi można określić operacje służb specjalnych ukierunkowane na państwo agresora i mające na celu zniechęcenie go do kontynuacji ataków tego typu. Państwo broniące się powinno dokonać oceny swoich możliwości oraz rozgraniczenia wydarzeń, na które powinno się zareagować oraz takich, na które nie można lub nie warto odpowiedzieć (koszt byłby za wysoki w stosunku do zysku dla bezpieczeństwa narodowego).

W kontekście tezy, że działania hybrydowe mogą w określonych warunkach być tylko wstępem do działań zbrojnych (otwartej wojny), należy położyć nacisk na

wzmocnienie zdolności odstraszania w zakresie sił konwencjonalnych, służb oraz sił specjalnych. Zdolności te, zakładając ich wystarczającą siłę, mogą stanowić czynnik zniechęcający potencjalnych agresorów do działań hybrydowych z uwagi na ryzyko – jawnej lub skrytej – odpowiedzi ze strony państwa broniącego się. Dotyczy to zwłaszcza tak strategicznych lokacji jaką jest Europa Środkowa i Wschodnia, która od wieków jest miejscem różnych konfrontacji zbrojnych.

Posiadanie zdolności zadania skutecznego i dotkliwego w skutkach odwetu jest jedyną zaporą dla agresji hybrydowej (oraz klasycznej – zbrojnej takiej jak wojna nuklearna). Z punktu widzenia Polski, konieczne jest kontynuowanie rozbudowy odporności (dostosowanego do specyfiki potencjalnego agresora hybrydowego – ang. *tailor-made*) i podejścia kompleksowego (ang. *whole of government / whole of socjety*). Wsparcie sojusznicze ze strony NATO, UE oraz innych międzynarodowych struktur kooperacji może być uzupełnieniem, ale nie głównym i jedynym gwarantem bezpieczeństwa. Wejście do NATO w 1999 r., a potem do UE (2004 r.) spowodowało modernizację polskich sił zbrojnych oraz usprawnienie mechanizmów współpracy, ale równocześnie stanowiło w wielu przypadkach zachętę do postawy zachowawczej w zakresie stałego wzmacniania krajowych zdolności obronnych (np. likwidacja obowiązkowej służby wojskowej w 2008 r.).

Do działań bojowych natury hybrydowej państwa wykorzystują przede wszystkim służby specjalne, które mogą realizować zadania nawet poprzez nieświadomych podwykonawców czy elementy przestępcze[595]. Dlatego w zakresie przeciwdziałania operacjom hybrydowym konieczne jest odpowiednie rozbudowanie i profesjonalne wzmocnienie cywilnych i wojskowych służb specjalnych w Polsce. Utworzenie dla nich oddzielnego, niezależnego od innych rodzajów sił zbrojnych dowództwa byłoby korzystne zarówno dla ich wzmocnienia, jak i wzrostu potencjału i skuteczności działania.

Polska powinna skorzystać z niektórych doświadczeń charakterystycznych dla izraelskiego modelu organizacji sił zbrojnych, sektora zbrojeniowego, budowania sprzyjających obronie postaw społeczeństwa, a także rekrutacji i szkolenia na potrzeby obronne kraju. Izraelski model kładzie nacisk nie tylko na wzmacnianie patriotycznego nastawienia obywateli (co w ostatnich latach miało miejsce także w Polsce), ale zapewnia

[595] Omówienie przypadków aktywności rosyjskiego wywiadu wojskowego przedstawiono w raporcie dla Kongresu USA w 2021 r. Więcej: A. S. Bowen, *Russian Military Intelligence: Background and Issues for Congress,* November 15, 2021 https://sgp.fas.org/crs/intel/R46616.pdf [dostęp: 13.08.2022].

konkretne instrumenty umożliwiające przygotowanie społeczeństwa do aktywnej obrony. Wspierane jest to zdolnością do szybkiej mobilizacji ludności, co – w połączeniu z jej wysokim poziomem wyszkolenia oraz uzbrojenia – może stanowić realną strategię odstraszania. Podejście Izraela do bezpieczeństwa i obrony – po odpowiednim zaadaptowaniu – może stanowić korzystny wzorzec usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym i innym dla państwa małego lub średniego takiego jak Polska. Ma to odniesienie do samodzielnej operacji obronnej danego kraju przy założeniu, że wsparcie sojusznicze może nie być udzielone natychmiast i w sile wymaganej dla skutecznej obrony kraju. Dodatkowym czynnikiem zwiększającym zagrożenie dla danego kraju jest jego położenie. W sytuacji napięć między Paktem Północnoatlantyckim i Rosją / Białorusią, członkowie NATO położeni na wschodniej flance tej organizacji są narażeni bardziej na potencjalny atak hybrydowy, niż kraje leżące w głębi terytorium Sojuszu.

W celu poprawy zdolności odstraszania Polska powinna doprowadzić do zwiększenia liczebności, wyposażenia i wyszkolenia armii oraz przywrócić i udoskonalić powszechne przeszkolenie wojskowe obywateli. Izrael ma siły zbrojne liczące 187 tys. plus 500 tys. szkolonych regularnie rezerwistów. Odnosząc się do przykładu Izraela, proporcjonalnie do liczby ludności, polskie siły zbrojne powinny liczyć, co najmniej 500 tys. żołnierzy oraz 1,5 miliona aktywnej rezerwy. Częścią wzmacniania sił zbrojnych powinno być zwiększenie możliwości i profesjonalizacji służb i sił specjalnych oraz usprawnienie ich koordynacji działania z innymi formacjami mundurowymi w kraju i za granicą. Ponadto, konieczne są działania mające na celu rozbudowanie potencjału krajowego przemysłu obronnego.

Uzupełnieniem głównej strategii przeciwdziałania zagrożeniom hybrydowym w postaci odstraszania, powinno być wzmocnienie odporności instytucji państwowych i społeczeństwa w sytuacji potencjalnego ataku tego typu. Działania w tym zakresie powinny być prowadzone na różnych płaszczyznach. Jednym z istotnych wymiarów przeciwdziałania zagrożeniom hybrydowym jest rozwój wolnych mediów w Polsce i innych krajach zachodnich, co pomoże wzmocnić odporność państw członkowskich NATO na dezinformację.

W kontekście wzrostu liczby i poziomu złożoności zagrożeń w cyberprzestrzeni, istotne jest opracowanie systemu funkcjonowania państwa pozwalającego na realizowanie

podstawowych, kluczowych z punktu wodzenia bezpieczeństwa funkcji bez dostępu do sieci. Podobnie powinno się podejść do szkoleń sił zbrojnych, które muszą być w stanie działać także w sytuacji braku np. dostępu do globalnej sieci satelitarnej GPS i lokalizacji (doskonalenie neutralizacji zagrożeń w sytuacji braku ułatwionej geolokalizacji prowadzą m.in. USA). Jak pokazały wyniki przeprowadzonych badań, nie powinno się przeceniać znaczenia kwestii cyberbezpieczeństwa kosztem całościowego przygotowania państwa do odparcia ataku: hybrydowego i konwencjonalnego (wojna). W konflikcie rosyjsko-ukraińskim w 2022 r. elementy cybernetyczne zostały przyćmione przez wojnę konwencjonalną, która skupiła na sobie uwagę wszystkich stron zaangażowanych w działania zbrojne. Rosja w początkowej fazie wojny nie zastosowała dewastujących cyberataków wobec ukraińskiej infrastruktury cyfrowej Ukrainy, ponieważ zależało jej na utrzymaniu jej operacyjności dla własnych potrzeb w przyszłości (po ewentualnym zajęciu tego kraju). Motywem takiego działania, zdaniem niektórych ekspertów zachodnich, mogła być także próba pozyskiwania informacji z tej sieci (usługi cyfrowe na Ukrainie są dostarczane m.in. przez podmioty rosyjskie)[596].

W zakresie zwalczania zagrożeń hybrydowych Polska musi być przygotowana na ich eskalację w postaci przede wszystkim nasilonego wykorzystania imigrantów jako żywej broni, manipulacji rynkiem energii, prób destabilizacji ekonomicznej i ataków w cyberprzestrzeni (na elementy infrastruktury krytycznej, administracji rządowej i sektora finansowego, ochrony zdrowia, wojska oraz służb bezpieczeństwa).

Obszar, w którym powinno się podjąć działania to m.in. relacja UE-NATO, która wymaga daleko idących usprawnień. UE, poprzez swoje kraje członkowskie, ma znacznie szersze możliwości przeciwdziałania zagrożeniom poniżej progu wojny, takimi jak zagrożenia hybrydowe. W interesie krajów NATO jest czerpanie z tych doświadczeń np. w zakresie koordynacji sankcji wymierzonych w hybrydowego agresora.

[596] *The Challenges of European Cybersecurity*, European Security and Defence College / National Defence Institute (Portugalia), seminarium online, 26-30 września 2022 r.

Zakończenie

W świetle wyników przeprowadzonych badań należy stwierdzić, że zagrożenia typu hybrydowego były i nadal są rzeczywistością, z którą trzeba się liczyć we współczesnym środowisku bezpieczeństwa. Ataki hybrydowe nie są niczym innym, jak prowadzeniem wojny bez jej formalnego wypowiedzenia – metodami niejawnymi lub trudnymi do zidentyfikowania. W tym kontekście podjęcie działań zwalczających przypadki agresji hybrydowej (dezinformacja, sabotaż itp.) jest koniecznością i powinno być priorytetem władz. Tym bardziej, że przykład Ukrainy pokazuje, że działania hybrydowe mogą (i zwykle są w istocie) wstępem do podporządkowania sobie danego kraju: bezpośredniego (aneksja) lub też w sposób pośredni – na przykład przez włączenie go do swojej strefy wpływów poprzez sprzyjających krajowi agresora polityków lub całe przywództwo państwa (przykład ZSRR i krajów satelickich).

Doświadczenie Izraela w zakresie wielokierunkowego wzmacniania sił zbrojnych oraz dostosowywania strategii obronnej zasługuje na uwagę i przestudiowanie pod kątem ewentualnego wykorzystania go do usprawnienia działań mających na celu przeciwdziałanie zagrożeniom hybrydowym oraz innym rodzajom zagrożeń dla bezpieczeństwa narodowego w Polsce. Izraelski model organizacji armii oraz systemu obrony państwa, zwłaszcza patriotycznego nastawienia oraz przygotowania społeczeństwa do aktywnej obrony (co ma zdolności odstraszania) jest niezwykle korzystny w przypadku przemyślanego i odpowiedzialnego budowania skutecznej strategii obrony państwa małego lub średniego takiego jak Polska (w operacji samodzielnej lub przy założeniu, że wsparcia sojuszniczego – jak pokazują fakty historyczne – nie można zakładać za pewnik, a w każdym razie – nie będzie ono udzielone natychmiast i w sile wymaganej dla skutecznej obrony kraju).

Jak dowiodły badania, przykład Izraela, którego państwowość kształtowała się w specyficznych, bardzo wymagających i niepewnych uwarunkowaniach, pokazuje znaczenie odstraszania w celu zapewnienia bezpieczeństwa narodowego. Podczas gdy wiele państw, w tym – najpotężniejszy militarnie kraj NATO – Stany Zjednoczone, inwestuje w podobne działania, Izrael jest wyjątkowy pod względem umieszczania odstraszania w centrum swojej strategii przeciwdziałania zagrożeniom hybrydowym (w tym – terrorystycznym).

Polityka odstraszania posiada pewne ograniczenia i czasem interwencja zbrojna może stanowić jedyny sposób przeciwdziałania zagrożeniu. Izrael prowadzi politykę odstraszania względem przywódców Hamasu w Strefie Gazy, ale, jak zauważył Benjamin Netanjahu w maju 2021 r., jeśli wymierzone w Izrael ataki rakietowe nie ustaną, nie można wykluczyć ostatecznego podboju palestyńskiej enklawy. Izraelski premier odnosząc się do muzułmańskich bojowników stwierdził, że można „ich podbić – i to zawsze jest otwarta możliwość – albo możesz ich powstrzymać[597]".

Polska powinna skorzystać z niektórych doświadczeń charakterystycznych dla izraelskiego modelu rekrutacji i szkolenia na potrzeby obronne kraju. W celu poprawy zdolności odstraszania Polska, biorąc pod uwagę przebieg wydarzeń historycznych w XX i XXI w. powinna w pierwszej kolejności wzmocnić swój potencjał obronny, co będzie miało także wartość odstraszającą. Wsparcie sojusznicze, jakkolwiek bardzo cenne, należy traktować jako uzupełnienie, a nie podstawę doktryny obronnej.

Przygotowanie do obrony ojczyzny to obowiązek całego społeczeństwa, a nie tylko ograniczonej liczebnie grupy żołnierzy sił zawodowych. Polska powinna doprowadzić do zwiększenia liczebności armii. Izrael ma siły zbrojne liczące ponad 170 tys. żołnierzy (około 70% z poboru) plus prawie 500 tys. szkolonych regularnie rezerwistów. Odnosząc się do przykładu Izraela, proporcjonalnie do liczby ludności (cztery razy więcej w Polsce), polskie siły zbrojne powinny liczyć, co najmniej 680 tys. żołnierzy oraz 2 miliony aktywnej – czyli przechodzącej regularne szkolenia bojowe – rezerwy (mającej za sobą 2-3 lata obowiązkowej służby wojskowej). W ramach tej reformy powinno się znacznie rozbudować zarówno polskie siły jak i służby specjalne zdolne do działania poza granicami i realizowania skutecznych, zgodnych z polską racją stanu operacji odstraszających różnego rodzaju (także niesymetrycznych, np. atak kinetyczny jako odpowiedź na poważne ataki hybrydowe zagrażające bezpieczeństwu narodowemu: bytowi państwa i jego obywateli.

Pozostawanie przez Polskę frontowym krajem NATO oraz analiza skutków inwazji rosyjskiej na Ukrainie (wyniszczenie zasobów materialnych państwa na czele z ludnością) przemawiają także za rozważeniem pilnego rozwoju krajowego cywilnego i wojskowego sektora nuklearnego, a wcześniej – oficjalne lub dokonane innymi kanałami – pozyskanie

[597] *Netanyahu says Israel could 'conquer' Gaza if 'deterrence' not achieved,* The Times of Israel, 19 May 2021 https://www.timesofisrael.com/netanyahu-says-israel-could-conquer-gaza-if-deterrence-not-achieved/ [dostęp: 5.12.2022].

defensywnej broni nuklearnej, która miałaby potencjał odstraszający. Zahamowanie rozwoju cywilnego sektora energetyki nuklearnej w Polsce przez rząd premiera Tadeusza Mazowieckiego w 1989 r. oraz brak wymiernych efektów na tym polu przez ponad 30 następnych lat, należy ocenić w tym kontekście przynajmniej, jako ogromne zaniedbanie. Wstrzymano rozpoczętą już budowę elektrowni jądrowej w Żarnowcu (zaawansowanie budowy wynosiło 36%, obiekty zaplecza wykonano w 85% wznosząc ich ponad 630, w budowę było zaangażowanych około 70 firm krajowych i 9 przedsiębiorstw zagranicznych), co przyniosło straty rzędu 2 miliardów USD. Równie niekorzystny efekt dla odstraszającego potencjału obronnego Polski miała likwidacja obowiązkowej służby wojskowej, czterokrotne zmniejszenie polskiej armii oraz brak rozwoju adekwatnych do zagrożeń, krajowych systemów uzbrojenia defensywnego (m.in. obrony powietrznej)[598]. Czynnik nuklearny jest bardzo istotny. Zastosowanie przez Rosję groźby użycia broni nuklearnej stanowiło przykład zastosowania techniki wprowadzającej zamieszanie i niepewność w procesie decyzyjnym państw wspomagających Ukrainę i niewątpliwie ograniczyło zakres i tempo wsparcia udzielonego temu krajowi. Gdyby Ukraina posiadała broń jądrową, władze w Moskwie musiałyby uwzględnić to ograniczając swój szantaż atomowy.

Polska, jak wykazały wyniki badań, od lat jest celem ataków informacyjnych, m.in. ze strony Federacji Rosyjskiej. Powtarza się propagowanie zarzutów o rzekomy rasizm, agresywną politykę zagraniczną pod dyktando wrogiego Rosji Zachodu i zamiar dokonania nabytków terytorialnych kosztem Ukrainy. Aby sprostać wyzwaniu obrony przed zagrożeniami hybrydowymi tego typu Polska powinna wzmocnić służby państwowe odpowiedzialne za przeciwdziałanie dezinformacji oraz ściśle i efektywnie zabiegać u sojuszników o adekwatne do sytuacji wsparcie: oficjalne lub zakulisowe. Przykład braku stosownej reakcji, na odpowiednim szczeblu politycznym w przypadku zarzutów Rosji pod adresem Polski o rzekome doprowadzenie do II wojny światowej jest tu znamienny.

Szybkie i zdecydowane reagowanie w grupie bratnich państw na ataki informacyjne oraz stała współpraca prewencyjna z państwami sojuszniczymi powinny być zdecydowanie

[598] G. Jezierski, *Kalendarium budowy elektrowni jądrowej w Żarnowcu, czyli... jak straciliśmy swoją szansę?* Gigawat Energia 30.01.2006, https://web.archive.org/web/20110716074324/http://gigawat.info/archiwum/article/articleview/667/1/60/index.html dostęp: 31.12.2022 r.

wzmocnione. Mimo rozbieżności w wewnętrznej polityce UE i – w mniejszym stopniu w NATO – działania wspierające Polskę powinny być zdecydowanie wzmocnione. Powinno to przejawiać się zarówno w zwiększonej ilości żołnierzy amerykańskich na terytorium Polski, jak i prowadzeniem polityki wspierającej modernizację i wzmacnianie sił zbrojnych przez flankowe kraje członkowskie NATO. Poprzez odpowiednią politykę, Polska powinna skłonić państwa położone wewnątrz terytorium NATO, takie jak Niemcy do większej solidarności z władzami w Warszawie, zwłaszcza w sytuacji wojny u granic Paktu, jak miało to miejsce w 2022 r. (wojna Ukrain-Rosja).

Aby skutecznie przeciwdziałać dezinformacji, jak wykazały wyniki badań, pozycję Polski mogą poprawić m.in. wspólne, międzysojusznicze konferencje na wysokim szczeblu, briefingi dla mediów, newslettery czy artykuły publikowane w opiniotwórczych mediach, które powinniśmy realizować we współpracy z podobnie myślącymi państwami. Przekaz informacyjny z Polski powinien być częściej wzmacniany przez przedstawicieli któregoś z sojuszniczych krajów natowskich – będących także w G7 – jest jedyną szansą na to, że narracja Warszawy przebije się przez dezinformacje uważanej za jedną z najlepszych na świecie, doświadczonej dyplomacji stałego członka Rady Bezpieczeństwa ONZ jakim jest Rosja. Warto jednak pamiętać, że rozbudowana machina propagandowa Federacji Rosyjskiej, która – w wielu aspektach problemowych i geograficznych – posiada przynajmniej nieformalne wsparcie Chin, także ewoluuje, szybko uczy się na błędach oraz nieustannie poszukuje słabych punktów przeciwnika. Polska powinna, więc zachować czujność i ogromne zaangażowanie w kontrowaniu rosyjskich narracji w mediach.

W Polsce powinno powstać centrum analityczno koncepcyjne, które byłoby ukierunkowane na przeciwdziałanie zagrożeniom hybrydowym, ale także miałoby kompetencje w kwestii przedstawiania Sejmowi oraz rządowi rekomendacji dotyczących szerszego wymiaru bezpieczeństwa narodowego w ujęciu długoterminowym. Ośrodek taki (np. pod nazwą: „Stała Rada Bezpieczeństwa RP") byłby finansowany z pieniędzy publicznych ale powinien on być niezależny od wpływów politycznych i zmieniających się często w Polsce ekip rządowych (a co za tym idzie – koncepcji bezpieczeństwa i obrony). Na potrzebę takiego rozwiązania wskazuje przykład braku stworzenia skutecznej obrony powietrznej kraju, co dobitnie potwierdził przypadek braku reakcji defensywnej w sytuacji wtargnięcia w polską przestrzeń powietrzną wystrzelonego przypadkowo przez Ukrainę

(broniącą się przed atakami strony rosyjskiej) pocisków i ich uderzenie na terytorium RP, w Przewodowie w 2022 r.

W Czechach w 2017 r. powołano Centrum przeciwko Terroryzmowi i Zagrożeniom Hybrydowym, które jest zasilane przy wykorzystaniu aktualnego budżetu czeskiego MSW. Ta wyspecjalizowana jednostka analityczna i komunikacyjna zajmuje się monitorowaniem zagrożeń związanych bezpośrednio z bezpieczeństwem wewnętrznym obejmując – pośrednio lub bezpośrednio wiążące się z przeciwdziałaniem zagrożeniom hybrydowym – incydenty związane z migracjami, bezpieczeństwem zgromadzeń publicznych, terroryzmem i ekstremizmem, ale także z dezinformacją.

Wykorzystując monitoring zagrożeń centrum dokonuje oceny wyzwań i przedstawia opcje rozwiązań merytorycznych i legislacyjnych, które będą wdrożone tam, gdzie to możliwe. W kompetencjach jednostki znajduje się także rozpowszechnianie wiedzy i podnoszenie świadomości zagrożeń wśród obywateli i ekspertów.

Należałoby rozważyć utworzenie takiego centrum w Polsce, które dostarczałoby rekomendacji dotyczących długoterminowych celów bezpieczeństwa państwa.

Planując działania w zakresie przeciwdziałania zagrożeniom hybrydowym należy pamiętać o trudnościach, które wszelkie próby ochrony bezpieczeństwa narodowego napotykają w państwach demokratycznych. Istotę tych trudności w trafny sposób opisał oficer francuskiego wywiadu i znawca problematyki dezinformacji i propagandy Władimir Wołkow, według którego „dezinformacja może być skuteczna tylko jeśli cel w jakiejś mierze współdziała i jeśli jest ona prowadzona za pośrednictwem mass mediów. W państwach totalitarnych państwo posiada monopol informacyjny, ludność jest więc zabezpieczona przed ingerencją tego typu (…) W dziedzinie dezinformacji kraje tak zwanego wolnego świata są pozbawione wszelkich możliwości ofensywnego działania. W dodatku nie łatwo jest im też bronić się przed dezinformacją, bo z samej definicji są przywiązane do wolności swych mass mediów i z prawnego punktu widzenia nic nie może przeszkodzić przeciwnikowi w ich opanowaniu. A jednak Zachód musi znaleźć jakieś środki zapobiegawcze jeśli chce zachować swą niezależność i poziom życia, bo oba te elementy idą w parze[599]”.

[599] F. Schoen, Ch.J. Lamb, *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Washington 2012, podaję za: M. Wojnowski, *Środki i metody wywierania wpływu na kampanie wyborcze i wybory w Stanach Zjednoczonych przez Związek Sowiecki w okresie Zimnej Wojny*, Raport Specjalny Warsaw Institute 04 czerwca 2021,

Budowanie zaufania w społeczeństwie, co podkreśla Arsalan Bilal z Centrum Studiów nad Pokojem Uniwersytetu w Tromsø – Norweskiego Uniwersytetu Arktycznego, należy uznać za kluczowy instrument chroniący przed zagrożeniami hybrydowymi. Dotyczy to zwłaszcza ataków obliczonych na destrukcję systemów obronnych państw, które obecnie posiadają demokratyczny model rządów w stylu zachodnim (tzw. liberalna demokracja). Co więcej, jak dodaje on „zaufanie pozostaje warunkiem sine qua non, aby jakakolwiek polityka czy strategiczna odpowiedź na zagrożenia hybrydowe przyniosła efekty. (…) Niepokojące jest to, że w wielu krajach zachodnich (…) instytucje państwowe tracą wiarygodność z powodu malejącego zaufania publicznego. W Stanach Zjednoczonych zaufanie publiczne spadło z 73% w latach 50. do 24% w 2021 r. Podobnie w Europie Zachodniej poziom zaufania spada systematycznie od lat 70.[600]".

Problem utraty zaufania do siebie dotyka też jednostek w społeczeństwie danego kraju. Tracąc poczucie jedności społecznej, dany kraj jest bardziej narażony na porażkę w przypadku ataku hybrydowego. Poszukując skutecznego podejścia w zakresie przeciwdziałania zagrożeniom hybrydowym, A. Bilal wskazuje, że „budowanie, odbudowywanie i umacnianie zaufania mają nadal zasadnicze znaczenie dla stworzenia trwałej odporności w obliczu zagrożeń hybrydowych. (…) Budowanie zaufania w ramach społeczności i między nimi powinno być podstawą wysiłków na rzecz neutralizacji działań i zagrożeń hybrydowych. Wymaga to nieustannych wysiłków na poziomie strukturalnym i politycznym w celu stworzenia silnych więzi między państwem a obywatelami, opartych na znaczącej przejrzystości, odpowiedzialności i włączeniu społecznym[601]."

W świetle wyników przeprowadzonych badań należy stwierdzić, że kwestia usprawnienia sposobów przeciwdziałania zagrożeniom hybrydowym we współczesnym państwie, w tym – w Polsce, nabiera coraz większego znaczenia w kontekście wzrostu napięć w międzynarodowym środowisku bezpieczeństwa. Wypracowanie metod skutecznego przeciwdziałania zagrożeniom hybrydowym, jak wykazały wyniki badań, ma szczególnie

https://warsawinstitute.org/pl/amerykanska-demokracja-jako-cel-rosyjskich-sluzb-specjalnych-srodki-metody-wywierania-wplywu-na-kampanie-wyborcze-wybory-w-stanach-zjednoczonych-przez-zwiazek-sowiecki-w-okresie-zimnej-wojny/ [dostęp: 24.12.2022].

[600] A. Bilal, *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie" jako antidotum,* NATO, 30 listopada 2021, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html [dostęp: 29.11.2022].

[601] Tamże.

istotne znaczenie dla małych i średnich krajów, takich jak Polska. Część rozwiązań, która sprawdziła się w przypadku krajów takich jak Izrael, powinna być wprowadzona przez Polskę bezzwłocznie przy konsensusie politycznym (m.in. wzmocnienie potencjału odstraszania, rozbudowa krajowego przemysłu zbrojeniowego, pozyskanie adekwatnego do regionalnych zagrożeń wsparcia strategicznego sojuszników). Jednakże, z uwagi na złożony charakter zagrożeń hybrydowych oraz ich ewolucję w przyszłości istnieje konieczność prowadzenia dalszych badań. Sprawne identyfikowanie zagrożeń hybrydowych oraz kompleksowe, systemowe wdrażanie usprawnień sposobów przeciwdziałania zagrożeniom hybrydowym jest procesem ciągłym – obliczonym na długi okres czasu. Działania w tym zakresie wymagają m.in. konsensusu głównych środowisk politycznych i konsultacji społecznych, środków finansowych, konsekwentnych i ponadpartyjnych prac legislacyjnych oraz współpracy z sojusznikami. Dlatego, metody usprawnienia przeciwdziałania zagrożeniom hybrydowym wymagają tym bardziej dalszych badań, uwzględniających zmienność zagrożeń i okoliczności, a także nowe wyzwania związane z dynamicznie zmieniającą się polityką bezpieczeństwa współczesnych państw i ryzykiem zmiany sojuszy, rozwojem nowych technologii militarnych, cyfrowych, informacyjnych, a także dążeniem hybrydowych agresorów do utrzymania swoich działań w szarej strefie – poniżej progu wojny.

Bibliografia

Publikacje zwarte

Aleksandrowicz T.R., *Terroryzm międzynarodowy*, Warszawa 2015.

Aleksandrowicz Tomasz R., *Agresja w cyberprzestrzeni. Problematyka art. 51 Karty Narodów Zjednoczonych. Uwagi de lege lata i de lege ferenda* [w:] Nowicka I., Mocarska D. (red.), *Współczesne problemy prawa. Nadużycia prawa*, tom 2, Szczytno 2016.

Apanowicz J., *Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne*, Difin 2005.

Davis N., *Boże igrzysko*, Kraków 1999.

Dawidczyk A., Jurczak, J., *Metody, techniki, narzędzia nauk o bezpieczeństwie*, Difin, 2019.

Frost M., Michelsen N., *International Ethics and Information Warfare*, [w:] O. Fridman, V. Kabernik, J. C. Pearce (red.), *Hybrid Conflicts and Information Warfare. New Labels, Old Politics*, Boulder-Colorado, USA 2019.

Kijewski T., *Zagrożenia hybrydowe, a bezpieczeństwo państwa na przykładzie konfliktu na Krymie w 2014 r. z uwzględnieniem aspektu przeciwdziałania terroryzmowi,* [w:] *XX-lecie walki z terroryzmem – bilans i konsekwencje, Tom I., Współczesne zagrożenia – Strategie reagowania – Edukacja*, B. Wiśniewska-Paź, D. Szlachter (red.), Wydawnictwo A. Marszałek w Toruniu, 2022.

Kijewski T., *Znaczenie zagrożeń hybrydowych dla bezpieczeństwa państwa na przykładzie wojny w Syrii w 2011 r.*, [w:] W. Zubrzycki, J. Cymerski (red.), *Terroryzm/Antyterroryzm #20 lat po 9/11*, Szczytno 2023.

Kluczowe megatrendy w bezpieczeństwie państwa w XXI wieku, Difin, Warszawa 2020.

Kubiak M., Wróblewski R. (red.), *Oblicza współczesnych wojen,* Warszawa 2018.

Lorenz W., *Odstraszanie. Strategia i polityk*a, Polski Instytut Spraw Międzynarodowych, 2021.

Majewski T., *Miejsce celów, problemów i hipotez w procesie badań naukowych*, AON 2003.

Pacek B., Grochocka J.A. (red.), *Konflikt hybrydowy na Ukrainie*: *aspekty teoretyczne i praktyczne* / Piotrków Trybunalski, 2017.

Pawłowski, Zdrodowski, Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Marszałek 2020.

Podstawy walki informacyjnej, Warszawa 2016.

Shirreff R., *Wojna z Rosją*, Rebis, 2017.

Śmiałek K., Śmiałek W. (red.), *Ewolucja wojen: wielość uwarunkowań, Toruń 2018.*

Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego" Wyd. II, Warszawa 2018.

Terrorism. Commentary on security documents, VOLUME 141 – Hybrid warfare and the gray zone threat, Douglas C. Lovelace, Jr. (red.), Oxford University Press, 2016.

Terrorism. Commentary on security documents, VOLUME 146 – Russia's Resurgence, Douglas C. Lovelace, Jr. (red.), Oxford University Press, 2017.

Wasiuta O., Wasiuta S., *Wojna hybrydowa Rosji przeciwko Ukrainie*. Arkana – Kraków 2017.

Wojna, jako narzędzie polityki XXI wieku. Stare pojęcia – nowe konotacje, [w:] W. Kostecki, K. Smogorzewski (red.), *Siła we współczesnych stosunkach międzynarodowych*, Warszawa 2017.

Akty prawne

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. z 2020 r. poz. 27

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U.2020.0.1856) https://lexlege.pl/ustawa-o-zarzadzaniu-kryzysowym/.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.U. 2019 poz. 742.

Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi, Dz.U. 2020 poz. 158.

Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, Dz.U. 2019 poz. 2418.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz.U. z 2019 r. poz. 796.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z 2020 poz.1369.

Dokumenty strategiczne, rezolucje, raporty i inne

Cyberataki jako element kampanii hybrydowych. Studium kampanii Ghostwriter, prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), *MSZ, 21 kwietnia 2022.*

Cybersecurity & Cyber Diplomacy, prezentacja w ramach seminarium online na zasadach Chatham House, European Security Defence College 25-29 kwietnia 2022.

Deklaracja końcowa szczytu NATO w Warszawie – wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., BBN 2016 https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf

Dezinformacja jako główna oś kampanii hybrydowych, prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), *MSZ, 21 kwietnia 2022.*

NATO 2022 Strategic Concept, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

Prezentacja o przeciwdziałaniu dezinformacji w Wielkiej Brytanii w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

Projekt Doktryny Bezpieczeństwa Informacyjnego RP, BBN, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf.

Rezolucja Parlamentu Europejskiego z dnia 10 października 2019 r. w sprawie ingerencji zewnętrznej w wybory i dezinformacji w krajowych i unijnych procesach demokratycznych (2019/2810(RSP).

Rozmowa z prof. dr hab. Tomaszem Grzegorzem Grosse w czasie konferencji *Bezpieczeństwo wschodniej flanki NATO*, Warszawa 19 października 2022 r.

Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, NATO 2016.

The Challenges of European Cybersecurity, European Security and Defence College / National Defence Institute (Portugalia), seminarium w formie online na zasadach Chatham House (bez przypisywania danej wypowiedzi do uczestnika), 26-30 września 2022 r.

Traktat Północnoatlantycki, Biuro Bezpieczeństwa Narodowego https://www.bbn.gov.pl/download/1/15754/TraktatPolnocnoatlantycki.pdf.

Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, Komisja Europejska 2016 (JOIN/2016/018 final) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52016JC0018

Wzmacnianie odporności, jako kluczowa metoda przeciwdziałania zagrożeniom hybrydowym – odporność w NATO, UE i lessons learned z wybranych państw, prezentacja w ramach seminarium online pt. *Zagrożenia hybrydowe (*na zasadach Chatham House – bez przypisywania danej wypowiedzi do autora), MSZ, 21 kwietnia 2022.

Zagrożenia hybrydowe z perspektywy instytucjonalnej Polski, UE, NATO – Polityki i instrumenty UE oraz NATO, seminarium online pt. *Zagrożenia hybrydowe (*na zasadach nie atrybucji Chatham House), MSZ, 21 kwietnia 2022.

Artykuły drukowane

Gapys J., Nowak M., *Polityka niemieckich i radzieckich okupantów wobec polskiego ziemiaństwa w latach II wojny światowej*, Przegląd Wschodnioeuropejski 2, 2011.

Jagiełło B., *Unia Europejska wobec wyzwań dla bezpieczeństwa europejskiego i jego zagrożeń,* M. Grącik, K. Żukrowska (red.), *Bezpieczeństwo międzynarodowe. Teoria i praktyka,* 2006.

Jakubowski M., *Gwardia Narodowa – Natychmiast Cz. II,* Polityka Polska. Wolny narodów – w silnym państwie, nr 2(10) luty 2016.

Artykuły i źródła internetowe

A multi-dimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation, European Commission – Directorate-General for Communication Networks, Content and Technology, March 2018 https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

Abbasi R., *New Warfare Domains and the Deterrence Theory Crisis*, E-International Relations, May 13 2020 https://www.e-ir.info/2020/05/13/new-warfare-domain-and-the-deterrence-theory-crisis/

Abed S., *Syria 2011: A Four Month Timeline of the Western Manufactured Uprising*, The Rabbit Hole, August 15, 2017 https://sarahabed.com/2017/08/15/syria-2011-a-four-month-timeline-of-the-western-manufactured-uprising/

Allison G., *Why ISIS Fears Israel*, The National Interest, August 8, 2016 https://www.belfercenter.org/publication/why-isis-fears-israel

Ataki cybernetyczne, zamachy terrorystyczne, Polska Agencja Prasowa, 3.10.2022 https://www.pap.pl/aktualnosci/news%2C1441577%2Cataki-cybernetyczne-zamachy-terrorystyczne-putin-chce-calkowita-zmiane-w.

Babraj R., *Dezinformacja w dobie cyfrowej rewolucji*, 19 maja 2020 https://cyberpolicy.nask.pl/dezinformacja-w-dobie-cyfrowej-rewolucji/.

Baidatz Y., Adamsky D., *Not Just Deterrence*, Israel Defense 4/03/2015 https://israeldefense.co.il/en/content/not-just-deterrence

Balcewicz J., *Strategia bezpieczeństwa UE 2020-2025*, 21 sierpnia 2020 https://cyberpolicy.nask.pl/strategia-bezpieczenstwa-ue-2020-2025/.

Beres L. R., Shoval Z., *Creating A Seamless Strategic Deterrent: An Israel Case Study*, 05.13.2019, Modern War Institute https://mwi.usma.edu/creating-seamless-strategic-deterrent-israel-case-study/

Beres L.R., *Israel's Nuclear Strategy: Enhancing Deterrence in the New Cold War (Part I), The Bridge*, May 29, 2018 https://thestrategybridge.org/the-bridge/2018/5/29/israels-nuclear-strategy-enhancing-deterrence-in-the-new-cold-war-part-i

Bilal A., *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie" jako antidotum,* NATO, 30 listopada 2021 https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html.

Bogusz M., *Unrestricted Warfare*, portal Za Wielkim Murem: Chiny i Azja 2018 https://zawielkimmurem.net/2018/10/28/qiao-liang-wang-xiangsui-unrestricted-warfare/.

Borowski J., *Przydacz: Sojusz postanowił wzmocnić wschodnią flankę, to zadanie dla dyplomatów i polityków*, Radio Opole 19.10.2022 https://radio.opole.pl/104,631182,przydacz-sojusz-postanowil-wzmocnic-wschodnia-fl.

Boulègue M., Polyakova A., *The Evolution of Russian Hybrid Warfare*, 29 stycznia 2021.

Bowen A. S., *Russian Military Intelligence: Background and Issues for Congress*, November 15, 2021 https://sgp.fas.org/crs/intel/R46616.pdf.

Bryjka F., *Rosyjscy kontraktorzy w służbie Kremla*, Warsaw Institute, https://warsawinstitute.org/wp-content/uploads/2019/08/ROSYJSCY-%E2%80%9EKONTRAKTORZY%E2%80%9D-W-S%C5%81U%C5%BBBIE-KREMLA-Warsaw-Institute.pdf.

Clark M., *Russian Hybrid Warfare*, Military Learning and the Future of War, Institute for the Study of War – ISW September 2020 https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf

Clark M., *The Russian Military's Lessons Learned in Syria*, Military Learning and the Future of War, Institute for the Study of War – ISW January 2021 https://www.understandingwar.org/sites/default/files/The%20Russian%20Military%E2%80%99s%20Lessons%20Learned%20in%20Syria_0.pdf

Countering Hybrid Threats and enhancing resilience, The Security and Defence Policy Directorate – EU, SECDEFPOL 2022.

Crimea parliament passes independence declaration, Interfax News Agency, 11 Mar 2014 https://interfax.com/newsroom/top-stories/44577/

Crisis in Crimea, Britannica https://www.britannica.com/place/Crimea/History#ref341465

Cyberatak to wojna naszych czasów, Rzeczpospolita, 03.12.2009 https://www.rp.pl/artykul/401049-Cyberatak-to-wojna-naszych-czasow.html.

DeBenedictis K., *Russian Hybrid Warfare and the Annexation of Crimea The Modern Application of Soviet Political Warfare*, Londyn 2022.

Departament Stanu USA https://www.state.gov/u-s-relations-with-syria/Ford R. S.

Deterring hybrid warfare: a chance for NATO and the EU to work together? (ang.), NATO.int.

Deterring Terror. English Translation of the Official Strategy of the Israel Defense Forces, G. Allison (red.), Belfer Center for Science and International Affairs, Harvard Kennedy School 2016 https://www.belfercenter.org/sites/default/files/legacy/files/IDFDoctrineTranslation.pdf

Duncan A. J., *New 'Hybrid War' or Old 'Dirty Tricks'? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment*, Canadian Military Journal, Vol. 17, No. 3, Summer 2017 http://www.journal.forces.gc.ca/Vol17/no3/PDF/CMJ173Ep6.pdf.

Entebbe raid, Encyclopedia Britannica, 2 Sep. 2022, https://www.britannica.com/event/Entebbe-raid

EU-HYBNET 2022 https://euhybnet.eu/about/partners/.

European Commission. A Multi-Dimensional Approach to Disinformation. Report of the Independent High Level Group on Fake News and Online Disinformation, Luxembourg 2018.

Everyone Should Save Syria from Falling into Hell, Interview with Syrian Deputy Foreign Minister Faisal al Mekdad – DER SPIEGEL, by Susanne Koelbl in Damascus, SPIEGEL Gruppe, 05.02.2013 https://www.spiegel.de/international/world/interview-with-syrian-deputy-foreign-minister-faisal-al-mekdad-a-881678.html.

Filimonov G., *The Color Revolutions in the Context of Hybrid Wars*, Hybrid Conflicts And Information Warfare New Labels, Old Politics, [w:] O. Fridman, M. Galeotti, *Russia's Hybrid War as a Byproduct of a Hybrid State*, War on the Rocks, December 6, 2016 https://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/

Fisher M., *Russian infiltration of Ukrainian military complicates Canadian training mission*, National Post, Apr 14, 2015 https://nationalpost.com/news/world/russian-infiltration-of-ukrainian-military-complicates-canadian-training-mission

Full text of Vladimir Putin's speech of September 30, 2022, transcript of the speech on the DPR, LPR, Zaporozhye and Kherson regions, Eprimefeed.com, October 11, 2022 https://eprimefeed.com/latest-news/full-text-of-vladimir-putins-speech-of-september-30-2022-transcript-of-the-speech-on-the-dpr-lpr-zaporozhye-and-kherson-regions/192853/.

Giles O., *How did the Syrian Civil War Become a Proxy War? And will it ever end?*, National Interest, 13.09.2019 https://nationalinterest.org/blog/middle-east-watch/how-did-syrian-civil-war-become-proxy-war-80716

GlobalFirepower 2022 https://www.globalfirepower.com/country-military-strength-detail.php?country_id=israel

Golov A., *Israeli Deterrence in the 21st Century,* Memorandum No. 155, Tel Aviv: Institute for National Security Studies, June 2016 https://www.inss.org.il/wp-content/uploads/systemfiles/INSSMemo155.03.1.Golov.ENG.pdf

Hajduk J., Stępniewski T., *Wojna hybrydowa Rosji z Ukrainą: Uwarunkowania i instrumenty* „Studia Europejskie 4/2015", Centrum Europejskie Uniwersytetu Warszawskiego 2015 https://journalse.com/pliki/pw/4-2015_hajduk.pdf.

Heistein, A., Michlin-Shapir V., Russia's Hybrid-Warfare Victory in Syria, 19.05.2016 https://nationalinterest.org/feature/russias-hybrid-warfare-victory-syria-16273.

History of Crimea. Early history to the Crimean War https://www.britannica.com/place/Crimea/History https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

Hoffman F. G., Hybrid warfare and challenges, JFQ: Joint Force Quarterly, 2009. https://smallwarsjournal.com/documents/jfqhoffman.pdf.

Hoffman F., Conflict in the 21st Century: The Rise of the Hybrid Wars, https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf; za: Piekarski M. *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych, „*Terroryzm – studia, analizy, prewencja" 2022.

Hybrid COE 2022 https://www.hybridcoe.fi/who-what-and-how/

Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf

Hybrid Warfare of the Future, CEPA July 28, 2021 https://cepa.org/hybrid-warfare-of-the-future-sharpening-natos-competitive-edge/

Instrukcja pisania prac dyplomowych, Instytut Prawa, Administracji i Ekonomii Uniwersytetu Pedagogicznego w Krakowie, 2017 https://ipaie.up.krakow.pl/wp-content/uploads/2017/11/Vademecum_Seminarzysty.pdf.

Israel Defense Forces, *Encyclopedia* Britannica, 20 Oct. 2022, https://www.britannica.com/topic/Israel-Defense-Forces

Israel, *Report of the Winograd Commission*, How does law protect in war? (the "Online Casebook"), The International Committee of the Red Cross https://casebook.icrc.org/case-study/israel-report-winograd-commission

Israel, *The World Factbook*, CIA 2022 https://www.cia.gov/the-world-factbook/countries/israel/#military-and-security

Israeli Commando of Entebbe to give first hand account of the Greatest Hostage Rescue in History, 11/08/2022 https://www.southtahoenow.com/story/11/08/2022/israeli-commando-entebbe-give-first-hand-account-greatest-hostage-rescue-history

Izrael czy Iran? Kto dysponuje większą siłą militarną?, Rzeczpospolita 07.06.2018 https://www.rp.pl/konflikty-zbrojne/art9762901-izrael-czy-iran-kto-dysponuje-wieksza-sila-militarna

Jakubczak R., *Budujemy wojska wewnętrzne czy Obronę Terytorialną?,* Instytut Bezpieczeństwa i Rozwoju Międzynarodowego, 17.08.2018, https://instytutbirm.pl/budujemy-wojska-wewnetrzne-czy-obrone-terytorialna/.

Jakubczak R., *Obronę trzeba budować od fundamentów*, wywiad w ramach Forum Strategicznego Defence24.pl i Fundacji Instytut Bezpieczeństwa i Strategii (FIBiS) 11.11.2020, https://defence24.pl/polityka-obronna/prof-jakubczak-obrone-trzeba-budowac-od-fundamentow.

Jasper S., Moreland S., *The Islamic State is a Hybrid Threat: Why Does That Matter?,* Small Wars Journal, 12.02.2014 https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter.

Jezierski G., *Kalendarium budowy elektrowni jądrowej w Żarnowcu, czyli... jak straciliśmy swoją szansę?* Gigawat Energia 30.01.2006 https://web.archive.org/web/20110716074324/http://gigawat.info/archiwum/article/articleview/667/1/60/index.html

Johnson, D. E., *Preparing for Hybrid Opponents: Israeli Experiences in Lebanon and Gaza,* RAND Corporation, 2011 https://www.rand.org/pubs/research_briefs/RB9620.html

Johnson, D. E., *Military Capabilities for Hybrid War: Insights from the Israel Defense Forces in Lebanon and Gaza,* RAND Corporation 2010 https://www.rand.org/pubs/occasional_papers/OP285.html

Kabernik V., Pearce J. C. (z-lib.org), Londyn 2019 https://cepa.org/the-evolution-of-russian-hybrid-warfare-introduction/

Karolewski A., Rejman-Karolewska M., *Konflikt hybrydowy zagrożeniem dla bezpieczeństwa granic Rzeczpospolitej Polskiej,* [w:] Przegląd Naukowo-Metodyczny Edukacja Dla Bezpieczeństwa, Rok XI Numer 3/2018 (40), Wydawnictwo Wyższej Szkoły Bezpieczeństwa w Poznaniu, Poznań 2018 http://www.przeglad.wsb.net.pl/uploads/1/0/3/7/10371016/pnm_3_2018_ca%C5%81o%C5%9A%C4%86_-_druk_ostateczny.pdf.

Karouny M., *Syria to send in army after 120 troops killed,* Reuters, JUNE 6, 2011 https://www.reuters.com/article/idCATRE7553AI20110606.

Komornicki L, *Rosja nie skończy wojny! Zmuszą Putina do pokoju?* Gen., wywiad w programie Express Biedrzyckiej, Super Express 8.11.2022 https://www.youtube.com/watch?v=NJq19RA2ogg.

Komornicki L.: *Obrona państwa powinna mieć charakter powszechny*, wywiad dla Defence24.pl 28.08.2020 https://defence24.pl/sily-zbrojne/gen-komornicki-obrona-panstwa-powinna-miec-charakter-powszechny.

Krajowy Plan Zarządzania Kryzysowego, Rządowe Centrum Bezpieczeństwa, 2022 https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego.

Kuper S., *Hybrid warfare and a new role for Australia's Special Forces?*, Defence Connect 4.07.2019, https://www.defenceconnect.com.au/key-enablers/4355-hybrid-warfare-and-a-new-role-for-australia-s-special-forces.

Kuzio T., D'Anieri P., *Annexation and Hybrid Warfare in Crimea and Eastern Ukraine*, Jun 25 2018 https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/

Kwiecińska M., *Nowy wymiar konfliktów zbrojnych: konflikt hybrydowy a konflikt pełzający*, Doctrina Studia Społeczno-Polityczne 13/2016, Akademia Sztuki Wojennej, Wydział Zarządzania i Dowodzenia http://www.doctrina.uph.edu.pl/stara/doctrina_2016/6_Kwiecinska.pdf.

Lambeth, B. S., *The Winograd Commission's Findings*, [w:] *Air Operations in Israel's War Against Hezbollah: Learning from Lebanon and Getting It Right in Gaza,* RAND Corporation, 2011 https://www.jstor.org/stable/pdf/10.7249/mg835af.14.pdf?addFooter=false

Landis J., *What happened at Jisr al-Shagour?,* SyriaComment.com, 13.06.2011 https://www.joshualandis.com/blog/what-happened-at-jisr-al-shagour/.

Legucka A., *Walka z rosyjską dezinformacją w UE*, Polski Instytut Spraw Międzynarodowych, 6 sierpnia 2019.

Lentzos F. *The Russian disinformation attack that poses a biological danger, the Bulletin of the Atomic Scientists,* November 19, 2018 https://thebulletin.org/2018/11/the-russian-disinformation-attack-that-poses-a-biological-danger/ [29.11.2022].

Lewicki S., *Jak silny jest Izrael?,* Portal Myśli Konserwatywnej – Konserwatyzm.pl, 4 września 2021 https://konserwatyzm.pl/lewicki-jak-silny-jest-izrael/

Lloyd G., *Hybrid Warfare and Active Measures*, Small Wars Journal 10.10.2021 https://smallwarsjournal.com/jrnl/art/hybrid-warfare-and-active-measures

Londoño E., Miller G., *U.S. starts delivering weapons to Syrian rebels,* Toronto Star, 11.09.2013 https://www.thestar.com/news/world/2013/09/11/us_starts_delivering_weapons_to_syrian_rebels.html.

Lorenz W., *Deterrence in the Baltic Sea Region. A View from Poland*, The Hague Centre for Strategic Studies January 2022 https://hcss.nl/wp-content/uploads/2021/12/04-Deterrence-in-the-Baltic-Sea-Region-HCSS-2022.pdf

Łuczak D., *Wojna hybrydowa*, Przegląd Bezpieczeństwa Wewnętrznego, Agencja Bezpieczeństwa Wewnętrznego, 05.11.2015 https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html.

Matusiak M., *Paradoksy izraelskiej polityki. Krótki kurs*, Ośrodek Studiów Wschodnich im. Marka Karpia, 2022-09-27 https://www.osw.waw.pl/sites/default/files/PW_87_Paradoksy%20izraelskiej%20polityki_net_0.pdf

Matvienko Y., *How Israel reformed the intelligence and special services,* BulgarianMilitary.com January 9, 2022 https://bulgarianmilitary.com/amp/2022/01/09/how-israel-reformed-the-intelligence-and-special-services/

Mefford B., *Ukraine embraces openness with new report on Russian hybrid warfare challenges,* Atlantic Council, February 1, 2021 https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-embraces-openness-with-new-report-on-russian-hybrid-warfare-challenges/.

Metzger P., *The Imperative to Maintain Focus in Syria, Newsweek 16.04.2021* https://www.newsweek.com/imperative-maintain-focus-syria-opinion-1583346

Michalik Ł., *Rosyjski UR-77 Meteorit zniszczony jednym granatem*, MSN 20.10.2022 https://www.msn.com/pl-pl/wiadomosci/polska/rosyjski-ur-77-meteorit-zniszczony-jednym-granatem-dos%C5%82ownie-wyparowa%C5%82/ar-AA13aD21?ocid=msedgntp&cvid=087693ba5a244e4492dbb0783d8860c5.

Molenda K.: *Nasza praca to nie działanie pojedynczych samotnych wilków*, Cyberdefence24, 03.09.2021 https://cyberdefence24.pl/armia-i-sluzby/gen-bryg-karol-molenda-nasza-praca-to-nie-dzialanie-pojedynczych-samotnych-wilkow.

Monaghan S., *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice,* Hybrid CoE Paper 12, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf

MSZ Rosji: Armia cybernajemników prowadzi przeciwko nam wojnę, Rzeczpospolita, 29.03.2022 https://www.rp.pl/dyplomacja/art35965491-msz-rosji-armia-cybernajemnikow-prowadzi-przeciwko-nam-wojne.

NATO Communication and Information Agency – Cyber Security Service Line https://www.ncirc.nato.int/Home/About.

NATO's response to hybrid threats, strona internetowa NATO, 2.07.2018 https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=uk.

Nemeth W. J., *Future war and Chechnya: a case for hybrid warfare*, Naval Postgraduate School, Monterey, California, June 2002 https://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1.

Nemeth W. J., *Russia's State-centric Hybrid Warfare*, The International Centre for Defence and Security (ICDS) / *ICDS Diplomaatia magazine*, 17.04.2015 https://icds.ee/en/russias-state-centric-hybrid-warfare/

Netanyahu says Israel could 'conquer' Gaza if 'deterrence' not achieved, The Times of Israel, 19 May 2021 https://www.timesofisrael.com/netanyahu-says-israel-could-conquer-gaza-if-deterrence-not-achieved/

Nippert M., Fisher D.*, Revealed: China's network of influence in New Zealand*, NZ Herald, 20.09.2017, https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11924169.

Oldberg I., *The Long War in Donbas: Causes and Consequences,* The Swedish Institute of International Affairs, 2020 https://www.ui.se/globalassets/ui.se-eng/publications/ui-pub6/lications/2020/ui-report-no.-1-2020.pdf

Olech A., *Współpraca NATO i Unii Europejskiej w obliczu zagrożeń hybrydowych, ze szczególnym uwzględnieniem terroryzmu*, *Instytut Nowej Europy*, 11 grudnia 2020

https://ine.org.pl/wspolpraca-nato-i-unii-europejskiej-w-obliczu-zagrozen-hybrydowych-ze-szczegolnym-uwzglednieniem-terroryzmu/.

Overview of countermeasures by the EU28 to the Kremlin's subversion operations How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies?, European Values Think-Tank, 16.05.2017 https://www.europeanvalues.net/wp-content/uploads/2017/05/Overview-of-countermeasures-by-the-EU28-to-the-Kremlin%E2%80%99s-subversion-operations-1.pdf.

Pacholski Ł., Rokosz A., *Siły zbrojne Izraela*, Defence 24, 17.11.2012 https://defence24.pl/sily-zbrojne/sily-zbrojne-izraela

Parafianowicz Z., *O co chodzi w wojnie na Ukrainie?*, wywiad dla telewizji internetowej https://www.youtube.com/watch?v=uqo_9_fG3dA.

Paulauskas K., *Zagadnienie odstraszania*, *Przegląd NATO* 5 sierpnia 2016 https://www.nato.int/docu/review/pl/articles/2016/08/05/zagadnienie-odstraszania/index.html

Pearson E., *Operation Wrath of God*. Encyclopedia Britannica, 2 May. 2018 https://www.britannica.com/topic/Operation-Wrath-of-God

Piekarski M. *Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych,* „Terroryzm – studia, analizy, prewencja" 2022, s. 89-90.

Pindják P., *Deterring hybrid warfare: a chance for NATO and the EU to work together?,* NATO Review, 18 November 2014 https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html

Piwowarski J. A., *Metodologiczne i badawcze założenia pracy dyplomowej z dyscypliny nauk o bezpieczeństwie – przykład*, „Security, Economy & Law" 4/2019 (XXV), s. 26 –39, DOI: 10.24356/SEL/25/2 http://security-economy-law.pl/wp-content/uploads/2020/05/SEL-25_26-39.pdf.

Private Military Consulting Company RSB-Group (Russian Security Systems) https://rsb-group.org/about 2022

Rácz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, The Finnish Institute of International Affairs https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf

Rada Federacji Rosyjskiej za operacją na Ukrainie, TVP Info, 01.03.2014 https://www.tvp.info/14214218/rada-federacji-rosyjskiej-za-operacja-na-ukrainie

Relations with Asia-Pacific partners, NATO 12.06.2022 https://www.nato.int/cps/en/natohq/topics_183254.htm.

Repin S., *Syria and Ukraine. Key Features of the Kremlin's 'Hybrid' War*, Inform Napalm – News Syria, 22.10.2015 https://informnapalm.org/en/syria-and-ukraine-key-features-of-the-kremlin-s-hybrid-war/

Roell P., *Migration – A New Form of "Hybrid Warfare"?* Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW, May 2016 https://www.ispsw.com/wp-content/uploads/2016/05/422_Roell_RINSA.pdf

Rogozińska A., *Niemilitarne zagrożenia dla Ukrainy w kontekście działań hybrydowych prowadzonych przez Federację Rosyjską*, INE, 24 listopada, 2019 https://kopia.ine.org.pl/niemilitarne-zagrozenia-dla-ukrainy-w-kontekscie-dzialan-hybrydowych-prowadzonych-przez-federacje-rosyjska/

Rühle M., *Odstraszanie: co może sprawić, a czego nie*, Przegląd NATO, 20 kwietnia 2015 https://www.nato.int/docu/review/pl/articles/2015/04/20/odstraszanie-co-moze-sprawic-a-czego-nie/index.html

Rühle M., Roberts C., *Enlarging NATO's toolbox to counter hybrid threats*, NATO Review, 19 March 2021 https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html

Rühle M., Roberts C., *Zwiększanie zasobności środków NATO do zwalczania zagrożeń hybrydowych*, Przegląd NATO 19 marca 2021 https://www.nato.int/docu/review/pl/articles/2021/03/19/zwiekszanie-zasobnosci-srodkow-nato-do-zwalczania-zagrozen-hybrydowych/index.html.

Safar Jalani M., *The Russian invasion of Ukraine happened because the world gave Vladimir Putin a free pass in Syria*, MENA Source, Atlantic Council, March 9, 2022 https://www.atlanticcouncil.org/blogs/menasource/the-russian-invasion-of-ukraine-happened-because-the-world-gave-vladimir-putin-a-free-pass-in-syria/.

Schmitt M. N., *Counter-Terrorim and the Use of Force in International Law*, The Marshall Center Papers, No 5, 2002.

Schoen F., Lamb Ch.J., *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Washington 2012, podaję za: Wojnowski M., *Środki i metody wywierania wpływu na kampanie wyborcze i wybory w Stanach Zjednoczonych przez Związek Sowiecki w okresie Zimnej Wojny*, Raport Specjalny Warsaw Institute 04 czerwca 2021 https://warsawinstitute.org/pl/amerykanska-demokracja-jako-cel-rosyjskich-sluzb-specjalnych-srodki-metody-wywierania-wplywu-na-kampanie-wyborcze-wybory-w-stanach-zjednoczonych-przez-zwiazek-sowiecki-w-okresie-zimnej-wojny/.

Schroefl, J., Välimäki J., *The Syrian Civil War: Russia As A Hybrid Threat Actor*, [w:] *Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence,* Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf .

Seebeck L., *Indo-Pacific needs to establish a center for countering hybrid threats*, Nikkei Asia, 11.06.2022 https://asia.nikkei.com/Opinion/Indo-Pacific-needs-to-establish-a-center-for-countering-hybrid-threats.

Siły Obronne Izraela, Ambasada Izraela w Polsce (Departament Wojskowy) https://embassies.gov.il/warsaw/Departments/Wojskowy/Pages/wojskowy.aspx

Siły obronne Izraela, Konflikty.pl 19.11.2006 https://www.konflikty.pl/technika-wojskowa/na-ladzie/sily-obronne-izraela/

Słownik języka polskiego, Wydawnictwo Naukowe PWN 2022 https://sjp.pwn.pl

Syria: historia konfliktu, Rodgers L., Gritten D., Offer J., Asare P. (red.), BBC, 11 marca 2016 https://www.bbc.com/news/world-middle-east-26116868

Syrian Civil War, *Encyclopedia Britannica*, 17 Jul. 2020, https://www.britannica.com/event/Syrian-Civil-War

Szymański P., *NATO i Unia Europejska wobec zagrożeń hybrydowych,* OSW, 24.4.2020 https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-04-24/nato-i-unia-europejska-wobec-zagrozen-hybrydowych.

Terrorism. Commentary on security documents, VOLUME 141 – Hybrid warfare and the gray zone threat, Douglas C. Lovelace, Jr. (red.), Oxford University Press, 2016, s. 9-10 (ix-x)

The crisis in Crimea and eastern Ukraine, Encyclopaedia Britannica https://www.britannica.com/place/Ukraine/The-Poroshenko-administration

*The future of Syria. ISIS, the Iranians and the displaced millions, w*ebinarium *The Woodrow Wilson Center*, Apr. 5, 2022 https://www.wilsoncenter.org/event/future-syria-isis-iranians-and-displaced-millions

The Landscape of Hybrid Threats: A Conceptual Model. Public Version, European Union / Hybrid CoE, 2021 https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf

The Syrian Civil War. A New Stage, But Is It The Final One? April 2019 Policy Paper 2019-8 https://www.mei.edu/sites/default/files/2019-04/Ford_The_Syrian_Civil_War.pdf

Trends in world military expenditure 2021, SIPRI 2022. https://www.sipri.org/sites/default/files/2022-04/fs_2204_milex_2021_0.pdf

Turecki K., Jagielski P. *Ronen Bergman: niektórzy moi rozmówcy zostali zabici, Onet,* 26 marca 2019 r. https://wiadomosci.onet.pl/tylko-w-onecie/ronen-bergman-niektorzy-moi-rozmowcy-zostali-zabici/q1f4bk3

U.S. Relations With Israel, US Department of State, JANUARY 20, 2021 https://www.state.gov/u-s-relations-with-israel/

Unia Europejska po raz pierwszy stosuje sankcje związane z *cyberatakami*, Biuro Rzecznika Prasowego, Ministerstwo Spraw Zagranicznych, 31.07.2020 https://www.gov.pl/web/dyplomacja/unia-europejska-po-raz-pierwszy-stosuje-sankcje-zwiazane-z-cyberatakami.

Välimäki J., *ISIS as A Hybrid Threat Actor: From Iraq And Syria To A New Rise In Africa*, [w:] *Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence*, Hybrid CoE Research Report 5, The European Centre of Excellence for Countering Hybrid Threats, March 2022 https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf.

Ward M., *Refugees Forced to Return to Syria Face Imprisonment, Death at the Hands of Assad*, Atlas Institute for International Affairs March 14, 2019

https://www.internationalaffairshouse.org/refugees-forced-to-return-to-syria-face-imprisonment-death-at-the-hands-of-assad/

What is Hybrid CoE?, The European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finland, 2022 https://www.hybridcoe.fi/who-what-and-how/

Wilk A., Olszański T. A., Górecki W., *Porozumienie mińskie – rok gry pozorów*, OSW, 2016-02-10 https://www.osw.waw.pl/pl/publikacje/analizy/2016-02-10/porozumienie-minskie-rok-gry-pozorow

Wilk A., *Rosyjska interwencja wojskowa na Krymie,* Analizy – Ośrodek Studiów Wschodnich, 2014-03-05 https://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie

Wilk A., Żochowski P., Konończuk W., *Konflikt w Donbasie – wymuszona deeskalacja?* ANALIZY OSW, 2014-06-11 https://www.osw.waw.pl/pl/publikacje/analizy/2014-06-11/konflikt-w-donbasie-wymuszona-deeskalacja

Wojnowski M. , *Mit „wojny hybrydowej". Konflikt na terenie państwa ukraińskiego w świetle rosyjskiej myśli wojskowej XIX–XXI wieku,* Przegląd Bezpieczeństwa Wewnętrznego Wojna hybrydowa – WYDANIE SPECJALNE, Agencja Bezpieczeństwa Wewnętrznego 05.11.2015 https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html.

Wojnowski M., *Konflikty na tle rasowym jako narzędzie destrukcji Stanów Zjednoczonych w działaniach rosyjskich służb wywiadowczych* Przegląd Bezpieczeństwa Wewnętrznego nr 23 (12) 2020 https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-15/1719,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-23-12-2020.html.

Wojnowski M., *Środki i metody wywierania wpływu na kampanie wyborcze i wybory w Stanach Zjednoczonych przez Związek Sowiecki w okresie Zimnej Wojny. Raport – Część I, Warsaw Institute,* 4 czerwca 2021 https://warsawinstitute.org/pl/amerykanska-demokracja-jako-cel-rosyjskich-sluzb-specjalnych-srodki-metody-wywierania-wplywu-na-kampanie-wyborcze-wybory-w-stanach-zjednoczonych-przez-zwiazek-sowiecki-w-okresie-zimnej-wojny/.

Yeşiltaş M., *Neighboring A Civil War Turkey's Border Security With Syria*, SETA 10.2015 20151028162016_analysis_17.pdf (setav.org).

Zwalczanie dezinformacji w odniesieniu do koronawirusa, strona internetowa Komisji Europejskiej 16 czerwca 2022 r. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_pl.