Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Nauk o Polityce i Bezpieczeństwie

mgr inż. Sławomir CIEŚLA

ROZPRAWA DOKTORSKA

BUDOWA NARODOWEGO SYSTEMU ANTYDOSTĘPOWEGO JAKO DETERMINANTA WZMOCNIENIA ODPORNOŚCI POLSKI

Promotor:
dr hab. Zdzisław Polcikiewicz, prof. UMK

Promotor pomocniczy:
dr Robert Reczkowski

Toruń 2024

SPIS TREŚCI

WSTĘP

Posiadanie silnych sił zbrojnych jest podstawą naszego bezpieczeństwa, ale nie mogą one być silne, jeśli nasze społeczeństwa są słabe; tak więc naszą pierwszą linią obrony muszą być silne społeczeństwa zdolne do zapobiegania, przetrwania, adaptacji i odbicia się od wszystkiego, co się stanie

Jens Stoltenberg, Sekretarz Generalny NATO

Jedną z zasadniczych potrzeb zarówno człowieka, jak i wszelkich zbiorowości, w tym także państwa, jest bezpieczeństwo[1]. Bezpieczeństwo rozumiane jest jako pewność istnienia, posiadania oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (ich niewystępowania lub eliminowania), ale powstaje także wskutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego[2]. Warto zwrócić uwagę, że bezpieczeństwa nie należy rozpatrywać jedynie w odniesieniu do pojedynczego człowieka. Jest to także zasadnicza potrzeba społeczności oraz państw i narodów. Przez bezpieczeństwo państwa (bezpieczeństwo narodowe) należy rozumieć „[…] najważniejszą wartość, potrzebę narodową i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki, gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym obronę i ochronę państwa jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie”[3].

Dlatego też zapewnienie bezpieczeństwa narodowego jest jednym z głównych obowiązków, które stoją przed danym państwem. Jest ono oczekiwane i wymagane przez jego obywateli. Dążenie do zaspokojenia potrzeby bezpieczeństwa oznacza realizację wszelkich dostępnych przedsięwzięć zarówno przez człowieka, jak i władze samorządowe oraz państwowe. Określenie poziomu bezpieczeństwa jest zagadnieniem niezwykle

[1] Potrzeba bezpieczeństwa została uwzględniona na drugim miejscu w hierarchii tuż za potrzebami fizjologicznymi (egzystencjalnymi). Por. A. Maslow, *Motywacja i osobowość*, Warszawa 2010, s. 62–64.

[2] R. Zięba, J. Zając, *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski – Ekspertyza*, Warszawa 2010, s. 8.

[3] W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wyd. AON, Warszawa 2011, s. 31.

trudnym, chociażby ze względu na jego subiektywność. Konkludując, można przyjąć, że dążenie do zapewnienia bezpieczeństwa jest procesem ciągłym i wymaga systematycznych działań ogółu obywateli w celu stworzenia oraz doskonalenia mechanizmów przyczyniających się do osiągnięcia zakładanego jego poziomu.

Tempo zmian w środowisku bezpieczeństwa postępuje w tempie wykładniczym. Znaczny wpływ na takie postrzeganie mają szybkie zmiany w technologii powodujące przełamywanie dotychczasowo obowiązujących barier czasowych i przestrzennych. W związku z tym wydarzenia i decyzje podjęte w określonym miejscu mają niebagatelny wpływ na funkcjonowanie społeczeństw w innych regionach. Trwająca wojna w Ukrainie, aktywność Chin na Morzu Południowochińskim, roszczenia w stosunku do Tajwanu czy też rozszerzanie się organizacji państw BRICS[4] (często nazywanych też Globalnym Południem) to tylko kilka indykatorów wskazujących na zmierzanie w kierunku świata wielobiegunowego, w wyniku czego najprawdopodobniej dojdzie do zachwiania globalnej równowagi sił. Na poczucie bezpieczeństwa mają wpływ także takie zidentyfikowane trendy w środowisku bezpieczeństwa jak starzenie się społeczeństw w krajach rozwiniętych i związane z tym obawy o funkcjonowanie rynków pracy, zmiana klimatu, narastający problem związany z migracjami czy też tworzeniem się społeczeństw równoległych[5]. Przez ostatnie lata świat doświadczał znaczących zmian w obszarach: politycznym, społecznym, gospodarczym i środowiskowym, na które znaczący wpływ miał gwałtowny rozwój technologii. Zbieg kilku trendów politycznych, społeczno-gospodarczych i technologicznych na nowo definiuje globalny kontekst bezpieczeństwa, powodując, że złożoność, nieporządek i niepewność stały się nową normą. W przeciwieństwie do tego konwergencja trendów, napędzana przez technologię i innowacje, może zaoferować perspektywę rozwiązania globalnych problemów, takich jak ubóstwo, niedobór zasobów naturalnych, dostęp do usług zdrowotnych i edukacji[6]. Wszelkie zidentyfikowane powyżej czynniki zwiększają niepewność i złożoność, a zarazem stanowią wyzwanie dla zdolności poszczególnych państw do zarządzania rosnącym zestawem wzajemnie powiązanych problemów. Złożoność problemów wynikająca z wzajemnych zależności pomiędzy sferą cywilną a wojskową, a także kompresją czasu niezbędnego na analizę oraz zaplanowanie działań naprawczych, tylko pogłębia obawy związane z zapewnieniem bezpieczeństwa.

[4] Nazwa pochodzi od pierwszych liter angielskiej wersji nazw: Brazylia, Rosja, Indie, Chiny, RPA. Przyp. aut.
[5] Por. J. Mokrzycki, R. Reczkowski, S. Cieśla, *Analiza środowiska bezpieczeństwa w perspektywie 2035 roku*, Bydgoszcz 2020, s. 5.
[6] *The Strategic Foresight Analysis Report 2017,* Allied Command Transformation, Norfolk 2017, s. 15.

Przedstawione powyżej czynniki wpływające na poziom bezpieczeństwa skłaniają do konkluzji, że w dalszym ciągu niezwykle istotne dla Polski jest jej członkostwo zarówno w strukturach NATO, jak i Unii Europejskiej. Z jednej strony pozwala to na uzyskanie gwarancji bezpieczeństwa przed agresją zbrojną, z drugiej zaś daje szansę na rozwój gospodarczy.

Analiza trendów i wynikające z nich implikacje dla środowiska bezpieczeństwa przedstawione w dotychczasowych sojuszniczych raportach *Strategic Foresight Analysis* opracowywanych w Allied Command Transformation (ACT), a także m.in. w Stanach Zjednoczonych (*Joint Operating Environment 2040, National Intelligence Council's Global Trends report*), Wielkiej Brytanii (*Global Strategic Trends*), Kanadzie (*Future Security Environment 2013–2040*) czy też w Polsce (opracowana w Centrum Doktryn i Szkolenia Sił Zbrojnych *Analiza środowiska bezpieczeństwa w perspektywie 2035 roku*) stały się bazą do określenia kierunków, w jaki sposób Sojusz mógłby zrealizować kilka kluczowych działań: ustanowić i stosować jednolitą wizję, adaptować się i przekształcać w celu wypełniania swoich podstawowych zadań (obrony zbiorowej, zarządzania kryzysowego i bezpieczeństwa kooperatywnego), sprostać pełnemu zakresowi wyzwań związanych z bezpieczeństwem oraz rozwijać ramy koncepcyjne dla sił i zdolności niezbędnych do osiągnięcia sukcesu w perspektywie wykraczającej poza średniookresowy horyzont planowania. Działania te pozwolą także NATO stawić czoła szeregowi wyzwań związanych z bezpieczeństwem i zapewnią środki odstraszania i obrony, a także posłużą ochronie wspólnych wartości i zapewnieniu stabilności poza regionem euroatlantyckim.

Wielu ekspertów zwraca uwagę na rozszerzanie się środowiska operacyjnego daleko poza tradycyjnie dotychczas postrzegane obszary odpowiedzialności sił zbrojnych. Ocenia się, że środowisko to będzie charakteryzować się ciągłą konkurencją pomiędzy podmiotami zarówno państwowymi, jak i niepaństwowymi wykorzystującymi wszelkie dostępne instrumenty oddziaływania. Zwraca się przy tym uwagę na zacieranie się granic pomiędzy działaniami w aspektach cywilnym i wojskowym oraz we wszystkich domenach (fizycznych i niefizycznych). W środowisku tym działalność prowadzą zróżnicowane podmioty często niezależnie od siebie. Skuteczna działalność w takim środowisku wymaga proaktywnego myślenia, skutecznej łączności, świadomości sytuacyjnej, ciągłego i systematycznego doskonalenia procedur, a także szybkości działania. Przyszłe działania będą prowadzone w wielowymiarowym (fizycznym, wirtualnym i kognitywnym) oraz wielodomenowym

środowisku operacyjnym. Pomimo że natura działań wojennych pozostaje niezmieniona, to ich charakter ewoluuje i nadal będzie ewoluował. Zdaniem części ekspertów współczesna wojna obejmuje nie tylko konfrontację zbrojną przeciwstawnych sił zbrojnych, ale wiele różnorodnych wrogich działań poniżej progu wojny na obszarze całego państwa, skierowanych przeciwko gospodarce czy społeczeństwu. Zatem zrozumienie i adaptacja zmian w środowisku pozwoli na właściwe przygotowanie państwa do prowadzenia działań. Osiągnięcie sukcesu w takich uwarunkowaniach uzależnione jest od wzajemnych relacji pomiędzy społeczeństwem, władzami samorządowymi i państwowymi a siłami zbrojnymi. Konieczne staje się wypracowanie sposobu działań umożliwiających skupienie i synchronizację wysiłków w celu budowania przewagi oraz proaktywnego kształtowania środowiska operacyjnego zgodnie z posiadanymi mocnymi stronami. Stworzenie przestrzeni decyzyjnej gwarantujące możliwość generowania różnych opcji reagowania na aktywność przeciwnika pozwala na kreowanie dla niego dylematów na szczeblu zarówno strategicznym, operacyjnym, jak i taktycznym. Jedną z takich koncepcji rozwijaną w ostatnich latach jest *NATO Warfighting Capstone Concept* – NWCC (pol. nadrzędna koncepcja działań bojowych NATO). Wraz z niektórymi innymi koncepcjami NWCC wdraża strategię wojskową NATO, nowoczesne podejście określające wojskowo-strategiczne cele Sojuszu oraz sposoby i środki ich realizacji. NWCC zawiera opis środowiska operacyjnego i przyszłych działań wojennych w 2040 roku, aby zidentyfikować implikacje dla przyszłych militarnych instrumentów siły (ang. *Military Instruments of Power* – MIoP[7]). Analiza trendów oraz implikacje z nich wynikające dla środowiska bezpieczeństwa pozwoliły na określenie pięciu obszarów, w których rozwijanie zdolności umożliwi uzyskanie zdecydowanej przewagi nad adwersarzami. Zapewniają one spójność w całym zakresie wysiłków na rzecz rozwoju działań wojennych. Oferują ponadto nowe, przyszłościowe, wielodziedzinowe i przekrojowe podejście do myślenia, organizowania i działania wojskowego. Należą do nich: *cognitive superiority, layered resilience, infuence and power projection, cross-domain command* oraz *integrated Multi-domain defence*[8] (pol. przewaga poznawcza, wielowarstwowa odporność, projekcja siły i wpływów, dowodzenie wielodomenowe oraz zintegrowana obrona wielodomenowa).

[7] *Military instrument of power* to pojęcie z dziedziny strategii wojskowej, które odnosi się do narzędzi, jakimi dysponuje państwo w celu osiągnięcia swoich celów politycznych i militarnych. W skład tych narzędzi wchodzą między innymi siły zbrojne, wywiad, dyplomacja, a także gospodarka i kultura. Por. Joint Doctrine Note 1-18, *Strategy,* Joint Chiefs of Staff, Waszyngton 2018 r., s. 25.

[8] *NATO Warfighting Capstone Concept,* Allied Command Transformation, maj 2023 r., s. 2-12.

Jedną z kwestii rozwijanych w ramach wspomnianego wyżej NWCC jest budowa odporności, która rozumiana jest jako zdolność do absorpcji wstrząsów i walki we wszystkich aspektach: wojskowym, cywilno-wojskowym i wojskowo-cywilnym[9]. Zwraca się przy tym szczególną uwagę na konieczność ścisłej koordynacji w sferach cywilnych i wojskowych. Tylko takie kompleksowe działania uwzględniające ciągłość dowodzenia i kierowania, wzajemną znajomość potrzeb oraz możliwości, budowę redundantnych systemów wzmocni, a także przyczyni się do rozbudowy odporności całego państwa. Należy również zwrócić uwagę na fakt, że budowa odporności odbywa się głównie w sferze cywilnej.

Powinno się przy tym wspomnieć, że już w czasie szczytu NATO w Warszawie w 2016 r. stwierdzono, że to odporność jest niezbędną podstawą wiarygodnego odstraszania i obrony oraz skutecznego wypełniania podstawowych zadań Sojuszu[10]. Podczas tego spotkania postanowiono zwiększyć odporność NATO na pełne spektrum zagrożeń i kontynuować rozwijanie indywidualnej oraz zbiorowej zdolności do przeciwstawienia się każdej formie ataku zbrojnego.

Budowa odpornego państwa to wysiłek całego społeczeństwa, którego efektem będzie zwiększenie zdolności m.in. do zachowania ciągłości kierowania państwem, funkcjonowania służby zdrowia czy też funkcjonowania infrastruktury krytycznej. Jak ważne są to zagadnienia, przekonujemy się codziennie, śledząc doniesienia i raporty z przebiegu wojny rozpętanej przez Rosję w Ukrainie. Zaangażowanie całego społeczeństwa, sektora publicznego i prywatnego, struktur państwowych i samorządowych, środowiska naukowego i organizacji pozarządowych na rzecz budowania odporności powinno stać się wyzwaniem na najbliższe lata. Warto zwrócić uwagę na zapis zawarty w opracowanej w Wielkiej Brytanii narodowej strategii odporności (ang. *The National Resilience Strategy. A Call for Evidence*): „Każdy obywatel i organizacja mają do odegrania rolę w zwiększaniu znaczenia odporności Wielkiej Brytanii, a narodowa odporność jest przedsięwzięciem całej społeczności kraju. Aby opracować skuteczną strategię na rzecz odporności Wielkiej Brytanii, ważne jest, abyśmy ją zrozumieli i wcielili w życie szeroki wachlarz poglądów i dowodów na to, jakie powinny być nasze priorytety w zakresie budowy naszej przyszłej odporności. Twoje zaangażowanie w nasze pytania w ramach *Call for*

[9] Tamże, s. 12.
[10] *Commitment to enhance resilience*, Pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/official_texts_133180.htm?selected Locale=en, 2016 [dostęp: 27.07.2021].

Evidence zapewni nieoceniony wkład w tę pracę”[11]. Należy zatem stwierdzić, że także w polskich warunkach trzeba przygotować narodową strategię odporności, która całościowo zajmowałaby się tym wyzwaniem. Jak wynika ze słów Grzegorza Matyasika, zastępcy dyrektora Rządowego Centrum Bezpieczeństwa próbę opracowania dokumentu krajowego w tym obszarze podjęło Rządowe Centrum Bezpieczeństwa, przygotowując *Koncepcję kompleksowego wzmacniania odporności*. Wskazano w nim na zasadność dążenia do wzmocnienia odporności jako wysiłek realizowany przez administrację publiczną, różne instytucje, służby, samorządy, przedsiębiorstwa, środowiska i grupy społeczne w celu zwiększenia bezpieczeństwa państwa oraz jego obywateli i mieszkańców[12].

Budowanie odporności oraz późniejsze jej utrzymanie na założonym poziomie (czy też jej odbudowa po sytuacji kryzysowej) powinno być elementem holistycznie tworzonego systemu bezpieczeństwa państwa. Nie można pozwolić na skupienie wysiłków na realizacji zadań tylko w jednym obszarze, nawet tak istotnym jak odporność. O złożoności problemu mogą świadczyć konkluzje ekspertów z Rządowego Centrum Bezpieczeństwa (RCB), opracowujących wspomnianą koncepcję, dotyczące szeregu dokumentów z zakresu zarządzania kryzysowego oraz bezpieczeństwa narodowego, które swoim zakresem obejmują problematykę wzmacniania odporności i powinny być podstawą do stworzenia jednolitego i spójnego systemu. Zaliczono do nich między innymi: *Krajowy Plan Zarządzania Kryzysowego* (KPZK), *Raport o zagrożeniach bezpieczeństwa narodowego*, *Wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego*, *Narodowy Program Ochrony Infrastruktury Krytycznej* (NPOIK), *Plan Reagowania Obronnego Rzeczypospolitej Polskiej* (PRO RP) oraz plany operacyjne funkcjonowania administracji publicznej, *Rządowy Program Rezerw Strategicznych oraz Strategię cyberbezpieczeństwa RP na lata 2019 – 2024*[13].

Podjęte w Polsce działania na rzecz opracowania spójnej koncepcji w obszarze odporności są zdecydowanie krokiem w dobrą stronę. Pozwolą one na usystematyzowanie wiedzy oraz wskazanie kierunków działania na rzecz jej budowy. Uzupełnieniem działań podjętych na rzecz budowy odporności może być rozwinięcie narodowego systemu antydostępowego. Taki system może być wykorzystany do osłony i zabezpieczenia

[11] *The National Resilience Strategy. A Call for Evidence*, Cabinet Office, London 2021, s. 10 (pkt 9). Pobrano z lokalizacji: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/10014 04/Resilience_Strategy_-_Call_for_Evidence.pdf [dostęp: 22.07.2023].

[12] G. Matyasik, *Jak wygląda polska odporność?,* Infosecurity24, 04.04.2023 r., pobrano z lokalizacji: https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [dostęp: 10.09.2023].

[13] Tamże.

elementów infrastruktury krytycznej, co wpłynie na zwiększenie odporności. Zaproponowane w dalszej części dysertacji założenia takiego systemu wpisują się w ogłoszone na szczycie NATO w 2016 r. minimalne standardy występujące w siedmiu obszarach: gwarancji ciągłości rządów; zabezpieczenia dostaw energii; zarządzania przemieszczaniem się ludności; wydolności służby zdrowia w czasie wojny; zabezpieczenia zapasów żywności i wody; infrastruktury telekomunikacyjnej; transportu. Można dostrzec, że większość z tych obszarów może ochronić efektywnie zorganizowany system antydostępowy.

Takimi systemami dysponują niektóre państwa (np. Rosja, Chiny czy Iran) i stanowią one przykład możliwości zabezpieczenia niektórych elementów wpływających na odporność państwa. Zwraca się jednak uwagę, że systemy te były organizowane z całkowicie różnych powodów, ale można dostrzec wspólny mianownik. Mianowicie mają one zapewnić realizację strategicznych celów danego państwa. Wydaje się, że także w przypadku Polski można mówić o budowie i utrzymaniu odporności państwa jako o wyzwaniu strategicznym.

Czy można jednak stwierdzić, że nawet najlepszy system antydostępowy będzie w stanie skutecznie reagować w sytuacji zagrożenia, szczególnie w warunkach wysokiej intensywności współczesnych konfliktów? Nasuwa się jednoznaczna odpowiedź – nie. Natomiast z całą pewnością zasadne jest prowadzenie badań prowadzących do zorganizowania efektywnego i spójnego systemu. W ostatnich latach w gremiach wojskowych, ale także w środowisku cywilnym, dyskutowano i prowadzono badania, gry wojenne oraz różnego rodzaju ćwiczenia w zakresie pokonywania systemu antydostępowego stworzonego przez Rosję, a także Chiny. Zauważono pewną prawidłowość: systemem rosyjskim zajmowała się większość uczestników, natomiast Chinami zdecydowanie mniejsza liczba – głównie Amerykanie. Cechą charakterystyczną jest jednak skupienie wysiłków na poszukiwaniu sposobów pokonania takich systemów. Specjaliści dochodzili do bardzo podobnych wniosków. Stwierdzono, że pokonanie takiej bariery jest możliwe, natomiast pociągnie to za sobą ogromne straty ludzkie oraz w sprzęcie, a także będzie olbrzymim wyzwaniem logistycznym. Autor biorąc udział w niektórych z tych projektów, postanowił zaprojektować taki system, który mógłby stać się elementem odstraszającym przeciwnika oraz stwarzającym mu duży problem. Można spotkać się z opinią, że w ostatnich latach zbyt mały nacisk kładziono na kwestie zdolności do obrony całego własnego terytorium i w zbyt dużej mierze liczono na siły wzmocnienia NATO.

Zasadne staje się zatem pytanie, w świetle rosyjskich działań w Ukrainie, czy takie podejście jest słuszne? Z drugiej strony istnieje obawa, że taka pomoc może przyjść zbyt późno, co potwierdzają różne ośrodki eksperckie, np. amerykański *think tank* Atlantic Council[14]. Dlatego większość ekspertów sugeruje, że właściwie zorganizowany system antydostępowy, posiadający zdolności do odstraszania, ale i wyeliminowania znaczących środków agresora, może być istotnym elementem systemu bezpieczeństwa narodowego.

Jedną z najistotniejszych motywacji dla autora niniejszej dysertacji były dotychczasowe opracowania, przede wszystkim te skupiające się na pokonaniu systemu antydostępowego, i prawie całkowity brak propozycji w zakresie budowy podobnego systemu w Polsce. Konieczność budowy odpornego państwa i niedobór materiałów w tym zakresie skłoniły autora do przeprowadzenia badań i określenia stanu odporności Polski. Zdaniem autora pozwoliło to w konsekwencji na zidentyfikowanie silnych i słabych stron, wskazanie pożądanych kierunków zmian oraz zaproponowanie założeń systemu antydostępowego jako elementu wpływającego na zachowanie odporności państwa. Z tych względów rozprawa ma charakter nie tylko poznawczy, ale także utylitarny.

Dla osiągnięcia celu rozprawy przyjęto strukturę obejmującą: wstęp, rozdział metodyczny, cztery rozdziały merytoryczne oraz zakończenie. Rozdziały są tematycznie związane z przyjętymi i rozwiązywanymi problemami badawczymi.

We **wstępie** przedstawiono sytuację problemową, a także strukturę i zawartość poszczególnych rozdziałów rozprawy.

Rozdział pierwszy w całości poświęcono metodologii badań, a jego układ jest typowy dla dysertacji. Przedstawiono w nim: uzasadnienie wyboru tematu, przedmiot i cel badań, problemy oraz hipotezy badawcze, metody, techniki i narzędzia stosowane w procesie badawczym, dobór i charakterystykę próby badawczej, a także obszar i teren badań wraz z ograniczeniami oraz przebieg procesu badawczego.

W **rozdziale drugim** scharakteryzowano współczesne środowisko bezpieczeństwa i operacyjne w zakresie wpływu na bezpieczeństwo narodowe Polski. Istotną częścią rozdziału są prognozy rozwoju środowiska bezpieczeństwa, a na ich podstawie zidentyfikowano potencjalne wyzwania i zagrożenia dla bezpieczeństwa Polski.

[14] K. Turecki, *Atlantic Council: NATO musi się przygotować na rosyjską inwazję*, Onet.pl, 25.07.2016, pobrano z lokalizacji: https://wiadomosci.onet.pl/tylko-w-onecie/atlantic-council-nato-musi-sie-przygotowac-na-rosyjska-inwazje /44ceqr [dostęp: 10.03.2020].

W **rozdziale trzecim** określono istotę odporności państwa, a także zidentyfikowano i przedstawiono zasadnicze zagrożenia dla tej odporności. W dalszej części rozdziału zaproponowano warunki, jakimi powinno się charakteryzować odporne państwo. Na podstawie przeprowadzonych przez autora badań podjęto próbę określenia stopnia odporności Polski na zidentyfikowane zagrożenia w kontekście odporności państwa w siedmiu obszarach określonych w czasie szczytu NATO w Warszawie w 2016 r.

W **rozdziale czwartym** scharakteryzowano systemy antydostępowe wybranych krajów, uznając je za elementy mogące przyczynić się do zachowania oraz wzmocnienia właściwego poziomu odporności. Podjęto próbę opisania dwóch najbardziej reprezentatywnych sposobów rozbudowy takich systemów podjętych przez Chiny i Rosję. Zwrócono uwagę na podstawowe różnice w ich budowie, a przede wszystkim na odmienne podejście do określenia celów, które stały u podstaw ich tworzenia.

W **rozdziale piątym** określono założenia oraz przedstawiono propozycję budowy narodowego systemu antydostępowego jako elementu wzmacniania odporności Polski. Szczególną uwagę zwrócono na możliwości takiego systemu w zakresie zagwarantowania bezpieczeństwa przepływów strategicznych oraz zapewnienia ciągłości działania elementów infrastruktury krytycznej. W tym względzie autor skupił się na przedstawieniu założeń systemowych oraz określeniu, czym taki system powinien się charakteryzować, czy też jakie powinien posiadać zdolności. Nie podjęto próby wyspecyfikowania środków mogących być częścią takiego systemu. W opinii autora część informacji związanych z tym obszarem należy do informacji wrażliwych (niejawnych), dlatego też nie powinny być przedstawiane w pracy o charakterze jawnym. Co ważne, wyniki wywiadów przeprowadzonych z ekspertami zajmującymi się problematyką systemów antydostępowych w znaczny sposób wpłynęły na poglądy autora w tej kwestii.

Każdy rozdział jest zakończony wnioskami, w których podjęto próbę przedstawienia rozwiązań przyjętych problemów badawczych, a także rekomendacjami dotyczącymi pożądanych kierunków zmian w rozpatrywanych zagadnieniach związanych z zachowaniem i wzmacnianiem odporności państwa.

Ważnym elementem dysertacji jest także **zakończenie**, w którym bazując na uzyskanych wynikach badań, odniesiono się do stopnia rozwiązania przyjętych problemów badawczych oraz weryfikacji hipotez. Przedstawiono także syntetyczne wnioski ogólne, a także propozycję założeń narodowego systemu antydostępowego. W zakończeniu podkreślono potrzebę dalszego prowadzenia badań naukowych w obszarze budowy

odporności oraz tworzenia systemu utrudniającego przeprowadzenie skutecznego ataku na Polskę, wskazując przy tym pożądane kierunki dalszej penetracji naukowej.

Dysertacja jest analitycznym opracowaniem o charakterze zarówno teoretycznym (poznawczym), jak i praktycznym. Jej wartość utylitarna wynika z całościowego ujęcia problematyki związanej z budową, utrzymaniem czy też odbudową odporności państwa, jak również propozycją rozwiązań w zakresie tworzenia narodowego systemu antydostępowego, co jest szczególnie istotne w aspekcie bezpieczeństwa naszego państwa.

ROZDZIAŁ I

METODOLOGICZNE PODSTAWY PROCESU BADAŃ

Miarą prawdy jest pewność tego, kto ją poznaje

Kartezjusz

Bezpieczeństwo dotyczy wszelkich sfer życia społecznego, ale również wytworów materialnych, które powinny spełniać wymagania społeczne i techniczne standardów bezpieczeństwa. Badanie potrzeb społecznych podstawowego podmiotu bezpieczeństwa w aspekcie jego przetrwania, uniezależnienia się od zagrożeń i zagwarantowania jego rozwoju sprowadza się nie tylko do zmaterializowania się jego potrzeb w systemach społecznych, ale również wymaga poprawy jakości życia, na którą składają się wytwory materialne i niematerialne. W procesie badań bezpieczeństwa dokonujemy zatem poznania naukowego, którego efekty mogą i powinny być spożytkowane do rozwoju cywilizacyjnego. Dlatego też pierwotny cel poznania naukowego, rozumiany jako poszerzenie obszarów wiedzy, filozofowie i metodolodzy rozszerzają również na cel utylitarny i planistyczny postrzegany w kategoriach projektowania bezpieczeństwa. W związku z tym, że aspekty bezpieczeństwa sytuowane są we wszystkich sferach życia podmiotu bezpieczeństwa, zasadne jest uwzględnianie szerokiego aspektu stosowanych metod, technik i narzędzi badawczych do poznania, oceny, prognozowania i projektowania bezpieczeństwa[15].

1.1. Uzasadnienie wyboru tematu

Punktem wyjściowym do podjęcia tematu niniejszej dysertacji była ogłoszona, Postanowieniem Prezydenta Rzeczypospolitej Polskiej z dnia 12 maja 2020 roku, *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, w której zwraca się uwagę na potrzebę rozwijania zdolności odpornościowych[16] (ang. *resilience*) państwa. Jak zauważają autorzy *Strategii…*, potrzeba ta wynika przede wszystkim z konieczności zapewniania zarówno państwu, jak i jego obywatelom poczucia bezpieczeństwa. Wydaje się jednak, że wskazana powyżej definicja nie wyjaśnia w pełni przedmiotowego zagadnienia. Chociażby dlatego, że literatura przedmiotu wskazuje na zasadność określania odporności jako

[15] A. Czupryński, B. Wiśniewski, J. Zboina (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Wyd. CNBOP-PIB, Józefów 2017, s. 5.

[16] Odporność to zdolność przeciwstawiania się czemuś, niepoddawania się działaniu lub naciskowi. Utożsamiana jest z wytrzymałością, a w rozumieniu powszechnym postrzegana jest jak cecha organizmu w walce z chorobami. Por. *Mały słownik języka polskiego,* Warszawa 1968, s. 490.

zdolności państwa, na wszystkich jego poziomach, do zorganizowania systemu zapewniającego niedopuszczenie przeciwnika do rozpoczęcia ataku (w każdym wymiarze np. zbrojnym, poniżej progu wojny, cybernetycznym itd.), odparcie tego ataku, wszelką pomoc ludności poszkodowanej w wyniku tych działań w zakresie niezbędnym do zachowania zdrowia i życia. To także zapewnienie ciągłego funkcjonowania obiektów infrastruktury krytycznej[17]. Należy także stwierdzić, że o odporności powinniśmy mówić nie tylko w odniesieniu do stanu kryzysu lub wojny, ale jej budowa powinna rozpocząć się już dzisiaj – w stanie stałej gotowości obronnej państwa, a jednym z elementów wzmacniania odporności państwa w wymiarze militarnym może być budowa systemu antydostępowego (ang. *Anti-Access/Area Denial*, A2/AD)[18].

Analizując konflikty zbrojne na przestrzeni wieków, można dojść do wniosku, że koncepcje czy też rozwiązania tego typu, czyli swoisty *zakaz dostępu do obszaru*, nie są nowością XXI wieku, a historia wojskowości zna co najmniej kilka przykładów, które mogą wydawać się nader archaiczne. Chińczycy zbudowali i utrzymywali przed wiekami w sprawności jedną z najsłynniejszych fortyfikacji obronnych, jaką jest Wielki Mur Chiński[19], przywódcy imperium osmańskiego rozmieszczali działa na brzegach Bosforu, by nie dopuścić do przejścia okrętów przeciwnika z Morza Śródziemnego na Morze Czarne, a Francuzi po pierwszej wojnie światowej zbudowali swoją XX-wieczną wersję wielkiego muru – Linię Maginota[20]. Z kolei II wojna światowa, a szczególnie wyścig zbrojeń okresu

[17] Zgodnie z obowiązująca ustawą o zarządzaniu kryzysowym infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy zaopatrzenia w energię, surowce energetyczne i paliwa, systemy łączności, sieci teleinformatyczne, systemy finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej oraz systemy produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (art. 3 ust. 2 ustawy o zarządzaniu kryzysowym). Przyp. aut.

[18] Element A2 oznacza działania ograniczające, w części lub całkowicie, dostęp potencjalnego przeciwnika do określonego teatru działań/obszaru operacyjnego, natomiast element AD oznacza ograniczenie temu przeciwnikowi swobody działania na zajmowanym przez niego terenie/obszarze. Przyp. aut.

[19] Wielki Mur Chiński – nazwa systemów obronnych składających się z zapór naturalnych, sieci fortów i wież obserwacyjnych oraz murów obronnych z ubitej ziemi, murowanych lub kamiennych, osłaniających północne Chiny przed najazdami ludów z Wielkiego Stepu. Tradycyjnie przyjmuje się, że Wielki Mur rozciągał się od Shanhaiguan (nad zatoką Liaodong) do Jiayuguan w górach Nan Shan na długości ok. 2 400 km. Nazywany jest też „Murem 10 000 Li" (Li – jednostka miary, oznaczająca „nieskończoną długość" muru). Pobrano z lokalizacji: http://www.budowle.pl/budowla,wielki-mur-chinski [dostęp: 16.03.2017].

[20] Linia Maginota – nazwa francuskich fortyfikacji zbudowanych, a następnie wzmacnianych w latach 1929–1940 na wschodnich granicach państwa. Dzielą się na: fortyfikacje na granicy z Niemcami i Luksemburgiem, Linię Obrony Renu, Nowe Fronty (w tym tzw. Przedłużenie Linii Maginota), fortyfikacje na granicy z Belgią i fortyfikacje na granicy z Włochami. Doświadczenia z walk na froncie zachodnim podczas I wojny światowej wpłynęły na powstanie nowej defensywnej francuskiej doktryny wojennej. Chęć uniknięcia w przyszłym

zimnej wojny, który po niej nastał, przyniosła początki nowoczesnych technologii służących współczesnej koncepcji A2/AD – oprócz rozwoju lotnictwa wojskowego rozwój środków do jego wykrywania i zwalczania, między innymi radiolokacji i systemów obrony powietrznej oraz zarówno klasycznych, jak i rakietowych systemów artyleryjskich o dużych zasięgach. Aktualnie koncepcja A2/AD[21] jest stechnicyzowaną XXI-wieczną[22] formą rozwinięcia tego typu pomysłów prowadzenia działań w przestrzeni powietrznej oraz kosmicznej, na lądzie i morzu, a także w cyberprzestrzeni. Dlatego też ma ona zasadniczy wpływ na utrzymanie swobody przerzutu i przemieszczenia wojsk, zaopatrzenia i uzupełnień na teatr/y prowadzenia działań dla samodzielnego prowadzenia operacji (zarówno działania z art. 5. Traktatu Waszyngtońskiego[23], jak i spoza niego lub dla wsparcia sił sojusznika/koalicjanta. Wiąże się z tym konieczność zdobycia i utrzymania określonego

konflikcie konieczności toczenia wojny pozycyjnej na pozycjach polowych sprawiła, że generalicja wysuwała potrzebę przygotowania silnych fortyfikacji stałych jako osłony kraju i dla przygotowania rozstrzygającej ofensywy. W zamyśle jej projektantów i pomysłodawców miała ona być przeszkodą nie do pokonania dla ewentualnej agresji Niemiec na Francję i była klasycznym rozwinięciem zasad wojny pozycyjnej – francuska doktryna wojenna zakładała wyższość wojny obronnej – pozycyjnej nad działaniami ofensywnymi. Jej długość wynosiła ok. 450 km, a budowa pochłonęła blisko 2,9 mld franków. Składała się z blisko sześciuset głównych obiektów obronnych, ogółem zaś wybudowano ok. 5 800 wszystkich typów fortyfikacji i umocnień. Pobrano z lokalizacji: http://www.budowle.pl/budowla,liniamaginota [dostęp: 16.03.2017].

[21] Jak wynika z prowadzonych w krajach „zachodnich" analiz dotyczących koncepcji A2/AD (np. opracowanie RAND Corporation pt. *Smarter Power, Stronger Partners*) – podobnie o nowoczesnym wykorzystaniu sił i środków myśli wiele innych krajów, nie tylko Rosja, a do najpotężniejszych z nich należą Chiny. Samo określenie „koncepcji A2/AD" funkcjonuje w zachodniej przestrzeni pojęć wojskowych, co oznacza, że nie musi być w ten sposób nazywana (określana) w Rosji i Chinach. Przyp. aut.

[22] Pierwsze rozważania na temat obecnej koncepcji pojawiają się w analizach i raportach wojskowych (amerykańskich i sojuszniczych) z przełomu XX i XXI w., szczególnie w odniesieniu do militarnych zdolności Chin. Por. A. Krepinevich, B. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy*, Nowy Jork, 2015.

[23] Zgodnie z art. 5 Traktatu Waszyngtońskiego strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez artykuł 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego. O każdej takiej zbrojnej napaści i o wszystkich środkach zastosowanych w jej wyniku zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa. Zob. *Traktat Północnoatlantycki*, Waszyngton, 04.04.1949 r.

Działania spoza artykułu 5. (ang. *Non-Article 5 Crisis Response Operations* – NA5CRO) to operacje reagowania kryzysowego opisane jako takie, których prowadzenie ma na celu wypełnienie mandatu ONZ, UE lub OBWE oraz innych organizacji regionalnych. Obejmują one działania dyplomatyczne, polityczne, wojskowe i cywilne, zainicjowane i wykonane zgodnie z prawem międzynarodowym. Przyczyniają się do zapobiegania konfliktom oraz umożliwiają zarządzanie sytuacjami kryzysowymi lub służą celom humanitarnym w osiągnięciu zadeklarowanych celów Sojuszu. Por. *Operacje reagowania kryzysowego spoza artykułu 5*, DD/3.4(A), sygn. Szkol. 876/2013**,** Bydgoszcz 2013, s. 9-10.

stopnia kontroli przestrzeni powietrznej, kosmicznej oraz panowania na morzu czy w cyberprzestrzeni.

W związku z powyższym za celowe uważa się przeprowadzenie badań w przedmiotowym obszarze. Literatura przedmiotu, a szczególnie krajowa – poświęcona kwestii zarówno odporności państwa, jak i elementów systemu antydostępowego, dotyka tego obszaru w sposób ogólny i nie wyczerpuje tego tematu. Co więcej, można zauważyć, że zagadnieniem budowy odporności zajmują się przede wszystkim autorzy angielskojęzyczni. Z kolei pozycje polskojęzyczne są w większości powieleniem i odzwierciedleniem ich poglądów. Wobec powyższego podjęta przez autora w niniejszej dysertacji problematyka już z założenia powinna stanowić wartość dodaną w naukach o bezpieczeństwie, ponieważ pozwoli na uporządkowanie i usystematyzowanie wiedzy dotyczącej zarówno odporności państwa, jak i systemów antydostępowych.

1.2. Przedmiot i cele badań

Jak podkreśla Andrzej Czupryński, w procesie badań istotne jest określenie przedmiotu badań i jego kontekstu powstania lub funkcjonowania w przeszłości[24]. W literaturze przedmiotu spotyka się zamiennie stosowane pojęcia dotyczące identyfikacji i opisania przedmiotu poznania jako obszar badań, obiekt badań i przedmiot badań. Wydaje się, że takie podejście jest mało zasadne, by synonimicznie określać to, co jest przedmiotem poznania. Jednakże, pomimo braku sklasyfikowania tych trzech pojęć, należy podkreślić, że używane w rożnych kontekstach w stosunku do przedmiotu poznania spełniały swoje funkcje opisowe tego, co zamierzamy poznać, i w jakich relacjach znajduje się przedmiot badań z otoczeniem. Wychodząc z założenia, że poznajemy to, co jest materialne, możemy dookreślić w tym kontekście to, co poznajemy w aspekcie obszaru, obiektu i przedmiotu badań w ujęciu systemowym. Jeżeli poznajemy to, co jest materialne, to również to coś poznawane posiada zespół cech fizycznych. Cecha to element odróżniający podmiot lub przedmiot od innych, należący do tej samej klasy lub charakteryzujący dany przedmiot, istotę żywą, stany, procesy, czynności lub zjawiska. W tym rozumieniu pojęcie semantyczne cechy odnosi się do proponowanej triady pojęć: obszaru, obiektu i przedmiotu badań w podobnym ujęciu.

[24] A. Czupryński, *Obszar oraz obiekt i przedmiot badań w naukach o bezpieczeństwie*, [w:] A. Czupryński, B. Wiśniewski, J. Zboina (red.), *Nauki o bezpieczeństwie. Wybrane problemy badań*, Wyd. CNBOP-PIB, Józefów 2017, s. 29.

Na potrzeby niniejszej pracy przyjęto definicję przedmiotu badań przedstawioną przez Mariana Cieślarczyka, który stwierdził, że „[…] przedmiotem badań w naukach o bezpieczeństwie jest fenomen bezpieczeństwa oraz składające się na niego fakty (zdarzenia), procesy i bardziej szczegółowe zjawiska w sferze bezpieczeństwa, w jego różnych wymiarach przedmiotowych i między nimi, rozpatrywane w odniesieniu do konkretnych podmiotów, z punktu widzenia których analizujemy bezpieczeństwo, przy uwzględnieniu także wpływu warunków środowiskowych. Oczywiste jest, że przedmiotem badań będą także relacje między podmiotem a jego otoczeniem (środowiskiem), charakter tego otoczenia, ale także cechy danego podmiotu”[25].

W świetle takiej interpretacji przyjęto, że przedmiotem badań prowadzonych w ramach dysertacji będą potrzeby i możliwości budowy narodowego systemu antydostępowego (narodowych zdolności antydostępowych) w aspekcie jego wpływu na bezpieczeństwo Polski.

Na ostateczny kształt pracy miały wpływ ograniczenia czasowe, przestrzenne jak również te związane informacjami wrażliwymi (niejawnymi). Do ograniczeń czasowych należy zaliczyć przede wszystkim okres, w którym badania były prowadzone. Badania sondażowe z użyciem techniki wywiadu eksperckiego prowadzono w okresie od września 2021 do kwietnia 2022 r. W związku z powyższym, jak również z uwagi na dynamiczną sytuację międzynarodową, wyniki tych badań – jakkolwiek cenne i rzetelne – mogą być w pewnych obszarach nieco zdezaktualizowane. Dlatego też autor starał odnieść się do aktualnej sytuacji w przypisach oraz w części dotyczącej konkluzji będących podsumowaniem poszczególnych rozdziałów. Do drugiej grupy ograniczeń zaliczono te związane z obszarem prowadzenia badań, jak również obszarem rozpatrywanych problemów. Autor podjął próbę przeprowadzenia badań dotyczących spraw wewnętrznych Polski oraz spraw międzynarodowych. Umożliwiło to poszerzenie perspektywy związanej z problematyką budowy odporności i funkcjonowania systemów antydostępowych. Do szczególnie wartościowych autor zalicza informacje pozyskane od ekspertów z Hiszpanii i Estonii. Do trzeciej grupy ograniczeń zaliczono te związane z dostępem do informacji wrażliwych (niejawnych). Problematyka związana zarówno z utrzymaniem, jak i budową odporności jest w sporej części niedostępna ze względu na poziom jej klasyfikacji. Podobnie przedstawia się sytuacja z informacjami dotyczącymi systemów

[25] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa,* Wyd. Akademii Podlaskiej, Siedlce 2009, s. 212.

antydostępowych, które w dużej części są opatrzone wysokimi klauzulami poufności. Autor z racji posiadania dostępu do takich informacji podjął dużo wysiłku, aby w pracy znalazły się tylko informacje jawne. W każdej takiej sytuacji zastosowano odpowiedni przypis przywołujący źródło, z którego skorzystano.

Istotnym elementem etapu koncepcyjnego było określenie celu badań. Już Arystoteles wskazywał, że niezidentyfikowanie celów czyni z każdego działania czynnik pozorny, zatem warunkiem koniecznym badań naukowych jest ich planowość co do oczekiwanych efektów i procesu poznania[26]. Według *Słownika języka polskiego* cel jest to coś „do czego się dąży, co chce się osiągnąć"[27]. Z kolei W. Zaczyński cel badań definiuje jako „bliższe określenie tego, do czego zamierza badacz, co pragnie osiągnąć w swoim działaniu... podany w koncepcji cel musi legitymować się konkretnością, jasnością i realnością. Realność celu polega na wytyczaniu takich zamierzeń, które leżą w granicach możliwości danego badacza"[28]. Co więcej, jak podkreśla A. Czupryński „[…] w procesie poznania cel możemy sklasyfikować jako poznawczy i utylitarny. Cel poznawczy inspirują motywy, które skłaniają badacza do poznania naukowego i jest to dążenie do odkrycia prawdy naukowej – jak jest? Poprzez cel poznawczy następuje identyfikacja, deskrypcja, eksplanacja i diagnoza stanu oraz procesu bezpieczeństwa. Cel utylitarny wynika z wniosków z celu poznawczego i stanowi jego kontynuację w aspekcie poprawy jakości bezpieczeństwa. Cel utylitarny to rezultat, do którego zmierza postępowanie badawcze i jego efektem są: uwarunkowania spełnienia się prognozy, naprawa rzeczywistości, wynalazki. Poprzez cel utylitarny wnioskujemy, jak może być i co zasadne jest uczynić, by przeciwdziałać zagrożeniom bezpieczeństwa. Szczególnym elementem celu utylitarnego jest cel planistyczny, którego istotą jest naukowe przygotowanie procesu zmian w obrębie badanego przedmiotu. Podstawowe pytanie – jak zmienić przedmiot badań, by było tak, jak być powinno, tzn. bezpieczniej niż jest obecnie. Cel planistyczny ma głęboki związek z inżynierią bezpieczeństwa, ponieważ daje podstawy naukowe do projektowania bezpieczeństwa nie tylko w wymiarze społecznym, ale również technicznym. Zatem w ramach ogólnej konstatacji można powiedzieć, że celem badawczym jest to, co chcemy osiągnąć poprzez realizację badań.

[26] M. Krajewski, *O metodologii nauk i zasadach pisarstwa naukowego*. *Uwagi podstawowe*, Wyd. Uniwersytetu Śląskiego, Gliwice 2010, s. 20.
[27] *Słownik języka polskiego,* t.1, Wyd. PWN, Warszawa 1978, s. 235.
[28] W. Zaczyński, *Praca badawcza nauczyciela,* Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995, s. 52-53.

Jako cel poznawczy dociekań naukowych w niniejszej dysertacji przyjęto zbadanie potrzeb i możliwości budowy narodowego systemu antydostępowego oraz określenie jego wpływu na poziom bezpieczeństwa państwa. Celem diagnostycznym było zidentyfikowanie przyczyn słabości Polski w niektórych wewnętrznych i zewnętrznych zagrożeniach dla bezpieczeństwa narodowego. Natomiast jako cel praktyczny przyjęto określenie założeń i zaprezentowanie koncepcji budowy spójnego, wielowymiarowego systemu antydostępowego, który może wzmocnić odporność naszego państwa. Dlatego też dysertacja ma charakter nie tylko poznawczy, ale także utylitarny.

1.3. Problemy badawcze

Punktem wyjścia wszelkiego rodzaju procesów badawczych jest sformułowanie pytania, czy też zbioru pytań, które mają postać problemu i od którego powinno rozpoczynać się każde badanie. Dwa terminy: *problem* i *pytanie* występują w badaniach nader często i równie często bywają uważane za same przez się zrozumiałe i niewymagające żadnego wyjaśnienia[29]. J. Pieter problem badawczy traktuje jako „[…] swoiste pytanie, określające jakość i rozmiar pewnej niewiedzy (pewnego braku w dotychczasowej wiedzy) oraz cel i granice pracy naukowej”[30]. Inne spojrzenie na pojęcie problemu badawczego przedstawia W. Zaczyński, według którego „[…] sytuacja problemowa, którą jest zetknięcie człowieka z trudnością wraz z uświadomieniem sobie jej charakteru, prowadzi do stawiania pytań najpierw ogólnych, potem coraz bardziej szczegółowych”[31]. Natomiast w naukach o bezpieczeństwie problem badawczy – jak zauważa M. Cieślarczyk – rozumie się najczęściej jako „pytanie, na które badacz poszukuje odpowiedzi, zbierając i przetwarzając w sposób naukowy niezbędne informacje. Powinny to być informacje adekwatne do potrzeb, wiarygodne i wyczerpujące”[32].

Przedstawiona powyżej problematyka badawcza implikuje chęć uzyskania odpowiedzi na następujące pytanie główne, czyli problem główny, który brzmi następująco: w jakim stopniu budowa własnego narodowego systemu antydostępowego wpłynie na poziom odporności Polski, a tym samym na zwiększenie bezpieczeństwa narodowego?

[29] S. Nalaskowski, *Metody badań i diagnozowania edukacji*, UMK-MEN, Toruń 2000, s. 6.
[30] J. Pieter, *Zarys metodologii pracy naukowej*, PWN, Warszawa 1975, s. 90.
[31] W. Zaczyński, *Praca badawcza nauczyciela*, PWN, Warszawa 1995, s. 19-20.
[32] M. Cieślarczyk, dz. cyt., s. 218.

W wyniku operacjonalizacji problemu głównego dysertacji sformułowano następujące szczegółowe problemy badawcze, których rozwiązanie przyczyniło się do rozwiązania problemu głównego. Dzięki nim uzyskano odpowiedzi na następujące pytania:

1) Jaki jest charakter współczesnego środowiska bezpieczeństwa?
2) Jaka jest odporność Polski na współczesne zagrożenia?
3) Czym charakteryzują się współczesne systemy antydostępowe w wybranych państwach świata?
4) Jaki kształt powinien mieć nasz narodowy system antydostępowy?
5) Jaki może być wpływ narodowego systemu antydostępowego na bezpieczeństwo Polski oraz jakie zmiany legislacyjne, proceduralne, organizacyjne czy techniczne należy wprowadzić, aby zapewnić jego powstanie i funkcjonowanie?

1.4. Hipotezy badawcze

Próbą uzyskania odpowiedzi na sformułowane powyżej pytania badawcze są tzw. hipotezy robocze. Termin *hipoteza robocza* występuje w metodologii badań w dwóch znaczeniach: w sensie merytorycznym oraz w sensie logicznym. W pierwszym z nich termin ten oznacza koncepcję prawdopodobnej odpowiedzi na problem przed przeprowadzeniem badania. Gdy problem jest zdaniem pytającym, to hipoteza jest zdaniem oznajmującym. W sensie logicznym natomiast hipoteza jest rozumiana jako racja – dana, nieuznana i wymagająca sprawdzenia[33]. Z kolei T. Kotarbiński uznaje za hipotezę wszelkie twierdzenia częściowo tylko uzasadnione, przez to także wszelki domysł w postaci uogólnienia, osiągniętego na podstawie danych wyjściowych[34].

Z przyjętych powyżej problemów badawczych wynikają hipotezy, które są przypuszczalną odpowiedzią na zawarte w nich pytania. Główna hipoteza badawcza brzmi następująco: uważam, że w aktualnych uwarunkowaniach środowiska bezpieczeństwa Polski budowa narodowego systemu antydostępowego jest koniecznością i zdecydowanie wpłynie na podniesienie poziomu odporności naszego państwa na zagrożenia zewnętrzne oraz wewnętrzne, a tym samym przyczyni się do zwiększenia bezpieczeństwa narodowego. Wymaga to wprowadzenia wielu zmian legislacyjnych, organizacyjnych czy technicznych, a tym samym znacznych nakładów finansowych, ale należy podkreślić fakt, że bezpieczeństwo naszego państwa jest najważniejsze.

[33] S. Nalaskowski, dz. cyt., s. 10.
[34] T. Kotarbiński, *O pojęciu metody*, PWN, Warszawa 1975, s. 89.

Natomiast do zidentyfikowanych wcześniej problemów szczegółowych sformułowano następujące hipotezy szczegółowe:

H 1: oceniam, że współczesne środowisko bezpieczeństwa w perspektywie co najmniej do 2040 roku będzie cechowało się dużą złożonością i niepewnością. W konsekwencji należy liczyć się z występowaniem licznych zagrożeń, których źródłem może być zarówno podmiot państwowy, jak i niepaństwowy działający we wszystkich klasycznych domenach operacyjnych (ląd, morze, kosmos, przestrzeń powietrzna, cyberprzestrzeń), a także w domenach aktualnie pozostających poza klasyfikacją jako domena operacyjna – np. domena kognitywna. Dlatego nasze państwo powinno efektywnie rozwijać własny potencjał obronny i ochronny, aby skutecznie reagować na wszystkie zagrożenia we wszystkich stanach gotowości obronnej państwa. Ze względu na agresywną i mocarstwową politykę Rosji, traktowanej obecnie jako największe źródło zagrożeń dla Polski, podstawą odstraszania potencjalnego agresora powinny być nie tylko nowoczesne i dobrze wyposażone siły zbrojne, zdolne do prowadzenia operacji wielodomenowych, ale również efektywny system antydostępowy zdolny do neutralizowania przewagi przeciwnika.

H 2: uważam, że w budowę odpornego państwa powinny być zaangażowane wszystkie podmioty odpowiedzialne za bezpieczeństwo naszego państwa. Tylko holistyczne podejście może bowiem przynieść zamierzone efekty. Dlatego też za budowę odporności powinny być odpowiedzialne zarówno władze cywilne, jak i wojskowe. Nie można dopuścić do nieskoordynowanych działań, które w skrajnie niekorzystnych warunkach mogą doprowadzić do obniżenia, a nawet utraty odporności. Z dużym prawdopodobieństwem można założyć, że obecny stan odporności Polski jest na niskim poziomie oraz należy zintensyfikować prace nad jej wzmacnianiem.

H 3: uważam, że systemy antydostępowe funkcjonujące zarówno w Chinach, jak i w Rosji powodują powstanie następującego dylematu strategicznego dla członków Sojuszu: w jaki sposób i za jaką cenę je pokonać? Systemy te zapewniają możliwość niezakłóconej projekcji siły i osiągnięcie założonych celów w warunkach zmniejszonego ryzyka oddziaływania państw NATO. Nie do przecenienia jest także poczucie bezpieczeństwa strony dysponującej takimi systemami, chociażby dzięki możliwości zapewnienia ciągłości funkcjonowania własnych elementów infrastruktury krytycznej. Powoduje to konieczność uwzględnienia przez Sojusz wysokich strat, jak również zaplanowania ogromnego wysiłku logistycznego w celu uzyskania zakładanych rezultatów.

Niezwykle istotna jest także potrzeba przeznaczenia niebagatelnych środków finansowych na badania związane z rozwojem nowych narzędzi umożliwiających pokonanie takich systemów.

H 4: uważam, że dotychczas zbudowane systemy antydostępowe spełniają swoją funkcję głównie jako element odstraszania. Sądzę, że rozsądnie zaplanowany, we współpracy z innymi krajami regionu, system będący swojego rodzaju tarczą pozwoliłby na stworzenie warunków powodujących u przeciwnika poczucie niepewności w zakresie szacunkowych zysków. Budując taki system, nie można jednak skupić się tylko na budowie tarczy, za którą można bezpiecznie się ukryć. Należy także podjąć kroki zmierzające do tworzenia zdolności do rażenia przeciwnika we wszystkich domenach, jeszcze na jego terytorium. Tylko taki skoordynowany system tarczy i włóczni pozwoli na pojawienie się u przeciwnika przeświadczenia o niecelowości ataku.

H 5: oceniam, że właściwie rozwinięty w oparciu o koncepcję prowadzenia operacji wielodomenowych – narodowy system antydostępowy w znaczący sposób poprawi odporność Polski w niektórych jej obszarach. Właściwie skoordynowane i zsynchronizowane działania w obszarach dowodzenia, rozpoznania, rażenia, obrony przed uderzeniami oraz zabezpieczenia logistycznego w każdej z istniejących domen operacyjnych pozwoli na uzyskanie zmultiplikowanego efektu. Należy jednak podkreślić fakt, że przygotowanie takiego systemu będzie wymagało przeprowadzenia zmian prawnych, zakupu odpowiedniego sprzętu do realizacji zaplanowanych działań, jak również zmian w procesie szkolenia.

1.5. Metody, techniki i narzędzia badawcze

Właściwa (metodologicznie) weryfikacja hipotez jest warunkiem koniecznym do konstruowania twierdzeń naukowych, a w rezultacie budowania wiedzy naukowej, która w przeciwieństwie do wiedzy potocznej ma ustalony stopień pewności, wynikający z procesu badawczego. J. Lutyński podkreśla, że „[…] wiedza będąca rezultatem badań zmierza do obiektywizacji, do uniezależnienia od doznań poszczególnych jednostek, a nawet grup, do tego, aby mogła być zaakceptowana przez wszystkich na podstawie określonych danych”[35]. Z poglądami Lutyńskiego koresponduje twierdzenie B. Wiśniewskiego o potrzebie dostarczenia (dzięki zastosowaniu metody badawczej adekwatnej do przedmiotu badań, celu i problemu badawczego) informacji pozwalających na udzielenie wiarygodnych

[35] J. Lutyński, *Metody badań społecznych*, Łódzkie Towarzystwo Naukowe, Łódź 2000, s. 13.

i wyczerpujących odpowiedzi na pytania problemowe[36]. Istotnym elementem jest podkreślenie znaczenia metody naukowej w procesie badawczym. Według T. Tomaszewskiego „[…] metoda naukowa [w tym rozumieniu jako metoda badawcza] jest to sposób dochodzenia do twierdzeń uzasadnionych i sprawdzonych, czyli zespół czynności, które należy wykonać, i procesów, które muszą się odbyć, aby można było uzyskać uzasadnione i sprawdzone twierdzenie o badanych faktach”[37]. Dobór odpowiedniej metody warunkuje czynności określane jako techniki badań, które „w sensie logicznym są pojęciami podrzędnymi w stosunku do metody, a w sensie rzeczowym o znacznie węższym zakresie niż metoda. Technika badawcza ogranicza się do czynności pojedynczych lub pojedynczo jednorodnych. Metoda natomiast zawiera w sobie szereg działań o rożnym charakterze, zarówno koncepcyjnym, jak i rzeczowym, zjednoczonym celem generalnym i ogólną koncepcją badań”[38].

Mając powyższe na uwadze, dla osiągnięcia założonych celów, a przy tym zachowania maksymalnego obiektywizmu prowadzonych badań, w trakcie procedury badawczej wykorzystano spektrum metod badawczych, zarówno teoretycznych, jak i empirycznych. Co istotne, metody teoretyczne, traktowane w literaturze metodologicznej także jako operacje myślowe, służyły głównie do naukowego, myślowego uporządkowania i wielostopniowego przetworzenia nagromadzonego materiału empirycznego (faktów). Metody takie jak: analiza, synteza, abstrahowanie, porównanie, uogólnianie oraz wnioskowanie były wykorzystane we wszystkich etapach prowadzonych badań, także podczas formułowania założeń badawczych.

Dzięki analizie dokonano myślowego podziału przedmiotu badań na poszczególne części składowe oraz zbadano oddzielnie poszczególne części i dzięki temu określono związki, relacje i powiązania zachodzące między nimi. Analizie poddano m.in.: systemy antydostępowe wybranych państw, dzięki czemu wykryto istotne właściwości tych systemów oraz zidentyfikowano ich wpływ na poziom bezpieczeństwa poszczególnych państw. W celu połączenia wyodrębnionych i zbadanych w toku analizy części w nową całość wykorzystano syntezę, czyli metodę, która jest ściśle związana z analizą. Dostarczyła ona istotnej i nowej wiedzy o przedmiocie badań i pozwoliła na jego całościowe ujęcie.

[36] Zob. B. Wiśniewski (red.), *Bezpieczeństwo w teorii i badaniach naukowych*, Wyd. Wyższa Szkoła Policji, Szczytno 2011, s. 137.
[37] T. Tomaszewski, *Wstęp do psychologii*, PWN, Warszawa 1963, s. 26.
[38] T. Pilch, T. Bauman, *Zasady badań pedagogicznych*, Wyd. Akademickie Żak, Warszawa 2001, s. 71.

Niezwykle ważne w toku badań było również zastosowanie analizy typu SWOT[39], którą wykorzystano przede wszystkim do uporządkowania i analizy informacji dotyczących oceny odporności Polski. Co więcej, pozwoliła ona autorowi wykorzystać zgromadzone informacje do opracowania narodowej koncepcji systemu antydostępowego, opartej na silnych stronach i szansach, przy jednoczesnym eliminowaniu bądź ograniczaniu słabych stron i zagrożeń.

Analizie towarzyszyła także metoda abstrahowania, z wykorzystaniem której eliminowano (pomijano), izolowano (odłączano) oraz wyodrębniano nieistotne elementy przedmiotu badań, szczególne te, które miały charakter drugorzędny czy przypadkowy. Dzięki temu odrzucono nieistotne relacje, cechy, czynniki, zjawiska czy procesy, pozostawiając do dalszych badań tylko te, które mają zasadnicze znaczenie dla właściwego określenia zasadności budowy narodowego systemu antydostępowego.

Porównanie wykorzystano dla wykrycia cech podobieństwa i odmienności w badanych przedmiotach, zjawiskach, procesach, przez odniesienie go do innych przedmiotów, zjawisk, procesów. Pozwoliło to ustalić podobieństwa i różnice między badanymi przedmiotami i zjawiskami. Metoda ta była zastosowana m.in. podczas oceny rozwiązań organizacyjnych systemów A2/AD obowiązujących w wybranych państwach. Wskazanie podobieństw i cech wspólnych, ale także różnic było istotne dla właściwego określenia potrzeb narodowych w tym zakresie.

Poprzez zastosowanie metody uogólnienia możliwe było formułowanie twierdzeń ogólniejszej natury. Wnioski wyciągnięte z poszczególnych jednostkowych faktów i przesłanek generalizowano, po czym ujmowano w pewną całość oraz rozszerzano na ogół lub na duży zakres zjawisk czy faktów. Dzięki tej metodzie ujawniono cechy i zjawiska powtarzalne, co z kolei prowadziło do wykrywania prawidłowości oraz formułowania na tej podstawie nowych ogólnych założeń czy też dokonywania systematyzacji według przyjętych kryteriów. Metodę tę zastosowano m.in. jako element podsumowujący każdy rozdział merytoryczny oraz w zakończeniu dysertacji.

Nieodłącznym elementem procesu badawczego jest metoda wnioskowania nazywana inaczej rozumowaniem lub inferencją. Wnioskowanie zostało wykorzystane w każdym merytorycznym rozdziale dysertacji, głównie w jego części końcowej, w której

[39] SWOT to akronim, który pochodzi od pierwszych liter angielskich słów: *Strengths* (mocne strony), *Weaknesses* (słabe strony), *Opportunities* (szanse), *Threats* (zagrożenia). Metoda została opracowana w latach 60. XX wieku na Uniwersytecie Harvard w ramach projektu badawczego. Przyp. aut.

formułowano konkluzje, a także w zakończeniu rozprawy. Pozwoliło ono na zaprezentowanie nowej wiedzy dotyczącej przedmiotu badań, uzyskanej na podstawie istniejącego już dorobku naukowego oraz przeprowadzonych badań własnych, szczególnie w obszarze funkcjonowania narodowego systemu A2/AD i jego wpływu na bezpieczeństwo Polski.

Zastosowanie metod teoretycznych pozwoliło na zastosowanie naukowego rygoru myślenia (rozumowania, wnioskowania), zapewniło analityczne zbadanie, uporządkowanie i opis materiału empirycznego (faktów) oraz jego przetworzenie, a ponadto umożliwiło dokonanie weryfikacji hipotez, jak również kreowanie nowej teorii naukowej.

Obok metod teoretycznych w procesie badawczym zastosowano także kilka metod empirycznych, które były podstawowym źródłem informacji zdobywanych, przetwarzanych i weryfikowanych. Ich istota polega na bezpośrednim kontakcie badacza z przedmiotem badań w celu poznania określonych zjawisk, procesów czy faktów, w tym także: motywów, ocen, oczekiwań, opinii, procedur oraz sądów i – na tej podstawie – następuje wykreowanie nowych faktów naukowych. Co ważne, badania empiryczne różniły się od badań teoretycznych zastosowanymi technikami i narzędziami badawczymi, charakterystycznymi dla przyjętej empirycznej metody badań. W procesie badawczym główną metodą był sondaż diagnostyczny. Uzupełniające metody stanowiły metoda obserwacyjna oraz metoda badania dokumentów. Zastosowane metody empiryczne są charakterystyczne dla badań naukowych prowadzonych w naukach społecznych. Ich wykorzystanie znacznie podniosło wartość i wiarygodność uzyskanych rezultatów badań.

Zasadniczą i najważniejszą metodą zastosowaną w badaniach eksploracyjnych był wyżej wspomniany sondaż diagnostyczny. Jest to jedna z najpopularniejszych metod badań ilościowych, której zasadniczą funkcją jest gromadzenie informacji o interesujących badacza problemach w wyniku relacji osób badanych, tzw. respondentów. W ramach metody sondażowej wykorzystano przede wszystkim technikę wywiadu[40]. Wywiady miały formę jawną, skategoryzowaną i były prowadzone w oparciu o autorski kwestionariusz wywiadu, zawierający 5 pytań problemowych dotyczących istotnych kwestii rozwiązywanych w rozprawie. Wyniki badań eksperckich wykorzystano w treści rozdziałów merytorycznych oraz udokumentowano w załącznikach (nr 1 i nr 2).

[40] Najogólniej przez metodę sondażu rozumie się metodę badań, której podstawową funkcją jest gromadzenie informacji o interesujących badacza problemach w wyniku relacji słownych osób badanych nazywanych respondentami. M. Łobocki, *Metody i techniki badań pedagogicznych,* Kraków 2003, s. 243.

W badaniach empirycznych, jako uzupełniającą, wykorzystano metodę obserwacyjną. Obserwacja naukowa, prowadzona poprzez poznawanie faktów za pomocą zmysłów, ale także ujęcie ich we wzajemne związki i zależności, dostarczyła wiele ważnych spostrzeżeń naukowych. W ramach tej metody wykorzystano zarówno technikę obserwacji bez interwencji, czyli technikę obserwacji biernej, jak i technikę obserwacji z interwencją, zwaną także techniką obserwacji czynnej, która obejmowała sytuacje, w których autor osobiście ingerował w spontaniczny tok zdarzeń[41]. Zastosowanie tej metody było możliwe podczas wykonywania przez autora obowiązków i zadań służbowych na stanowisku szefa Oddziału Doktryn Połączonych w Sojuszniczym Dowództwie ds. Transformacji (ang. *Allied Command Transformation* – ACT) w Norfolk w USA. Pozwoliła ona na uzyskanie wielu ciekawych wniosków i rekomendacji z różnych przedsięwzięć szkoleniowych (szczególnie konferencji, warsztatów czy odpraw służbowych) prowadzonych zarówno w ACT, jak i instytucjach podległych oraz współpracujących z ACT. Autor uczestniczył w nich osobiście, przeważnie jako prowadzący, sprawozdawca lub obserwator. Przyczyniło się to do zwiększenia jego wiedzy w zakresie przedmiotu badań oraz obiektywizmu podczas formułowania wniosków.

Inną uzupełniającą metodą badawczą było badanie dokumentów. Analiza dokumentów polegała na gromadzeniu, selekcji, opisie oraz naukowej interpretacji faktów zawartych w różnych źródłach informacji opublikowanych w formie dokumentów, takich jak: akty prawne; doktryny i regulaminy; rozkazy, dyrektywy czy decyzje.

Analizie poddano także literaturę przedmiotu, w tym przede wszystkim publikacje o charakterze naukowym. Do kluczowych opracowań mających największy wpływ na ostateczną postać rozprawy należy zaliczyć przede wszystkim publikacje przedstawiające różnorodne postrzeganie aspektów związanych z oceną środowiska bezpieczeństwa, analizą trendów w zmieniającym się środowisku oraz wyniki badań ich wpływu na sposób projektowania narodowego systemu antydostępowego. Jako najistotniejsze, zdaniem autora, można wskazać *Środowisko bezpieczeństwa w ujęciu międzynarodowym* autorstwa J. Stańczyka, *Środowisko bezpieczeństwa w perspektywie 2035 roku* wydane przez Centrum Doktryn i Szkolenia Sił Zbrojnych, a także publikacje zagraniczne, np. *Global Trends 2040. A more contested World* czy też wydane przez World Economic Forum *Global Risk Report 2023 – 18th Edition*. Analiza tych publikacji pozwoliła autorowi na zrozumienie zmian

[41] J. Shaughnessy, J. Zechmeister, E. Zechmeister, M. Rucińska: *Metody badawcze w psychologii*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2002, s. 87.

zachodzących w środowisku bezpieczeństwa oraz ich wpływu na bezpieczeństwo Polski. W konsekwencji umożliwiło to opracowanie propozycji budowy narodowego systemu antydostępowego.

Z kolei analiza dostępnych publikacji z problematyki związanej z odpornością oraz z systemami A2/AD pozwoliła na przeprowadzenie oceny stanu odporności Polski oraz zaprojektowanie narodowego systemu antydostępowego. Do szczególnie wartościowych pozycji należy zaliczyć zdaniem autora przede wszystkim: *Concepts and Dilemmas of State Building in Fragile Situations From Fragility to Resilience* wydane przez OECD DAC, *What is resilience* opracowane przez Stockholm Resilience Centre, *NATO 2030: na drodze do nowej strategii* J. Gotkowskiej, a także *Russia's Military Posture in the Arctic Managing Hard Power in a 'Low Tension' Environment* oraz *Russia's A2/AD Capabilities: Real and Imagined* opracowane przez M. Boulegue.

Także aktywny udział autora w pracach związanych z analizami środowiska bezpieczeństwa Polski, realizowanych w ramach projektu pk. „Nowe Urządzenie Polskie – NUP 2X35", oraz *Strategic Foresight Analysis*, realizowanej przez Allied Command Transformation (ACT), przyczynił się do zwiększenia świadomości, a w końcowym efekcie pozwolił na podjęcie samodzielnych badań związanych z oceną stopnia odporności Polski oraz nakreślenie założeń narodowego systemu antydostępowego.

Niebagatelny wpływ na ostateczny kształt przedmiotowej publikacji miały różnego rodzaju specjalistyczne analizy i raporty publikowane przez wydawnictwa branżowe czy przedstawiane przez Najwyższą Izbę Kontroli oraz te opracowane przez czołowe światowe *think tanki* (np. RAND Corporation, Atlantic Council), a związane z poszczególnymi obszarami funkcjonowania państwa.

1.6. Dobór próby badawczej i charakterystyka respondentów

Aby osiągnąć cel pracy i uzyskać odpowiedzi na wcześniej przedstawione problemy badawcze, należało przeprowadzić wszechstronne badania na reprezentatywnym materiale badawczym. W badaniach sondażowych techniką wywiadu eksperckiego w sumie wzięło udział trzydziestu pięciu respondentów-ekspertów. Jako kryterium doboru przyjęto osoby posiadające największą wiedzę specjalistyczną oraz doświadczenie związane z przedmiotem badań.

Trzydziestu z łącznej sumy respondentów stanowili oficerowie starsi zajmujący stanowiska służbowe w narodowych komórkach i jednostkach organizacyjnych poziomu strategicznego i operacyjnego oraz wyższego szkolnictwa wojskowego[42]. Każdy z nich posiadał wysoki stopień wojskowy (w badaniu wzięło udział 13 oficerów w stopniu pułkownika, 11 w stopniu podpułkownika, 4 w stopniu majora oraz 2 pracowników cywilnych resortu obrony narodowej) oraz znaczny staż służby wynoszący ponad 20 lat, co przełożyło się na uzyskanie wielu wartościowych i nowych informacji dotyczących przedmiotu badań.

Natomiast pięciu pozostałych respondentów to osoby zajmujące stanowiska w instytucjach i organizacjach zagranicznych, takich jak: Uniwersytet McGill w Montrealu (Kanada), Baltic Defence Collage w Tartu (Estonia), Uniwersytet w Granadzie (Hiszpania) oraz Chatham House – Królewski Instytut Spraw Międzynarodowych (Wielka Brytania). Wspomniani eksperci cieszą się dużym dorobkiem naukowym. Czterech spośród nich posiada stopień naukowy doktora, a jeden – tytuł naukowy profesora. Ponadto ww. eksperci dużą część swojej aktywności naukowej poświęcają dziedzinie związanej z zapewnieniem bezpieczeństwa, a w szczególności sprawom dotyczącym funkcjonowania systemów antydostępowych.

1.7. Obszar i teren badań oraz przebieg procesu badawczego

Każde badanie naukowe jest „wieloaspektowym procesem zróżnicowanych działań mających zapewnić nam obiektywne, dokładne i wyczerpujące poznanie wybranego wycinka rzeczywistości przyrodniczej, technicznej, społecznej lub kulturowej"[43]. Badania koncentrują się przede wszystkim w obszarze badawczym, który w literaturze przedmiotu nazywany jest także polem badań lub polem badawczym. Przyjęty obszar penetracji naukowej, w którym były prowadzone poszukiwania rozwiązań problemów badawczych, obejmował przede wszystkim dyscyplinę nauk o bezpieczeństwie, która obecnie zajmuje się przede wszystkim problematyką związaną ze współczesnymi systemami (modelami) bezpieczeństwa w wymiarze nie tylko militarnym, ale także niemilitarnym.

[42] Eksperci pochodzili z takich instytucji jak: Biuro Bezpieczeństwa Narodowego, Sztab Generalny Wojska Polskiego, Dowództwo Operacyjne Rodzajów Sił Zbrojnych, Dowództwo Generalne Rodzajów Sił Zbrojnych, Centrum Doktryn i Szkolenia Sił Zbrojnych, Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Centrum Operacji Powietrznych – Dowództwo Komponentu Powietrznego, Centrum Operacji Lądowych – Dowództwo Komponentu Lądowego, Dowództwo Wojsk Obrony Terytorialnej, Akademia Wojsk Lądowych, Akademia Sztuki Wojennej. Przyp. aut.
[43] W. Zaczyński, dz. cyt., s. 9.

Badania naukowe przeprowadzono trzyetapowo zgodnie ze standardami metodologicznymi: etap wstępny – konceptualizacji, etap główny oraz etap końcowy – finalizacji badań.

Etap wstępny trwał od listopada 2020 r., czyli od rozpoczęcia przez autora działalności naukowo-badawczej w celu przygotowania dysertacji w trybie eksternistycznym, do końca 2021 r. W tym czasie określono przedmiot badań i ograniczenia, cele badań, a także ogólny problem badawczy i problemy szczegółowe. Stosownie do przyjętych problemów badawczych sformułowano hipotezy badawcze, co z kolei zdeterminowało wybór metod i technik badawczych. Na tym etapie opracowano również narzędzia badawcze, podjęto decyzję dotyczącą rodzaju i wielkości próby badawczej oraz organizacji badań.

Właściwie przygotowana i zweryfikowana koncepcja badań pozwoliła nie tylko na ich sprawne przygotowanie, ale także warunkowała skuteczność procesu badawczego na etapie drugim. Na tym etapie, po wyborze terenu badań i sposobu ich realizacji, a także organizacyjnym przygotowaniu badań, nastąpiło praktyczne przeprowadzanie badań właściwych (zasadniczych). Miały one na celu zgromadzenie wartościowego i wiarygodnego materiału empirycznego zgodnie z przyjętą koncepcją rozwiązania problemów badawczych. Badania sondażowe z wykorzystaniem techniki wywiadu realizowano w okresie od września 2021 do kwietnia 2022 r. Wywiady były prowadzone podczas bezpośredniej rozmowy z ekspertami w miejscach pełnienia przez nich służby, jak również z wykorzystaniem nowoczesnych technologii informatycznych – VTC.

Metodę obserwacyjną zastosowano od lutego 2021 r. do czerwca 2023 r. podczas najważniejszych przedsięwzięć szkoleniowych (konferencji, warsztatów, ćwiczeń i treningów) realizowanych w ACT w ramach działalności służbowej autora, spośród których do największych można zaliczyć: konferencje *GlobState* (4. i 5. edycja), *Military Committee Joint Standardization Board, Allied Joint Operations Doctrine Working Group, Multi-domain Operations Workshop, Strategic Foresight Analysis Workshop* oraz *International Concept Development and Experimentation Conference*.

Z kolei badanie dokumentów oraz analizę literatury przedmiotu prowadzono w okresie od października 2019 r. do końca 2022 r.

Na etapie końcowym, czyli podczas finalizacji badań, nastąpiło przygotowanie oraz analiza uzyskanych wcześniej danych empirycznych z wykorzystaniem metod teoretycznych, w tym szczególnie wnioskowania. Skonfrontowano dane z problemami badawczymi oraz zweryfikowano przyjęte hipotezy poprzez sprawdzenie, czy znajdują one potwierdzenie w uzyskanych wynikach badań. W rezultacie stwierdzono osiągnięcie celu badań. Na tym etapie sformułowano także wnioski szczegółowe i końcowe oraz opracowano i przedstawiono zgromadzony materiał w formie rozprawy naukowej.

ROZDZIAŁ II

CHARAKTERYSTYKA WSPÓŁCZESNEGO ŚRODOWISKA BEZPIECZEŃSTWA PAŃSTWA

Rozumienie otaczającego nas świata leży u podstaw badań prowadzonych w zakresie problematyki bezpieczeństwa jednostek, społeczności, społeczeństw, państw, społeczności międzynarodowej, ich organizacji oraz podejmowanych i prowadzonych działań[44]. W tym kontekście pojęcie środowiska bezpieczeństwa należy rozumieć szerzej niż otoczenie czy system. Na przykład w naukach o zarządzaniu otoczenie definiuje się jako coś, co znajduje się poza danym układem i tym samym nie należy do tego układu. Co ciekawe, otoczenie często bywa kojarzone ze środowiskiem, ponieważ odnoszone jest do tego, co znajduje się dookoła, a więc w naszym przypadku podmiotu bezpieczeństwa oraz ludzi pozostających w jakiejś relacji (takie utożsamienie otoczenia ze środowiskiem może wydawać się przekonujące). Ponadto otoczenie może być dalsze lub bliższe, a przykłady znajdujemy w teoriach organizacji. Oznacza wówczas czynniki i procesy, które bezpośrednio i pośrednio oddziałują na daną organizację (jak przedsiębiorstwo), wpływają na warunki jej funkcjonowania, określają reguły gry, a także możliwości rozwoju, kreując szanse, ale również bariery i zagrożenia[45].

Ze względu na to, że uwarunkowania bezpieczeństwa są pochodną środowiska, w jakim funkcjonuje dany podmiot, to również problematykę wyzwań i zagrożeń dla bezpieczeństwa – jak podkreśla Jerzy Stańczyk – należy zawsze analizować w jego konkretnych uwarunkowaniach środowiskowych, ponieważ środowisko bezpieczeństwa jest właśnie tą złożoną zmienną, która ukazuje nam mnogość czynników o różnorodnym charakterze – ilościowych i jakościowych oraz wymiernych i niewymiernych. To tylko potwierdza złożoną naturę bezpieczeństwa, także jako badanej przez naukę kategorii pojęciowej[46].

Mając powyższe na uwadze, jak również przedmiot badań i obszerność przedstawianej problematyki w niniejszej dysertacji, uwaga autora w tym rozdziale została w pierwszej kolejności skupiona na środowisku bezpieczeństwa państwa jako kategorii pojęciowej, a w drugiej kolejności – zarówno na jego charakterystyce, jak i prognozie rozwoju.

---

[44] J. Gryz, *Bezpieczeństwo państwa. Władza – polityka – strategia*, Akademia Obrony Narodowej, Warszawa 2013, s. 7.
[45] A. K. Koźmiński, W. Piotrowski, *Zarządzanie. Teoria i praktyka,* Wyd. PWN, Warszawa 2002, s. 30-31.
[46] J. Stańczyk, *Środowisko bezpieczeństwa państwa w ujęciu strategicznym*, [w:] „Studia Bezpieczeństwa Narodowego", nr 1/2015, vol. 7, Wyd. WAT, Warszawa 2015, s. 145.

2.1. Pojęcie, czynniki i uwarunkowania środowiska bezpieczeństwa

Analiza literatury przedmiotu wskazuje, że środowisko bezpieczeństwa państwa należy rozumieć szeroko z uwzględnieniem nie tylko roli terytorium, lecz także czynników przestrzennych i świadomościowych. Co więcej, potwierdzeniem znaczenia środowiska bezpieczeństwa jest jakże często nadawane mu ujęcie strategiczne, wyrażane poprzez przyjęcie formuły „strategicznego środowiska bezpieczeństwa”[47]. W tym względzie warto wyjaśnić znaczenie przymiotnika „strategiczny”, który z reguły przypisywany jest podmiotom określanym jako bardzo ważne z jakichś względów, czy strategii wojennej, i wiąże się z długoterminowymi działaniami mającymi doprowadzić do wytyczonego celu. A zatem w kontekście środowiska bezpieczeństwa przymiotnik wskazuje na jego nadrzędność i priorytetowość z punktu widzenia podmiotu.

Dlatego też Zbigniew Błażewicz twierdzi, że środowisko bezpieczeństwa jest obszarem „[…] na którym dzieją się (mogą się dziać) procesy (zdarzenia) najistotniejsze dla bezpieczeństwa organizacji (państwa, sojuszu, regionu, sąsiadów, ich sąsiadów, mocarstwa, instytucji międzynarodowych), opisywanym przez zewnętrzne i wewnętrzne czynniki warunkujące realizację interesów w dziedzinie bezpieczeństwa oraz osiąganie przez tę organizację celów strategicznych”[48]. Natomiast Marian Kozub uważa, że „[…] mowa tu wszakże o środowisku, którego istotnymi składowymi są m.in.: powietrze, woda, ziemia, zasoby naturalne, flora, fauna, ludzie, ale także cyberprzestrzeń oraz ich wzajemne relacje. Jednakże istotną część tego środowiska stanowią ponadto różnego rodzaju elementy zarówno wewnątrzsystemowe, jak i zewnętrzne o charakterze międzynarodowym, warunkujące realizację interesów w dziedzinie bezpieczeństwa. Co więcej, środowisko to charakteryzuje dynamiczne tempo zmian, niepewność, niejasność i nieprzewidywalność, ale i superkonkurencyjność czy też tworzone nowe bariery, dylematy oraz problemy trudne do rozwiązania”[49]. Co ciekawe, w dalszych swoich rozważaniach M. Kozub wskazuje, że na postać współczesnego środowiska bezpieczeństwa wpłynęły zasadniczo trzy zjawiska: rewolucja informacyjna, globalizacja i rozpad świata dwubiegunowego[50]. Powyższe

[47] J. Stańczyk, *Środowisko bezpieczeństwa w ujęciu międzynarodowym*, [w:] „Rocznik Bezpieczeństwa Narodowego”, nr 2/2018, vol. 12, s. 12.
[48] Z. Błażewicz, *Strategiczne środowisko bezpieczeństwa – istota i ewolucja*, [w:] M. Kubiński (red.), *Siły Zbrojne RP w procesie budowy narodowego potencjału odstraszania*, Akademia Obrony Narodowej, Warszawa 2015, s. 18.
[49] M. Kozub, *Myśleć strategicznie o bezpieczeństwie przyszłości*, Akademia Obrony Narodowej, Warszawa 2013, s. 108.
[50] M. Kozub, *Konflikty społeczno-militarne XXI wieku. Strategiczne środowisko bezpieczeństwa do roku 2030*, Wyd. Akademii Obrony Narodowej, Warszawa 2010, s. 23.

definicje są ze sobą zbieżne i akcentują ważne procesy oraz relacje z punktu widzenia określonego podmiotu bezpieczeństwa, które mają charakter zewnętrzny i wewnętrzny. Zależności te wpływają na kształt prowadzonej polityki bezpieczeństwa i realizację związanych z tym celów.

Z kolei Marian Cieślarczyk oraz Jan Czaja podkreślają, że „[…] istotną część środowiska bezpieczeństwa państwa stanowią ponadto różnego rodzaju elementy zarówno wewnątrzsystemowe, jak i zewnętrzne o charakterze międzynarodowym, warunkujące realizację interesów w dziedzinie bezpieczeństwa. Oba ich rodzaje mogą się przejawiać w swej obiektywnej i subiektywnej istocie. Pośród czynników wewnętrznych o obiektywnej istocie dostrzegamy m.in. środowisko geograficzne, potencjał ludnościowy, gospodarczy, naukowo-techniczny i organizacyjny państwa. Do czynników subiektywnych w tym zakresie należą np. percepcja środowiska międzynarodowego, postawy społeczne, koncepcje polityczne czy jakość instytucji. W ramach uwarunkowań zewnętrznych czynnikami obiektywnymi są m.in. trendy ewolucji środowiska międzynarodowego, pozycja państwa w systemie międzynarodowym, jego struktura, zasięg powiązań międzynarodowych i poszanowanie dla określonych norm prawnych. Czynnikami subiektywnymi są natomiast percepcja środowiska międzynarodowego (podobnie jak w czynnikach wewnętrznych), stosunek do stawianych państwu oczekiwań na arenie międzynarodowej, koncepcje polityki zagranicznej i aktywność międzynarodowa. Dookreślając istotę środowiska bezpieczeństwa, powinniśmy mieć więc również na uwadze także kulturę strategiczną i kulturę bezpieczeństwa”[51].

Takie ujęcie pojęcia „środowiska bezpieczeństwa” pozwala stwierdzić, że przez wielu ekspertów jest ono postrzegane jako system kształtowany przez szereg czynników pozostających między sobą w różnych relacjach. Do tych czynników zaliczane są m.in.: położenie geograficzne (geopolityczne), interakcje pomiędzy państwami, ich miejsce i rola w strukturach międzynarodowych, a także stopień technicznego zaawansowania posiadanych sił zbrojnych. Co ważne, o istocie zmian w środowisku bezpieczeństwa przesądzają w największym stopniu: natura rozgrywających się tam wojen, zmieniające się sojusze, rozwój zagrożeń nieograniczonych granicami państwowymi i przynależnością do

[51] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa*, Wyd. Akademii Podlaskiej w Siedlcach, Siedlce 2009; J. Czaja, *Teoretyczne i praktyczne podstawy budowy kultury strategicznej w Polsce*, [w:] *Strategia bezpieczeństwa narodowego Polski*, J. Gryz (red.), Wyd. PWN, Warszawa 2013, s. 21-43

określonych organizacji, proliferacja uzbrojenia i techniki wojskowej (zwłaszcza broni masowego rażenia) oraz szybkość wszelkich zmian zachodzących w danym środowisku[52].

Tym samym, jak twierdzą Andrzej Dawidczyk i Piotr Swoboda, „[…] do najistotniejszych cech charakteryzujących środowisko bezpieczeństwa państwa należą strategiczna zmienność, nieprzewidywalność, złożoność oraz niepewność procesów i zdarzeń. Każda z tych cech oczywiście zasługuje na odrębne potraktowanie i opis, jednak wydaje się, że kluczową cechą dla współczesnego środowiska bezpieczeństwa jest jego złożoność. Złożoność jest cechą środowiska, w którym wiele procesów i zdarzeń oddziałuje na siebie na wiele sposobów, wytwarzając zupełnie nowe kombinacje. To oznacza, że nie pojedyncze, prognozowane procesy determinują funkcjonowanie państwa, lecz całe ich zbiory. Jeżeli przyjrzymy się strategiom bezpieczeństwa licznych państw europejskich, ujrzymy prostą zależność: w otoczeniu państwa może się pojawić X zagrożeń (i tu wymienia się ich treść), dlatego należy się przygotować i przeciwdziałać im w sposób Y. Przedstawia się tam zatem pewną liczbę zagrożeń, które nie są ujmowane w sposób kompleksowy. Kilka, czasem kilkanaście zagrożeń – najczęściej z różnych sfer funkcjonowania państwa – wpływając na siebie wzajemnie, wytwarza sytuacje, którym państwo (jako organizacja wielkiej grupy społecznej) nie jest często w stanie sprostać. Złożoność powoduje więc, że w bardzo krótkim czasie te zagrożenia wytwarzają hybrydy i stawiają przed krajami nowe problemy bezpieczeństwa”[53]. Wagę znaczenia złożoności współczesnego środowiska bezpieczeństwa podkreślają również wcześniej cytowani M. Kozub czy R. Zięba, którzy uważają, że o złożoności środowiska bezpieczeństwa przesądzają takie procesy i zjawiska jak: anarchiczność środowiska międzynarodowego i jego turbulencyjność, wrażliwość i podatność podmiotów na negatywne impulsy płynące ze środowiska, normatywność stosunków międzynarodowych i ich instytucjonalizacja, stosunek do wojny napastniczej oraz kontroli zbrojeń, rozwój wielostronnych form współpracy międzynarodowej, napięcia związane z terroryzmem międzynarodowym, problemy zagrożeń ekologicznych, potrzeba ograniczania przestępczości zorganizowanej, wyhamowania konfrontacji cywilizacyjno-kulturowej, a także rozwój badań na rzecz zmniejszenia śmiertelności na skutek chorób

[52] G. H. Turbiville, J. W. Kipp, W. M. Mendel, *The Changing Security Environment,* [w:] „Military Review”, Fort Leavenworth, June-July 1997.
[53] A. Dawidczyk, P. Swoboda, *Projektowanie celów polityki bezpieczeństwa na użytek strategii bezpieczeństwa narodowego*, [w:] „Bezpieczeństwo narodowe”, nr 42/2023, Wyd. BBN, Warszawa 2023, s. 17-18.

epidemiologicznych[54]. Warto w tym miejscu również zaznaczyć, że jak podkreśla J. Stańczyk „[…] częścią współczesnego środowiska bezpieczeństwa jest również toczona w nim rywalizacja o potęgę i wpływy, a przynajmniej zawsze o interesy. Sytuacja ta zmusza do porównywania oraz równoważenia sił. Zauważyć w tym kontekście należy znaczenie siły i pozycji państw w stosunkach międzynarodowych. Współcześnie siła zbrojna nie jest oczywiście jej jedynym wyznacznikiem. Liczy się potencjał zdolny do mobilizacji oraz efektywność wykorzystywania posiadanych sił i środków, przekładająca się na swoistą żywotność państwa"[55].

W podsumowaniu można stwierdzić, że środowisko bezpieczeństwa państwa zawsze posiada indywidualne cechy wynikające z jego specyfiki, lecz także jest warunkowane obiektywnie zachodzącymi zjawiskami i procesami zarówno sferze wewnętrznej, jak i międzynarodowej. Z uwagi na te czynniki i ich zmienność środowisko bezpieczeństwa odznacza się dynamiką, a niekiedy również nieprzewidywalnością. Ponadto bezpieczeństwo analizowane z wykorzystaniem kategorii środowiska bezpieczeństwa w głównej mierze zależy więc od rozwoju stosunków społecznych dokonujących się w kontekście takich najważniejszych uwarunkowań jak postęp naukowo-techniczny, determinanty kulturowo-cywilizacyjne oraz cechy stosunków międzynarodowych. Jego pojmowanie i konceptualizacja będą przebiegały w zależności od procesów zachodzących w środowisku międzynarodowym i wewnętrznym państwa, w tym w zależności od postrzeganych wyzwań, zagrożeń, ryzyka i szans.

2.2. Obecne trendy oraz prognozy rozwoju środowiska bezpieczeństwa

Analizy współczesnego środowiska bezpieczeństwa prowadzone m.in. w ramach sojuszniczych projektów jak *NATO Strategic Foresight Analysis* czy *NATO Warfighting Capstone Concept,* ukierunkowane na identyfikację oraz ocenę trendów, czynników i uwarunkowań mogących mieć wpływ na wieloaspektowo rozumiane bezpieczeństwo w wymiarze sojuszniczym i narodowym oraz sposób prowadzenia działań militarnych, wskazują jednoznacznie, że przyszłe środowisko bezpieczeństwa dalej będzie cechować nieprzewidywalność i niepewność. Tezę tę potwierdzają również podobne programy i projekty realizowane są m.in. w Stanach Zjednoczonych (ang. *Global Trends 2040*),

[54] Zob. M. Kozub, *Myśleć strategicznie o bezpieczeństwie przyszłości*, Wyd. Akademii Obrony Narodowej, Warszawa 2013, s. 29-31; R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Wyd. Naukowe Scholar, Warszawa 1999, s. 40-46.
[55] J. Stańczyk, *Środowisko bezpieczeństwa w ujęciu międzynarodowym*, dz. cyt., s. 18.

Wielkiej Brytanii (ang. *The Global Strategic Trends Programme*) czy Polsce (Nowe Urządzenie Polskie – NUP 2X35). Co więcej, uwzględniając wpływ globalizacji, należy oczekiwać poszerzenia spektrum zagrożeń i wyzwań dla bezpieczeństwa RP w perspektywie średnio- i długookresowej oraz ich ewoluowania i ciągłej transformacji. Prawdopodobnie będzie to utrudniać przewidywanie i reakcję, a ze względu na dynamikę zachodzących zjawisk w środowisku bezpieczeństwa wzrośnie również znaczenie operacyjności zarządzania system obronnym, w tym znaczenie wykorzystywania nowoczesnych technologii w celu wsparcia np. procesów decyzyjnych. Należy również uwzględniać rozszerzenie teatru prowadzenia działań wojennych (przestrzeń kosmiczna, przestrzeń informacyjna, przestrzeń informatyczna).

2.2.1. Wpływ pandemii Covid-19 na środowisko bezpieczeństwa

Powszechnie uważa się, że pandemia Covid-19 jest i będzie przez długi czas po jej zakończeniu odniesieniem dla szeregu studiów oraz analiz dokonywanych obecnie, ale też w przyszłości przez ekspertów/analityków z różnych dziedzin, w tym tych zajmujących się na co dzień kwestiami bezpieczeństwa. Wynika to m.in. z faktu, że jej implikacje społeczne, polityczne, gospodarcze, a nawet militarne mogą oddziaływać pośrednio lub bezpośrednio na bezpieczeństwo globalne, regionalne i narodowe w perspektywie zarówno długookresowej, jak i krótkookresowej. Co ciekawe, wstępne analizy wpływu Covid-19 na środowisko bezpieczeństwa wskazują, że pandemia znacznie przyspieszyła i w perspektywie kolejnych lat jeszcze bardziej przyspieszy, np. upowszechnianie się chociażby nowoczesnych technologii zarówno wśród społeczeństwa, jak i na poziomie państw[56]. To pozwala twierdzić, że pandemia Covid-19 jest raczej multiplikatorem, czyli elementem dynamizującym i podkreślającym pewne, już wcześniej obserwowane, trendy oraz tendencje w przestrzeni międzynarodowej.

Jednocześnie należy stwierdzić, że Covid-19 nie stanowił totalnego zaskoczenia dla systemów bezpieczeństwa w skali całego świata, decydentów, służb czy sił zbrojnych, ponieważ siły zbrojne państw na całym świecie nieustannie prowadzą analizy w obszarze m.in. zagrożeń biologicznych. Dotyczą one w pierwszej kolejności minimalizacji ryzyk w sytuacji wysyłania kontyngentów na misje zagraniczne lub ochrony własnych żołnierzy,

[56] Por. R. Reczkowski, J.M. Raubo, Ł. Jureńczyk, A. Podraza, P. Turowski, *Świat po pandemii Covid-19 z wojną na Ukrainie w tle. Perspektywa rozwoju ładu światowego i środowiska bezpieczeństwa do 2040 roku. Wyzwania dla bezpieczeństwa Polski. t. 1 – wymiar polityczny i geopolityczny*, Wyd. CDiS SZ, Bydgoszcz 2023, s. 20-22.

jeśli ich służba odbywa się w środowisku występowania niebezpiecznych patogenów, oraz ochrony przed możliwym użyciem broni biologicznej, zarówno przez potencjalnych aktorów państwowych, jak i niepaństwowych (organizacje terrorystyczne, sekty itp.). Należy też podkreślić, że pod koniec XX i na początku XXI wieku (szczególnie w związku z atakami terrorystycznymi 11 września 2001 r. na World Trade Center w Nowym Jorku) groźba bioterroryzmu była istotnym punktem odniesienia dla tworzenia analiz związanych z całościowymi planami antyterrorystycznymi wielu państw[57]. Co więcej, wielokrotnie spekulowano na temat użycia o wiele groźniejszych patogenów niż SARS-CoV-2, np. wywołujących gorączki krwotoczne (wirus Ebola). Istotne w tym względzie jest również to, że wcześniejsze epidemie wywołane przez koronawirusy z grupy SARS (SARS-CoV-1)[58] i MERS-EMC/2012[59] stanowiły bogate źródło analiz dla państw czy instytucji odpowiedzialnych za aspekty bezpieczeństwa. Problematyka możliwych potrzeb działania w dobie epidemii/pandemii była zakorzeniona również w przestrzeni debaty społecznej i naukowej – od wysoce eksperckich prac wirusologów, epidemiologów – po publikacje popularnonaukowe obecne w literaturze, filmie czy źródłach internetowych.

Powyższe sprawiało, że istniało powszechne społeczne przeświadczenie o przygotowaniu państw do zdarzeń o charakterze epidemicznym, ponieważ w tym względzie prowadziły szereg przygotowań obejmujących takie komponenty funkcjonalne zdolności jak: personel, sprzęt, obiekty infrastruktury, procedury itd. Okazało się jednak, że realna sytuacja kryzysowa o globalnej skali oddziaływania wykazała szereg luk w tym obszarze. Jak podnoszą w swoim opracowaniu R. Reczkowski i in., „[…] finalnie pandemia Covid-19 (w różnym stopniu) zaskoczyła systemowo władze większości państw na świecie. Co istotne, dotyczyło to także państw o najsilniejszej pozycji regionalnej, a nawet globalnej, jeśli spojrzymy np. na walkę z pandemią w USA czy Chinach. W najgorszej sytuacji znalazły się te państwa, które nie rozwijały odpowiedniego zaplecza w zakresie *obrony totalnej*, czyli mówiąc w uproszczeniu – nowoczesnego ujęcia relacji obronności danego państwa, jego obrony cywilnej, systemu opieki zdrowotnej, gospodarki, systemu

[57] Tamże, s. 20-21.

[58] Wirus SARS, czyli SARS-CoV-1, był odpowiedzialny za epidemię SARS (chorobę dróg oddechowych, określaną też mianem „zespołu ostrej, ciężkiej niewydolności oddechowej") w latach 2002–2003. Jest to wirus należący do rodziny koronawirusów – podobnie jak znany nam dzisiaj SARS-CoV-2 – odpowiedzialny za chorobę Covid-19. Przyp. aut.

[59] MERS-EMC/2012, inaczej HCoV-EMS/2012 jest szóstym koronawirusem, o którym wiadomo, że infekuje ludzi i pierwszym ludzkim wirusem w linii betakoronawirusa C. Jest związany z koronawirusami nietoperzy, w szczególności egipskim nietoperzem grobowym i nie jest tym samym co SARS-CoV, ale jest z nim spokrewniony i wywołuje ostrą niewydolność oddechową. Przyp. aut.

finansowego itd. Uwidoczniły się również wszelkie mankamenty, jeśli chodzi o specyfikę zarządzania kryzysowego w przypadku łańcuchów dostaw kluczowych środków ochronnych oraz urządzeń z zakresu ratowania życia i zdrowia. Trzeba bowiem podkreślić, że wysoce problematyczne było chociażby pozyskiwanie maseczek ochronnych, ubrań ochronnych, nie mówiąc o bardziej skomplikowanym sprzęcie medycznym (np. respiratory). W odniesieniu do tego problemu kluczowa stała się dyskusja o dwóch elementach: służbach specjalnych oraz globalizacji z jej rozbudowanymi łańcuchami dostaw oraz rozmieszczeniem procesów produkcyjnych w państwach o najniższych kosztach pracy lub/i posiadających niższe standardy, jeśli chodzi o regulacje prawne względem przemysłu. Służby specjalne gwarantowały bowiem możliwości reaktywnego, ale mniej lub bardziej skutecznego wyławiania zmniejszających się w toku pierwszych fal pandemii zapasów. Co więcej, stały się kluczowym komponentem w sferze utrzymania orientacji przez rządy w warunkach szumów informacyjnych oraz zmieniającej się sytuacji polityczno-gospodarczej w skali globalnej, nie mówiąc nawet o wzrastających potrzebach kontrwywiadowczych. Zakres tych zadań był niezwykle szeroki począwszy od ochrony państwa przed możliwym oddziaływaniem informacyjnym, ukierunkowanym na destabilizację, tworzenie podziałów czy też wywoływanie paniki i niechęci względem władz, służb mundurowych i służby zdrowia aż po niezbędne zwiększenie ochrony sfery badań i rozwoju – w szczególności w obszarze medycyny i farmacji”[60].

Warto w tym miejscu podkreślić również fakt, że w ujęciu historycznym jakiekolwiek epidemie nie są zjawiskami wyjątkowymi, ale w zglobalizowanym, rozwiniętym świecie, w którym gospodarka opiera się na niezwykle złożonych, międzynarodowych łańcuchach produkcji i dostaw, perturbacje spowodowane epidemią na taką skalę jeszcze nie występowały. Jak zauważa Polski Instytut Ekonomiczny, pandemia Covid-19 – w odróżnieniu od ostatniego światowego kryzysu mającego miejsce w latach 2007–2009 – dotknęła kluczowe mechanizmy rynkowe, zarówno podaż, jak i popyt. Podaż została zachwiana w momencie przerwania łańcuchów dostaw, przede wszystkim z Chin, obnażając przy okazji nieodłączne słabości tych łańcuchów czy powodując przetasowania w globalnych łańcuchach dostaw. Następnie działania rządów doprowadziły do obniżenia poziomu aktywności gospodarczej, społecznej, oświatowej i kulturalnej począwszy od odwołania imprez masowych i ograniczenia zgromadzeń przez zawieszenie działalności

[60] R. Reczkowski, J.M. Raubo, Ł. Jureńczyk, A. Podraza, P. Turowski, *Świat po pandemii Covid-19 z wojną na Ukrainie w tle*…, dz. cyt., s. 21.

większości usług i branż, szczególnie w sektorze turystyki i transportu aż po wstrzymanie całej działalności poza niezbędną do funkcjonowania (ang. *lockdown*). Te działania z kolei obniżyły podaż, ale też ograniczyły popyt, redukując niemal w jednej chwili źródła dochodów wielu pracowników[61].

W ogólnej konstatacji – porównując oceny wielu ekspertów zajmujących się problematyką bezpieczeństwa – można powiedzieć, że pandemia Covid-19 z punktu widzenia nauk o bezpieczeństwie przybrała dwa oblicza. Z jednej strony, jak każdy kryzys, wygenerowała olbrzymie zagrożenia (np. zagrożenie epidemiczne, wzrost niepokojów społecznych spowodowanych wzrostem nakazów i zakazów ze strony państwa czy szerzącą się dezinformację w mediach społecznościowych itd.), w tym zagrożenia gospodarcze wynikające z zerwania tradycyjnych łańcuchów dostaw, głównie z Azji. Z drugiej jednak strony dostrzec należy szanse kreowane przez Covid-19 (np. skrócenie łańcuchów dostaw poprzez przeniesienie produkcji do Polski lub regionu Europy Środkowo-Wschodniej itd.)[62].

2.2.2. Wymiar polityczny i geopolityczny środowiska bezpieczeństwa

Przeprowadzone dotychczas badania środowiska bezpieczeństwa wskazują, że w jego wymiarze polityczno-geopolitycznym aktualnie mamy do czynienia z trzema dominującymi trendami. Pierwszy z nich dotyczy przebudowy ładu międzynarodowego prawdopodobnie w kierunku świata wielobiegunowego i policentrycznego, ale z dwoma biegunami dominującymi pod przywództwem USA z jednej strony i Chin – z drugiej. W trendzie drugim zauważa się, że świat znajduje się w strategicznej erze rywalizacji, w której nie ma już jednego państwa (globalnego przywódcy) posiadającego dominującą nad innymi państwami pozycję strategiczną. Natomiast trzeci trend wskazuje, że to obszar Indo-Pacyfiku staje się aktualnie gospodarczym centrum świata i prawdopodobnie główną areną rywalizacji o globalną dominację pomiędzy USA a Chinami w perspektywie co najmniej do 2040 roku[63].

Jak zauważa Komisja Europejska w swoim raporcie pt. *Strategic Foresight Report 2023*, w trwającym procesie przebudowy relacji międzynarodowych „[…] różni międzynarodowi aktorzy przyjmują nowe, często bardziej konfrontacyjne role. Wojna Rosji

[61] Zob. J. Grzeszak, F. Leśniewicz, P. Śliwowski, I. Święcicki, *Pandenomics: Zestaw narzędzi fiskalnych i monetarnych w dobie kryzysów*, Polski Instytut Ekonomiczny, Warszawa 2020.
[62] Zob. R. Reczkowski, J.M. Raubo, Ł. Jureńczyk, A. Podraza, P. Turowski, *Świat po pandemii Covid-19 z wojną na Ukrainie w tle…*, dz. cyt., s. 22; *Global Trends 2040: A More Contested World*, National Intelligence Council, Washington 2021.
[63] Tamże, s. 34.

przeciwko Ukrainie podważyła fundamenty multilateralizmu i międzynarodowego porządku opartego na zasadach. Chiny wkraczają w nową erę, koncentrując się na wpływach gospodarczych i dyplomatycznej asertywności, dążąc do systemowej zmiany porządku międzynarodowego. Pozostają systemowym rywalem i konkurentem gospodarczym, będąc jednocześnie partnerem wielostronnym. Natomiast USA podążają kursem głębokiej integracji polityki wewnętrznej i zagranicznej. Obejmuje to m.in.: wzmocnienie bazy przemysłowej, ochronę technologii nowej generacji, współpracę z partnerami międzynarodowymi w celu rozwijania partnerstw gospodarczych skoncentrowanych na globalnych wyzwaniach oraz mobilizację inwestycji w gospodarki wschodzące. Obserwujemy również rosnące dążenie krajów wschodzących do uzyskania wpływów i reprezentacji na forach międzynarodowych. Należą do nich potęgi o różnych modelach zarządzania i wartościach, kraje *hedgingowe* (wykazujące połączenie strategii współpracy i konfrontacji), a także mniejsze i niestabilne państwa domagające się sprawiedliwości klimatycznej”[64].

Z perspektywy bezpieczeństwa Polski jednym z największych źródeł niestabilności dla naszego państwa jest trwający konflikt rosyjsko-ukraiński oraz agresywna polityka Rosji w bliskim sąsiedztwie Polski. W perspektywie długoterminowej konflikt rosyjsko-ukraiński może zostać „zamrożony”, podobnie jak miało to miejsce z innymi konfliktami na obszarze poradzieckim trwającymi latami. Nie oznacza to jednak neutralizacji zagrożeń z nim związanych. Niestabilna sytuacja w Ukrainie będzie stanowić dogodny instrument polityki Rosji wpływania na sytuację bezpieczeństwa w Europie. Wobec powyższego jak wskazują wcześniej cytowani R. Reczkowski i in. „[…] prognozuje się, że w perspektywie kolejnej dekady, a prawdopodobnie również w perspektywie 2040 roku, Rosja:

- pomimo strategicznego osłabienia wywołanego konfliktem w Ukrainie oraz izolacji na arenie międzynarodowej dalej będzie wykorzystywała czynnik siły militarnej w formułowaniu presji względem NATO i państw zbliżonych interesami do Zachodu, szczególnie w kontekście ograniczonych pól manewrowania w innych aspektach relacji międzynarodowych (np. w obszarze handlu metalami szlachetnymi czy metalami ziem rzadkich);

[64] Por. *Strategic Foresight Report 2023*, European Commission, Brussels 2023, s. 8.

- będzie dążyć do pełnej integracji z Białorusią (politycznie, gospodarczo i militarnie), *de facto* ubezwłasnowolniając Białoruś i czyniąc ją zależną tylko od siebie;
- będzie pozostawać w niepewności strategicznej co do dalszego pogłębiania współpracy z ChRL, jednocześnie pozostanie skłonna do budowy tzw. bloku autokratycznego stojącego w opozycji do tzw. bloku zachodniego (demokratycznego) pod globalnym przywództwem USA;
- w celu zrekompensowania sobie strat poniesionych w wyniku rozpętania wojny w Ukrainie prawdopodobnie będzie dążyć do szybkiego przejęcia kontroli nad obszarami spornymi w rejonach arktycznych i zastosowania znanej sobie polityki faktów dokonanych; jednocześnie wywołując dodatkowe spory i napięcia, Rosja może zostać zmuszona do ograniczenia zaangażowania militarnego w innych kluczowych dla jej mocarstwowej polityki regionach świata;
- będzie kontynuowała próby podważania efektywności Zachodu, przede wszystkim w przestrzeni transatlantyckiej za pomocą rozbudowanego aparatu służb specjalnych, działań w cyberprzestrzeni oraz przestrzeni informacyjnej;
- będzie dążyć do większego zaangażowania w rywalizację na Bliskim Wschodzie oraz w Afryce; analogicznie możliwe są próby zagospodarowania rosyjskich aktywów operacyjnych w Naddniestrzu oraz w rejonie Bałkanów, szczególnie w Serbii, Bośni i Hercegowinie, Czarnogórze; możliwe są również zakulisowe działania w kooperacji z przestępczością zorganizowaną, w tym operacje pod fałszywą flagą nakierowane na zwiększenie zagrożeń niewojskowych i obniżenie poczucia bezpieczeństwa w całej Europie;
- mając status państwa „zbójeckiego" na Zachodzie istnieje wysokie prawdopodobieństwo zaostrzenia konfrontacji z dotychczasowymi partnerami Moskwy, którzy w pewien sposób dla Rosji znów stali się przeciwnikami. W tym względzie Kreml już zawiesił lub całkowicie może odejść od wielu porozumień z krajami Zachodu, w tym m.in. od porozumienia z USA w sprawie nierozprzestrzeniania broni atomowej, co z kolei może otworzyć drogę do otwartego wspierania przez Rosję programów atomowych realizowanych np. przez Iran czy Koreę Północną. Niepokoi również odejście Rosji od porozumienia w zakresie poligonowych testów broni jądrowej, co należy odczytywać jednoznacznie, że Rosja

za wszelką cenę chce wzmocnić swoją politykę odstraszania nuklearnego w celu osiągnięcia założonych celów polityczno-wojskowych”[65].

Prawdopodobnie zmiany w systemie międzynarodowym spowodują również, że będzie on wymagał tworzenia nowej architektury globalnego systemu bezpieczeństwa, w tym zapewne nowej roli NATO, która pozwoli społeczności międzynarodowej uporać się z nowymi jakościowo wyzwaniami i zagrożeniami. Również Siły Zbrojne RP będą musiały redefiniować swoją rolę i zaangażowanie w tak szybko zmieniających się uwarunkowaniach. Jednocześnie nie należy zapominać, że współczesne środowisko bezpieczeństwa oprócz polityki mocarstw kształtują również zjawiska, takie jak: globalizacja, współzależności pomiędzy państwami, cyfryzacja, umiędzynarodowienie kapitału czy pogłębiająca się polaryzacja społeczeństw w wymiarze politycznym, społecznym i ekonomicznym.

2.2.3. Wymiar ekonomiczny środowiska bezpieczeństwa

W ocenie ekspertów Światowego Forum Ekonomicznego w perspektywie krótko- i długoterminowej w aspekcie ekonomicznym środowiska bezpieczeństwa na świecie może dojść do bezprecedensowego splotu kryzysów – w tym zmian klimatycznych, inflacji, konfliktów zbrojnych oraz braku bezpieczeństwa żywnościowego – w najbardziej rozwijających się krajach świata. Wyzwania te są dodatkowo spotęgowane przez dalekosiężne skutki inwazji Rosji na Ukrainę, rosnące zadłużenia w wielu krajach, skutki pandemii Covid-19 oraz niszczycielskie klęski żywiołowe. Ponadto malejące perspektywy wzrostu i kurczące się zasoby fiskalne utrudniają krajom reagowanie na te kryzysy i inwestowanie w długoterminowe priorytety rozwojowe, w tym zdrowie, edukację czy ochronę socjalną. W związku z tym przewiduje się, że do 2030 r. kraje rozwijające się będą potrzebowały średnio 2,4 mld USD rocznie, aby sprostać globalnym wyzwaniom związanym ze zmianami klimatu, konfliktami czy pandemiami[66].

Na uwagę zasługuje również fakt, że wojna na Ukrainie zapoczątkowała nową serię kryzysów w sektorze żywności i energii na świecie, wywołując kolejne problemy, które przez dziesięciolecia postępu starano się rozwiązać. Co więcej, eksperci wskazują na dalszy wzrost „starych zagrożeń”, takich jak: inflacja, kryzys kosztów utrzymania, wojny handlowe, odpływ kapitału z rynków wschodzących, powszechne niepokoje społeczne,

[65] Por. R. Reczkowski, J. M. Raubo, Ł. Jureńczyk, A. Podraza, P. Turowski, *Świat po pandemii Covid-19 z wojną na Ukrainie w tle…*, dz. cyt., s. 52-56.
[66] Zob. *Global Risk Report 2023 – 18th Edition*, World Economic Forum, Geneva 2023, s. 6-12.

zaostrzanie się konfrontacji geopolitycznej czy nawet widmo wojny nuklearnej, czyli zagrożenia z którymi niewielu współczesnych liderów biznesu i decydentów politycznych miało dotychczas do czynienia. Ponadto zagrożenia te potęgowane są przez stosunkowo nowe zmiany w globalnym krajobrazie ryzyka, w tym przez niezrównoważony poziom zadłużenia, nową erę niskiego wzrostu, niskie globalne inwestycje i deglobalizację, spadek rozwoju społecznego po dziesięcioleciach postępu, szybki i nieograniczony rozwój technologii podwójnego zastosowania (cywilnego i wojskowego) oraz rosnącą presję wpływu zmian klimatu i ambicji wielu podmiotów stosunków międzynarodowych (np. UE, ONZ) w coraz krótszym okresie przejścia do świata funkcjonującego w temperaturze wyższej o 1,5°C[67].

Wszystko to sprawia, że w perspektywie co najmniej do 2030 roku dominującą cechą środowiska bezpieczeństwa w wymiarze ekonomicznym będzie niepewność. Dodatkowo niepewność tę będzie katalizować wykorzystanie przez kluczowe podmioty państwowe i niepaństwowe zasobów naturalnych, w tym przede wszystkim surowców energetycznych[68], pierwiastków ziem rzadkich i wody słodkiej jako instrumentu oddziaływania w grze polityczno-geopolitycznej, co dodatkowo może przysporzyć kolejnych punktów zapalnych na mapie świata.

2.2.4. Wymiar społeczny środowiska bezpieczeństwa

Obserwowane zmiany w środowisku bezpieczeństwa pozwalają stwierdzić, że świat wszedł w kolejną fazę globalnych przekształceń, których konsekwencji nie jesteśmy w stanie do końca przewidzieć. Ocenia się, że największe zmiany w obszarze społecznym środowiska bezpieczeństwa prawdopodobnie są jeszcze przed nami, ale to, czego świat już doświadczył po prawie dwóch dekadach XXI wieku, można uznać zaledwie za wstęp do czekających nas w kolejnych dekadach dalszych przełomów o charakterze jakościowym, które prawdopodobnie odmienią dzisiejszy horyzont myślowy społeczeństw, a zarazem

[67] Tamże.

[68] Według ekspertów pandemia pokrywa się bardzo dobrze w czasie z wygaszaniem kluczowych kontraktów długoterminowych z jednoczesnym odtworzeniem przestrzeni do rywalizacji o rynki energetyczne. W tym względzie ocenia się, że w perspektywie najbliższych 8–10 lat zaostrzy się rywalizacja i dobór instrumentów pomiędzy największymi energetycznymi graczami, którzy jednak nie będą chcieli oddać dotychczasowej pozycji, a nowi gracze, którzy będą chcieli wejść na rynek, będą stosowali inne instrumenty, więc ta presja będzie miała charakter polityczny i ekonomiczny. W związku z powyższym rynek surowcowy może stać się rynkiem importera, a nie eksportera. Zob. M. Ruszel, *Świat po pandemii COVID-19 w wymiarze ekonomicznym i zasobów naturalnych*. Raport z webinarium przeprowadzonego 18 marca 2021 roku przez Centrum Doktryn i Szkolenia Sił Zbrojnych w ramach kampanii analiz środowiska bezpieczeństwa pk. „Nowe Urządzenie Polskie – NUP 2X35", Bydgoszcz 2021, s. 7.

ujawnią nowe perspektywy i nowe zagrożenia w obszarze społecznym, z którymi będą musiały sobie radzić następne pokolenia[69].

Zdaniem ekspertów do najważniejszych trendów wpływających na funkcjonowanie społeczeństwa dziś i co najmniej do 2040 roku będą:

1) **Zmiany demograficzne.** Poddane analizie procesy demograficzne wskazują, że sytuacja ludnościowa zarówno regionalna, jak i lokalna jest trudna, a ponadto do 2040 roku nie należy oczekiwać znaczących zmian gwarantujących stabilny rozwój demograficzny. Regres demograficzny, którego doświadczamy, wiąże się z wieloma niepokojącymi procesami społecznymi: zmianami finansowania wydatków publicznych (zabezpieczenia emerytalno-rentowe), zmianami wzorów konsumpcji i inwestycji, produktywnością pracy ludzkiej, innowacyjnością, preferencjami politycznymi, niedoborem zasobów siły roboczej oraz zmianami w obszarze nauki i edukacji. Przewiduje się, że do 2040 roku nastąpi duży wzrost zapotrzebowania na usługi opieki społecznej i sektora zdrowia, co jest związane bezpośrednio z szybkim starzeniem się polskiego społeczeństwa. Ponadto zbyt długo utrzymujące się niskie wskaźniki urodzeń sprawiają, że zagrożona jest odtwarzalność populacji, zanika wymiana pokoleniowa na rynku pracy, a gospodarka musi posiłkować się importem siły roboczej. W konsekwencji pojawia się nowa klasa problemów społecznych związanych z obecnością imigrantów, pogłębiającą się hybrydyzacją kulturową społeczeństwa i nierównowagą pokoleń. Wobec powyższego identyfikacja spektrum problemów (a także być może i szans) wynikających ze zmian struktury demograficznej jest konieczna w celu efektywnego reagowania na zmiany demograficzne w Polsce i w konsekwencji dostosowania procesu naboru i rekrutacji do dynamicznie zmieniających się wymogów rynku pracy[70]. Należy również podkreślić, że opisane zmiany demograficzne będą także wyzwaniem dla systemu bezpieczeństwa narodowego. Ocenia się, że zmiany zachodzące w społeczeństwie będą miały wpływ na kształt przyszłych Sił Zbrojnych RP. W tym względzie wskazuje się, że społeczeństwo tworzące Siły Zbrojne RP poddane jest wielu negatywnym czynnikom, które będą miały kolosalny wpływ na kształt i jakość przyszłej armii. Problemy dotykające społeczeństwo spowodują wiele zmian w sposobie rekrutacji i zarządzania zasobami ludzkimi. Przykładem mogą być

[69] Zob. J. Mokrzycki, R. Reczkowski, S. Cieśla, *Analiza...*, dz. cyt., s. 23.
[70] Por. *Mały rocznik statystyczny Polski 2021*, GUS, Warszawa 2021.

opisywane zmiany demograficzne, w których widoczne zjawisko starzejącego się społeczeństwa prawdopodobnie wymusi dłuższy okres aktywności zawodowej żołnierzy.

2) **Migracje.** Eksperci wskazują na szereg zagrożeń wynikających z przemieszczania się ludności, zarówno w skali lokalnej, regionalnej, jak i globalnej. Przewiduje się, że w przeciągu kolejnych dwóch dekad nastąpi istotne zróżnicowanie kulturowe, co może być powodem wzrostu nastrojów ksenofobicznych, np. wynikających z niezadowolenia obywateli w związku z zatrudnianiem obcokrajowców zamiast rodzimych pracowników. Dodatkowo środowiska migrantów, które celowo separują się od ludności miejscowej, niechętne do asymilacji i nauki języka, będą tworzyć własne organizacje kulturalne, społeczne, polityczne, bez woli akceptacji systemu prawnego oraz różnic kulturowych państwa przyjmującego – tzw. społeczeństwa równoległe. Autorzy raportu *Migrant Smuggling Networks* podkreślają, że migracje staną się przyczyną nasilenia działalności grup przestępczych, które będą wykorzystywać szlaki migracyjne w zakresie dostarczania fałszywych dokumentów, organizacji nielegalnego przekraczania granic, handlu ludźmi, w tym prostytucji i innych form wykorzystywania seksualnego, handlu organami, przymusowej pracy, żebractwa, zmuszania do działalności przestępczej[71]. Zjawisko migracji oprócz zagrożeń dla środowiska bezpieczeństwa niesie ze sobą również szanse dla kraju przyjmującego. Napływający do kraju migranci będą mogli wesprzeć utrzymanie potencjału gospodarczego poprzez uzupełnienie niedoborów siły roboczej na rynku pracy. Należy podkreślić, że jest to również szansa na pozyskanie ekspertów zwłaszcza z branż, w których wcześniej odnotowano fluktuację pracowników do innych krajów europejskich.

3) **Pogłębienie nierówności społecznych.** Badania wykazują, że nierówności społeczne nie dotyczą wyłącznie biednych krajów, w których panuje hierarchia społeczna. Dzisiaj właściwie wszystkie państwa, także te najzamożniejsze, mierzą się z problemem rosnących różnic między biednymi a bogatymi. Pogłębiająca nierówność może katalizować konflikty społeczne, np. spowodowane wsparciem socjalnym udzielanym przez państwo, obniżającym produktywność

[71] Zob. *Europol-INTERPOL Report on Migrant Smuggling Networks.* Europol.eu, 17.05.2016, pobrano z lokalizacji: https://www.europol.europa.eu/publications-events/publications/europol-interpol-report-migrant-smuggling-networks#downloads [dostęp: 14.12.2021].

i spowalniającym wzrost gospodarczy. Dodatkowo może doprowadzić do wzrostu przestępczości, szczególnie w regionach uboższych. Analizując opisywane zjawisko pod kątem środowiska bezpieczeństwa, ocenia się, że pogłębiająca się nierówność w społeczeństwie powoduje wzrost zachowań radykalnych oraz tworzenie ruchów i organizacji ekstremistycznych. W kontekście nierówności społecznych, eksperci wskazali, że wyzwaniem dla państwa będzie wspieranie nie tylko osób starszych i samotnych oraz młodzieży mającej kłopoty z nauką i problemy rodzinne, ale również rynku lokalnego, w tym przede wszystkim małych przedsiębiorstw. Nierówność społeczna może być również szansą – jako motywacja do działania dla biedniejszej części społeczeństwa. Warunkiem, który zapewni wykorzystanie tej okazji, jest zbudowanie odpowiedniego zaplecza edukacyjnego oraz zapewnienie pakietu wspierającego przedsiębiorczość wśród społeczeństwa[72].

4) **Sekularyzacja.** Nasilenie się zjawiska sekularyzacji oraz rozpowszechnienie się światopoglądów technokratycznych i konsumpcyjnych wzmocni konkurencyjne wobec Kościoła instytucje, które proponują całkiem odmienne wartości moralne. Ocenia się, że prywatyzacja i subiektywizacja przekonań religijnych doprowadzi do stopniowego osłabiania pozycji Kościoła katolickiego w Polsce. Przewiduje się, że skutkiem sekularyzacji będzie rozpowszechnienie kultury masowej, która wpłynie na podatność społeczeństwa na hasła głoszone przez fundamentalistów religijnych oraz ugrupowania terrorystyczne. Ułatwi to rozwój fundamentalizmu antyreligijnego i tworzenie nieformalnych grup religijnych, które będą realnym zagrożeniem dla środowiska bezpieczeństwa. Wyzwaniem nie tylko dla państwa, ale również dla Kościoła będzie debata o miejscu religii w sferze publicznej. Tendencja odchodzenia części społeczeństwa od zinstytucjonalizowanych kościołów może pogłębić również trend polaryzacji, ponieważ w dalszym ciągu zdecydowana większość populacji naszego kraju deklaruje przynależność do Kościoła katolickiego[73].

[72] K. Georgieva, *No lost generation: can poor countries avoid the Covid trap?* The Guardian, 29.09.2020, pobrano z lokalizacji: https://www.theguardian.com/business/2020/sep/29/covid-pandemic-imf-kristalina-georgieva [dostęp: 25.01.2022].
[73] Por. *Mały rocznik statystyczny*..., dz. cyt.

5) **Kryzys zdolności poznawczych wywołany rozwojem nowych technologii**. Technologię XXI wieku cechuje niezwykle dynamiczny rozwój. Człowiek nie zawsze nadąża za nowościami technologicznymi, zwłaszcza osoby, które ze względu na wiek bądź status majątkowy nie mają do nich swobodnego dostępu. Stwarza to zagrożenie związane z manipulacją opinią publiczną, która może doprowadzić do destabilizacji ładu społecznego. Specjaliści oceniają, że kryzys zdolności poznawczych wywołany rozwojem nowych technologii może spowodować chaos informacyjny, pogłębienie nierówności w strukturze społecznej oraz wykluczenie całych grup z wykonywania zawodów związanych z wykorzystaniem najnowszych technologii. Dodatkowo osoby wykluczone technologicznie będą narażone na cyberprzestępstwa, ponieważ do 2040 roku zdecydowana większość naszych aktywności zostanie przeniesiona do sieci. Analizując opisywany trend, przewiduje się, że wyzwaniem dla organów państwa będzie zabezpieczenie praw obywateli i instytucji publicznych, zwłaszcza w cyberprzestrzeni. Dla społeczeństwa z kolei wyzwanie będzie stanowić poddanie się zasadom demokratycznej kontroli procesu zbierania danych o ich zachowaniach w sieci, które będą niezbędne do zapewnienia bezpieczeństwa w cyberprzestrzeni[74].

2.2.5. Wymiar technologiczny środowiska bezpieczeństwa

Obszar nowoczesnych technologii jest systematycznie poddawany licznym analizom przez różnego rodzaju instytucje i organizacje, w tym wojskowe (np. NATO, Sztab Generalny WP), gdyż stanowi jeden z zasadniczych czynników oddziałujących nie tylko na człowieka, ale również na kompleksowo postrzegane środowisko bezpieczeństwa.

Jak wskazują eksperci z branży IT, w ciągu ostatnich 5 lat nastąpił wzrost inwestycji w technologie (jeden z największych w historii), a o strategicznej roli technologii w funkcjonowaniu różnych organizacji świadczyć może fakt, że wiele z nich spodziewa się zwiększenia zatrudnienia specjalistów z tego obszaru w najbliższych latach. W ocenie ww. ekspertów, tylko podczas pierwszej fali pandemii Covid-19 firmy wydawały dodatkowo około 15 mld USD tygodniowo więcej na technologie, aby zapewnić bezpieczne przejście swoich organizacji na pracę w trybie zdalnym. Co więcej, w badaniach KPMG International i Harvey Nash zauważa się, że aż 51% ankietowanych firm w skali świata wdrożyło

[74] A. Zybertowicz, *Cyber kontra real. Cywilizacja w techno-pułpace*, Wyd. Nowej Konfederacji, Warszawa 2022.

rozwiązania chmurowe, 13% prowadzi programy pilotażowe, a 21% aktywnie rozważa zastosowanie takich rozwiązań (co stanowi niemal dwukrotny wzrost w stosunku do roku 2019). Także ponad połowa liderów działów IT z Polski wdrożyła rozwiązania chmurowe, natomiast co czwarty respondent poważnie zastanawia się nad implementacją chmury w perspektywie najbliższych lat. W przedmiotowych badaniach wskazano również, że branża IT równie mocno jest zainteresowana wdrożeniem innych technologii, m.in. sztucznej inteligencji, uczenia maszynowego (29% w skali globalnej i 25% w Polsce) czy inteligentnej automatyzacji (30% w skali globalnej i 25% w Polsce). Warto w tym badaniu zwrócić również uwagę na duży globalnie wzrost popularności platform sprzedażowych w modelu SaaS – wdrożenia takich rozwiązań na dużą skalę zwiększyły się ponad trzykrotnie z 7% w 2019 roku do 23% w 2020 roku[75].

Jednakże oprócz pozytywnych aspektów dostępu do zaawansowanej technologii eksperci podkreślają, że wystąpi również szereg zagrożeń mogących nie tylko prowadzić do katastrofalnych zmian, np. w strukturach państw, społeczeństw czy uregulowań etyczno-prawnych, ale w konsekwencji do destabilizacji środowiska bezpieczeństwa, zarówno lokalnego, regionalnego, jak i globalnego. W tym względzie raport *KPMG International* i *Harvey Nash* wskazuje, że pomimo dużych nakładów finansowych zapewniających wzrost bezpieczeństwa i prywatności podczas pandemii Covid-19 aż czterech na dziesięciu badanych liderów IT na świecie zasygnalizowało, że ich firma doświadczyła większej liczby cyberataków (dla Polski wskaźnik ten jest nieco wyższy i wynosi 43 %). Ponad trzy czwarte tych cyberincydentów było związanych z *phishingiem* (83 %), a prawie dwie trzecie ze złośliwym oprogramowaniem (62 %). Dane te mogą świadczyć o tym, że nagła konieczność pracy w trybie zdalnym zwiększyła ekspozycję organizacji na potencjalne ataki cybernetyczne. Jednocześnie należy zaznaczyć, że organizacje miały trudności ze znalezieniem wykwalifikowanych specjalistów do spraw cyberbezpieczeństwa, którzy mogliby wesprzeć tę poważną zmianę organizacyjną. Według ankietowanych liderów działów IT to właśnie cyberbezpieczeństwo jest obecnie najbardziej pożądaną umiejętnością techniczną na świecie (35 % wskazań). Co ciekawe, po raz pierwszy od ponad dziesięciu lat umiejętność związana z bezpieczeństwem znalazła się na czele listy globalnych deficytów umiejętności technologicznych[76].

[75] *CIO Survey 2020 Report: Everything changed. Or did it?,* KPMG, 18.11.2020, pobrano z lokalizacji: https://assets.kpmg/content/dam/kpmg/pl/pdf/2020/11/pl-Harvey-Nash-KPMG-CIO-survey-2020.pdf [dostęp: 25.01.2021].
[76] Tamże.

Powyższe twierdzenia pozostają w pełnej zgodzie z tezami głoszonymi również przez ekspertów od nowych i przełomowych technologii, którzy wskazują, że trendy takie jak: rosnący poziom zaawansowania technologicznego, upowszechnianie stosowania nowoczesnych technologii oraz rosnąca rola sektora komercyjnego w dalszym rozwoju technologicznym społeczeństwa jutra – nadal będą utrzymywać tendencję wzrostową i co najmniej w perspektywie do 2040 roku w znaczny sposób będą oddziaływać na wszystkie wymiary środowiska bezpieczeństwa.

2.2.6. Środowisko bezpieczeństwa w aspekcie środowiska naturalnego

Kwestie dotyczące środowiska bezpieczeństwa w odniesieniu do środowiska naturalnego są w dużym stopniu zdominowane przez postępującą od co najmniej 30 lat zmianę klimatu oraz jej daleko idące i równolegle pojawiające się skutki w wymiarze globalnym, regionalnym i lokalnym. Wnioski z analiz przeprowadzonych m.in. przez Międzyrządowy Zespół ds. Zmiany Klimatu (ang. *Intergovernmental Panel on Climate Change* – IPCC) wskazują, że zmiany klimatu postępują i w perspektywie co najmniej do 2035 roku wzrośnie zarówno temperatura powietrza na obszarach lądowych i morskich, jak i temperatura wody w oceanach. Lód morski, lodowce Arktyki oraz oba lądolody będą dalej topniały, w konsekwencji czego wzrośnie poziom mórz, a także zmieni się rozkład opadów. Ponadto zmiana ta wywrze wpływ na naturalne ekosystemy i siedliska ludzkie, rolnictwo, systemy wodne oraz wzrost zagrożenia bezpieczeństwa państwa w kontekście nasilających się negatywnych zjawisk pogodowych[77].

Istotne jest to, że zmianę klimatu aktualnie należy postrzegać jako czynnik zwielokrotniający zagrożenia (ang. *threat multiplier*), który zaostrza istniejące tendencje, napięcia i sytuacje niestabilności. Głównym problemem jest jednak to, że zmiana klimatu zagraża nadmiernym obciążeniem państw i regionów, w których sytuacja już jest trudna i gdzie łatwo wybuchają konflikty. Ważne jest, aby zdawać sobie sprawę, że zagrożenia te nie mają charakteru wyłącznie humanitarnego; znajdują się wśród nich także zagrożenia polityczne i zagrożenia bezpieczeństwa, które mają bezpośredni wpływ na interesy Europy. Ponadto, zgodnie z koncepcją bezpieczeństwa ludzi, oczywiste jest, że wiele kwestii związanych z wpływem zmian klimatu na bezpieczeństwo międzynarodowe łączy się ze sobą, a więc wymaga kompleksowych rozwiązań politycznych. Na przykład osiągnięcie

[77] Zob. J. Mokrzycki, R. Reczkowski, S. Cieśla, *Analiza...*, dz. cyt., s. 41.

milenijnych celów rozwoju byłoby poważnie zagrożone, gdyż zmiana klimatu, jeśli nie zostanie złagodzona, może całkowicie przekreślić lata działań na rzecz rozwoju[78].

Zmiana klimatu będzie również wpływać na środowisko bezpieczeństwa Sojuszu (w tym Sił Zbrojnych RP) oraz na jego zdolność do prowadzenia wspólnych misji. Zmiana klimatu przede wszystkim prowadzi do nasilenia częstotliwości i skali niekorzystnych zjawisk, takich jak katastrofy naturalne (susze, powodzie), brak wody pitnej czy głód. Te z kolei potęgują napięcia ekonomiczne, społeczne i polityczne. W ten sposób przyczyniają się do migracji, terroryzmu oraz lokalnych konfliktów. Ocieplenie klimatu i topnienie lodu w Arktyce nasilają rywalizację o dostęp do złóż surowców i szlaków komunikacyjnych. Siły Sojuszu, prowadząc wspólne operacje, będą musiały być przygotowane na problemy logistyczne wynikające ze skrajnych temperatur i trudnych warunków pogodowych. Wzrost częstotliwości kryzysów będzie wywierał presję na państwa NATO, aby angażowały siły zbrojne w usuwanie skutków katastrof naturalnych oraz wykorzystywały struktury i siły Sojuszu do prowadzenia misji reagowania kryzysowego. Wzrośnie też presja na zmniejszenie emisji gazów cieplarnianych przez siły zbrojne. Z jednej strony będzie to wymuszać ich modernizację, ale z drugiej – podnosić jej koszty oraz opóźniać inwestycje w nowy sprzęt i uzbrojenie. Zmiany klimatu tworzą także polityczne wyzwania dla Sojuszu. Społeczeństwa, postrzegające zmiany klimatu jako rosnące zagrożenie, mogą kwestionować użyteczność NATO. Postrzeganie sił zbrojnych jako źródła emisji i zanieczyszczeń, a NATO – jako organizacji, która nie włącza się w walkę ze zmianami klimatu, może negatywnie wpływać na nastawienie do Sojuszu, osłabiać jego polityczną spójność i zdolność do działania[79].

Powyższe sprawia, że istnieje konieczność zwiększenia posiadanych zdolności do radzenia sobie ze zmianą klimatu (wdrożenie odpowiednich środków przystosowania się do zachodzących zmian, jak również przygotowanie infrastruktury i sprzętu). To może z kolei prowadzić do zmiany struktury wydatków państwa, w której środki te mogą zostać przekierowane na działania łagodzące skutki zmiany klimatu. Na przekształcenie tej struktury mogą mieć również wpływ, występujące na terenie nie tylko Polski, ale całej Europy coraz częściej, gwałtowne burze, trąby powietrzne, susze i powodzie wywołujące

[78] Por. *Zmiany klimatu a bezpieczeństwo międzynarodowe* (PL Version), European Commission, Brussels 2015.
[79] Por. W. Lorenz, *NATO wobec zmian klimatu – oczekiwania i możliwości,* [w:] „Biuletyn PISM", nr 215 (2147), 28 października 2020.
.

straty wśród ludzi, upraw i infrastruktury. W tym względzie zwiększające się prawdopodobieństwo występowania katastrof naturalnych może przyczynić się do coraz częstszego wykorzystywania sił zbrojnych do realizacji zadań w obszarze pomocy humanitarnej (realizacja zadań zarządzania kryzysowego). Dodatkowo podjęcie współpracy cywilno-wojskowej przy zwalczaniu skutków tych katastrof wymusza niejako większe zrozumienie i zaufanie pomiędzy podmiotami cywilnymi (w tym interesariuszami pozarządowymi) oraz wojskowymi dla zapewnienia strategicznej koordynacji, planowania i usuwania skutków katastrof, a także wsparcia humanitarnego operacji.

2.3. Konkluzje

Analiza poszczególnych wymiarów środowiska bezpieczeństwa w niniejszym rozdziale pozwala wysunąć wniosek, że przyszłe środowisko bezpieczeństwa co najmniej w perspektywie do 2040 roku będzie nadal charakteryzować się dużą dynamiką zmian i niepewnością oraz występowaniem szeregu wyzwań i zagrożeń związanych z przemianami ładu międzynarodowego, możliwością wystąpienia globalnego kryzysu gospodarczego, migracjami czy zmianą klimatu.

Istotne z punktu widzenia bezpieczeństwa Polski wydaje się to, że tworzący się na naszych oczach nowy ład międzynarodowy (najprawdopodobniej wielobiegunowy i policentryczny, ale z dwoma dominującymi biegunami) – ukształtowany częściowo przez wyzwania pochodzące z imperialistycznych ambicji Rosji i Chin – będzie przede wszystkim platformą do wzmożonej rywalizacji pomiędzy podmiotami stosunków międzynarodowych. Co ważne, prawdopodobnie nowy ład może być przyczynkiem do rozpoczęcia zarówno nowych, jak i odmrożenia starych konfliktów zbrojnych, ponieważ państwa i podmioty niepaństwowe będą wykorzystywać nowe instrumenty oddziaływania, a przy okazji niszczyć normy międzynarodowe, które zapewniały stabilność polityczną w ostatnich dziesięcioleciach. Powyższe sprawia, że możemy wyobrazić sobie wiele prawdopodobnych scenariuszy dla świata w perspektywie do 2040 r. – od demokratycznego renesansu po transformację globalnej współpracy – oczywiście w zależności od interakcji czy ludzkich wyborów w tym czasie.

Należy mieć również na uwadze, że m.in. w wyniku szybkiego postępu technologicznego, w tym technologii informacyjnych, świat w 2040 roku będzie jeszcze bardziej złożony, ale i wrażliwszy na te procesy niż jest obecnie. Wiele trendów będzie się wzajemnie przenikać, dając w rezultacie kompleksową gamę zmian i efektów, jak chociażby

poważne zmiany w polityce światowej, zmiany w funkcjonowaniu poszczególnych społeczności i całej ludzkości, dalszy dynamiczny rozwój nowoczesnych technologii czy zwiększoną dbałość o środowisko naturalne. Przedmiotowe zmiany zwielokrotnią testy systemów odporności państw czy adaptacji społeczności do zmieniających się uwarunkowań geopolityczno-społeczno-ekonomiczno-technologicznych, często przekraczając zdolność istniejących systemów i modeli. Co więcej, nierównowaga między istniejącymi i przyszłymi wyzwaniami/zagrożeniami a zdolnością państw/instytucji i systemów do reagowania na nie prawdopodobnie jeszcze bardziej wzrośnie.

Dlatego też w ogłoszonej 12 maja 2020 roku *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* zwraca się uwagę właśnie m.in. na potrzebę rozwijania zdolności odpornościowych państwa, które są niczym innym jak zdolnościami do przeciwstawiania się czemuś, niepoddawania się działaniu lub naciskowi. Odporność ta utożsamiana jest z wytrzymałością, a w rozumieniu powszechnym postrzegana jako cecha organizmu w walce z chorobami. Potrzeba ta wynika przede wszystkim z konieczności zapewniania zarówno państwu, jak i jego obywatelom poczucia bezpieczeństwa. Wydaje się zatem zasadne określenie odporności jako zdolności państwa, na wszystkich jego poziomach, do zorganizowania sytemu zapewniającego niedopuszczenie przeciwnika do rozpoczęcia ataku (w każdym wymiarze np. zbrojnym, poniżej progu wojny, cybernetycznym itd.), odparcie tego ataku, wszelką pomoc ludności poszkodowanej w wyniku tych działań w zakresie niezbędnym do zachowania zdrowia i życia, a także utrzymanie obiektów infrastruktury krytycznej w ciągłej sprawności.

ROZDZIAŁ III

DIAGNOZA ODPORNOŚCI POLSKI NA ZAGROŻENIA

Zauważa się, że w ostatnich kilku latach istotnego znaczenia nabiera potrzeba budowania odporności, czyli, w dużym uogólnieniu, zdolności organizacyjnej państwa, a w konsekwencji także Sojuszu, do radzenia sobie z przezwyciężaniem pojawiających się kryzysów. Potrzeba zapewnienia odporności wynika z kolei z istniejących oraz powstających zagrożeń naturalnych i antropogenicznych. Analizując literaturę, wsłuchując się w wystąpienia decydentów, polityków, ekspertów zajmujących się na co dzień zagadnieniami bezpieczeństwa, można odnieść wrażenie, że termin „odporność" (ang. *resilience*) jest jakimś swoistym *novum*, czymś, na co dopiero w ostatnim czasie zaczęto zwracać uwagę. Można nawet odnieść wrażenie, że termin „odporność" stał się wszechobecny.

W rzeczywistości jednak, jak zwracają uwagę Popisil i Kuehn[80], termin ten wszedł na stałe do słownictwa związanego z budową państwa już w 2009 roku. Co więcej, jednym z przewodnich tematów szczytu NATO, który miał miejsce 14 czerwca 2021 r., była właśnie odporność. W jego trakcie określono m.in., że Sojusz powinien zwiększyć swój udział w poprawie szeroko rozumianej odporności państw członkowskich. Z kolei podczas szczytu NATO w Madrycie zgodnie z deklaracją ogłoszoną 29.06.2022 r. określono między innymi, że zwiększenie odporności jest odpowiedzialnością narodową, a zarazem zbiorowym zobowiązaniem. Zwiększenie to ma nastąpić m.in. poprzez opracowanie na poziomie krajowym celów i planów wdrożeniowych oraz wzmocnienie bezpieczeństwa energetycznego. Ponadto zakłada się przyspieszenie adaptacji we wszystkich dziedzinach, co wzmocni interoperacyjność oraz odporność na zagrożenia cybernetyczne i hybrydowe. Istotnym elementem jest także zapowiedź stosowania instrumentów politycznych i wojskowych Sojuszu w sposób zintegrowany oraz zacieśnienie współpracy cywilno-wojskowej i rozszerzenie partnerstwa z przemysłem[81]. Należy również zdać sobie sprawę, że budowa i utrzymanie odpornego państwa to bezpośrednia droga do zapewnienia mu bezpieczeństwa.

---

[80] J. Popisil J., F.P. Kuehn, *The Resilient State: New Regulatory Modes in International Approaches to Statebuilding?* [w:] University of Edinburgh „Research Paper Series", nr 2016/03, Edinburgh 2016, s. 4.

[81] *Madrid Summit Declaration*, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/official_texts_196951.htm [dostęp: 20.09.2022].

Celem niniejszego rozdziału jest wskazanie istoty odporności, próba określenia jej definicji w obszarze bezpieczeństwa, wskazanie najistotniejszych zagrożeń wpływających na proces jej budowania i utrzymania, a także próba oceny odporności Polski. Ponadto podjęto próbę określenia cech, jakimi powinno charakteryzować się odporne państwo. Zastosowano w tym celu metodę analizy literatury z obszaru bezpieczeństwa oraz badań w przedmiotowym obszarze przeprowadzonych przez RAND Corporation, a także wykorzystano analizę SWOT dotyczącą oceny stanu odporności państwa polskiego.

3.1. Pojęcie odporności państwa

Biorąc pod uwagę zauważalny proces przechodzenia wyrażenia „odporność" z terminu *stricte* technicznego do określenia opisującego jeden z elementów wpływających na stan obronności państwa czy Sojuszu, zasadne staje się zdefiniowanie tego pojęcia. Ponadto mając na względzie wszechobecność tego terminu, można skonstatować, że w wielu obszarach życia codziennego oznacza on zupełnie co innego. Terminu tego używa się do opisania ludzi i systemów powracających do poprzedniej kondycji po przejściowych negatywnych zmianach w ich funkcjonowaniu. Używa się go również w odniesieniu do systemów, które są w stanie przetrwać niekorzystne zjawiska – niezależnie od tego, czy powrócą one do poprzedniego stanu czy też nie. Można zatem założyć, że słowo to nie jest jedynie pustym pojęciem, a jego powszechne stosowanie w różnych dyscyplinach, obszarach itp. sugeruje, że jest to istotny, ważny termin[82]. Co więcej, można zauważyć, że odporność jest związana ze zmianą. Biorąc z kolei pod uwagę szybkie przemiany zachodzące w środowisku, technologii i społeczeństwie, tak szerokie użycie tego terminu odzwierciedla potrzebę jego zdefiniowania.

W polskiej literaturze „odporność" jest określana jako zdolność przeciwstawiania się czemuś, niepoddawania się działaniu lub naciskowi. Utożsamiana jest z wytrzymałością, a w powszechnym rozumieniu postrzegana jest jak cecha organizmu w walce z chorobami[83]. Inaczej termin ten jest określany w obszarze gospodarki materiałowej – jako zdolność do przeciwstawiania się ciał działaniu czynników fizycznych, chemicznych, biologicznych i innych. Miarą jest wielkość zmian zachodzących w materiale pod wpływem tych czynników, np. zgniatanie, rozdzieranie, starzenie, udarność itp.[84]. Analizując z kolei

[82] K. Knuth, *The term "Resilience" is everywhere — but what does it really mean?*, ENSIA, 07.05.2019, pobrano z lokalizacji: https://ensia.com/articles/what-is-resilience/ [dostęp: 26.07.2021].
[83] *Mały słownik języka polskiego*, Wydawnictwo Naukowe PWN, Warszawa 1968, s. 490.
[84] *Encyklopedia Gospodarki Materiałowej*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1989, s. 326.

problem z punktu widzenia ochrony zdrowia, można się spotkać z następującą definicją: „[…] stan niewrażliwości na działanie drobnoustrojów chorobotwórczych”[85].

Dla uzyskania szerszej perspektywy warto zapoznać się z definicjami, z którymi można spotkać się w literaturze angielskojęzycznej. Według prof. Ann Masten z University of Minnesota College of Education and Human Development idea odporności pojawiła się w naukach społecznych już w latach 70. XX wieku. Definiuje ona odporność jako zdolność dynamicznego systemu do pomyślnego przystosowania się do zakłóceń, które zagrażają funkcji systemu, jego żywotności lub przyszłemu rozwojowi[86]. Ciekawą definicję odporności proponuje Stockholm Resilience Centre. Określa ją jako zdolność systemu czy to jednostki, lasu, miasta czy gospodarki do radzenia sobie ze zmianami i dalszego rozwoju. Wskazuje, w jaki sposób ludzie i przyroda mogą wykorzystać różnego rodzaju zakłócenia, takie jak np. kryzys finansowy czy zmiany klimatyczne, aby pobudzić odnowę i innowacyjne myślenie[87]. Z kolei wg RAND Corporation odporność można zdefiniować jako zdolność dynamicznego systemu, np. społeczność, do przewidywania i pomyślnego przystosowywania się do wyzwań. Odporność jednostki to z kolei proces, zdolność lub wynik adaptacji w obliczu przeciwności losu, traumy, tragedii, zagrożeń lub znaczących źródeł stresu[88]. Na zakończenie warto wskazać, w jaki sposób pojęcie odporności jest określane w NATO. Zwraca się uwagę, że każdy kraj członkowski NATO musi posiadać odporność, aby być zdolnym do stawiania oporu i wyjścia z poważnego kryzysu, takiego jak klęska żywiołowa, awaria infrastruktury krytycznej, atak hybrydowy lub zbrojny. Odporność jest zdolnością społeczeństwa do stawiania oporu i odzyskania sprawności po ww. kryzysach i łączy w sobie zarówno gotowość cywilną, jak i zdolności wojskowe. Gotowość cywilna jest głównym filarem odporności sojuszników i krytycznym czynnikiem umożliwiającym kolektywną obronę Sojuszu, a NATO wspiera sojuszników w ocenie i wzmacnianiu ich gotowości cywilnej[89].

---

[85] *Encyklopedia PWN*, pobrano z lokalizacji: https://encyklopedia.pwn.pl/haslo/odpornosc;3949963.html, [dostęp: 23.07.2021].
[86] A. Masten, *Ordinary Magic: Resilience in Development*, Guilford Press, Nowy Jork 2015.
[87] S. Lade, *What is resilience*, Stockholm Resilience Centre, 19.02.2015, pobrano z lokalizacji: https://www.stockholmresilience.org /research/research-news/2015-02-19-what-is-resilience.html [dostęp: 21.07.2021].
[88] J. Acosta, A. Chandra, J. Madrigano, *An Agenda to Advance Integrative Resilience Research and Practice. Key Themes From a Resilience Roundtable*, RAND Corporation, 2017, s. 2-6.
[89] *Resilience and Article 3*, NATO, 02.08.2020, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/topics_ 132722.htm, 2021 [dostęp: 26.07.2021].

Konstatując, w wyniku przeanalizowania szeregu definicji, zasadne wydaje się określenie odporności jako zdolności państwa, na wszystkich jego poziomach, do zorganizowania sytemu zapewniającego niedopuszczenie do powstania niekorzystnych zjawisk (w każdym wymiarze np. zbrojnym, poniżej progu wojny, cyberprzestrzeni, klęsk żywiołowych itd.), sprostania ich efektom, do wszelkiej pomocy ludności poszkodowanej w wyniku tych zmian w zakresie niezbędnym do zachowania zdrowia i życia, zapewnienia ciągłego funkcjonowania obiektów infrastruktury krytycznej oraz dalszego rozwoju[90].

3.2. Zasadnicze zagrożenia dla odporności państwa

Złożoność i niepewność współczesnego środowiska bezpieczeństwa sprawia, że bezpieczeństwo państwa wymaga ciągłej analizy, zarówno zewnętrznych, jak i wewnętrznych uwarunkowań oraz czynników, jakie mają wpływ na środowisko[91]. Zagrożenia z kolei mogą pochodzić od podmiotów państwowych i niepaństwowych w postaci ataków terrorystycznych, ale również ataków cybernetycznych czy działań o charakterze hybrydowym, w których mogą się zacierać granice między konwencjonalnymi a niekonwencjonalnymi formami konfliktu. Mogą one również wynikać ze zmiany klimatu i klęsk żywiołowych, takich jak powodzie, pożary i trzęsienia ziemi oraz z zagrożeń biologicznych, takich jak np. pandemia Covid-19. Wyzwanie, jakim jest dostosowanie się do tych różnych rodzajów zagrożeń i reagowanie na nie, potęgują tendencje, które zmieniają środowisko bezpieczeństwa. Także takie cechy globalnej gospodarki jak m.in.: wzrost znaczenia korporacji transnarodowych, zwiększenie wolumenu przepływów międzynarodowych czynników produkcji, procesy finansyzacji oraz uzależnienie finansowe gospodarek krajowych od kapitału zewnętrznego – stanowią istotne źródło zewnętrznych zagrożeń bezpieczeństwa ekonomicznego państwa, a w szczególności jego bezpieczeństwa finansowego. Zagrożenia te generowane są zarówno na płaszczyźnie politycznej, ekonomicznej, jak i militarnej[92].

Mając na uwadze wszystkie uwarunkowania środowiska bezpieczeństwa Polski, zaproponowaną definicję odporności oraz wyspecyfikowane cechy odpornego państwa, poniżej dokonano zestawienia możliwych zagrożeń. Przedmiotowe zagrożenia podzielono

[90] S. Cieśla, *State Resilience*, [w:] *Strategic and Operational Challenges in the (Post) Pandemic World*, GlobState, vol. 4, issue 1, Bydgoszcz 2022, s. 13.
[91] S. Koziej, F. Wołkowicz, *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON, Warszawa, 1998, s. 12.
[92] M. Redo, P. Siemiątkowski, *Zewnętrzne bezpieczeństwo finansowe państwa*, Uniwersytet Mikołaja Kopernika, Toruń 2017.

na obszary według klasyfikacji PMESII[93]. Jednakże należy mieć na względzie, że oprócz możliwości występowania tego samego zagrożenia w kilku obszarach jednocześnie same obszary nie są od siebie odseparowane. Wzajemne odziaływanie na siebie poszczególnych obszarów, np.: ekonomicznego na polityczny i odwrotnie, sprawia, że postawienie widocznej granicy między tymi obszarami jest niemożliwe[94].

1) Zagrożenia w obszarze politycznym:
   - imperialistyczna i rewizjonistyczna polityka Federacji Rosyjskiej względem byłych państw ZSRR, jak również państw Europy Środkowo-Wschodniej;
   - reorientacja USA na Azję i Pacyfik;
   - erozja dotychczasowego systemu bezpieczeństwa w Europie i rozpad dotychczasowych sojuszy;
   - osłabianie więzi w Unii Europejskiej, NATO oraz sojuszy bilateralnych;
   - działalność służb specjalnych oraz akcje propagandowo-dezinformacyjne;
   - upartyjnienie struktur państwa i naruszanie praworządności oraz słabość struktur demokratycznych[95];
   - wywieranie nacisku politycznego (groźba sankcji, embarga, blokad);
   - dyskredytacja polityków;
   - słabość systemu zarządzania kryzysowego;
   - zmniejszenie nakładów na wydatki obronne.
2) Zagrożenia w obszarze militarnym:
   - demonstracja siły związana np. z realizacją planowych lub organizowanych *ad hoc* ćwiczeń wojskowych, niezapowiedziane podnoszenie gotowości bojowej wybranych jednostek;
   - odbudowa i dyslokacja sił Zachodniego Okręgu Wojskowego[96] Sił Zbrojnych Rosji umożliwiające im szybkie i niezapowiedziane przejście do działań ofensywnych;
   - ewentualna słabość systemu dowodzenia siłami zbrojnymi;

[93] Metoda PMESII, zwana generalną segmentacją otoczenia, dzieli otoczenie na następujące obszary: polityczny, militarny, ekonomiczny, społeczny, infrastruktury i informacyjny. Przyp. aut.
[94] S. Cieślewicz, A. Skiba, R. Reczkowski, *Współczesne bezpieczeństwo transatlantyckie – implikacje dla Sił Zbrojnych RP*, Wyd. CDiS SZ, Bydgoszcz, 2018, s. 46.
[95] Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Wydawnictwo UPH, Siedlce 2016, s. 72.
[96] Od 1 marca 2024 roku Zachodni Okręg Wojskowy zostanie zastąpiony przez dwa nowe okręgi – Moskiewski Okręg Wojskowy i Leningradzki Okręg Wojskowy. Przyp. autora.

- niekompatybilność założeń doktrynalnych (w tym nierespektowanie zasad określonych w Sojuszu);
- brak lub nierespektowanie porozumień (traktatów) rozbrojeniowych;
- konflikt regionalny w pobliżu granic Polski;
- rozwijanie systemów antydostępowych przez Rosję uniemożliwiających wypełnienie przez NATO zobowiązań sojuszniczych;
- dysproporcje potencjału bojowego Rosji i Sojuszu[97].

3) Zagrożenia w obszarze ekonomicznym:
   - obniżenie tempa rozwoju gospodarczego;
   - niewykorzystanie w pełni unijnych środków pomocowych;
   - ograniczanie wymiany handlowej, w tym zakłócanie/zerwanie łańcuchów dostaw;
   - nadwyżka importu, np. artykułów spożywczych;
   - utrata rynków zbytu i ograniczenia w dostępie do rynków wewnętrznych innych państw;
   - wysoki poziom inflacji i obniżenie poziomu życia obywateli;
   - ograniczanie dostępu do nowoczesnych technologii;
   - interwencjonizm państwowy;
   - zmniejszenie wydatków na badania naukowe i promowanie innowacyjności;
   - przeniesienie działalności gospodarczej do tzw. szarej strefy.
4) Zagrożenia w obszarze społecznym:
   - niekorzystna sytuacja demograficzna – starzenie się społeczeństwa;
   - polaryzacja społeczeństwa na tle ideologicznym, religijnym, ekonomicznym itd., a w konsekwencji naruszanie praw człowieka[98];
   - wpływanie na świadomość społeczeństwa i kształtowanie jego postaw za pomocą zorganizowanej kampanii informacyjnych w różnego rodzaju mediach z wykorzystaniem metod i technik przyporządkowanych walce kognitywnej (ang. *Cognitive Warfare*);
   - niekontrolowane migracje;
   - wyalienowanie społeczne[99];

[97] C. Reach, E. Geist, A. Doll, J. Cheravitch, *Competing with Russia Militarily Implications of Conventional and Nuclear Conflicts*, RAND Corporation, Santa Monica 2021, s. 9-15.
[98] J. Mokrzycki, R. Reczkowski, S. Cieśla, *Analiza...* dz. cyt., s. 23-27.
[99] Z. Ciekanowski, J. Nowicka, H. Wyrębek, *Bezpieczeństwo…*, dz. cyt., s. 83.

- rozkład systemu służby zdrowia;
- utrata zaufania do służb mundurowych (np. policji);
- przestępczość zorganizowana.

5) Zagrożenia w obszarze infrastruktury:
   - niewystarczająca koordynacja działalności sektora państwowego i prywatnego (narodowego oraz międzynarodowego) oraz nadmierna centralizacja tego sektora;
   - niekorzystne stosunki własnościowe – większość elementów znajduje się w rękach podmiotów zagranicznych;
   - niewłaściwy sposób ochrony elementów infrastruktury krytycznej;
   - podatność na ataki cybernetyczne;
   - wykorzystywanie przestarzałej technologii;
   - działalność terrorystyczna;
   - katastrofy naturalne i budowlane.
6) Zagrożenia w obszarze informacyjnym:
   - wykorzystywanie przestarzałej technologii;
   - niewłaściwe gromadzenie, przechowywanie i przetwarzanie informacji w sieciach teleinformatycznych (np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna);
   - problemy związane z prawami obywatelskimi osób lub grup społecznych (np. sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego)[100].

3.3. Sposoby budowy odporności państwa

Jak już wcześniej wspomniano, w *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* zwraca się uwagę na potrzebę rozwijania zdolności odpornościowych państwa. Truizmem jest stwierdzenie, że o odporności powinno się mówić nie tylko w odniesieniu do stanu kryzysu lub wojny. Jej budowa i rozwój powinny przede wszystkim rozpocząć się w czasie pokoju. Dlatego też celowe jest podjęcie wszelkich wysiłków zarówno na poziomie narodowym, jak i międzynarodowym oraz sojuszniczym, aby tworzyć i utrzymać odporne państwo. Działania te powinny mieć jasno określony cel

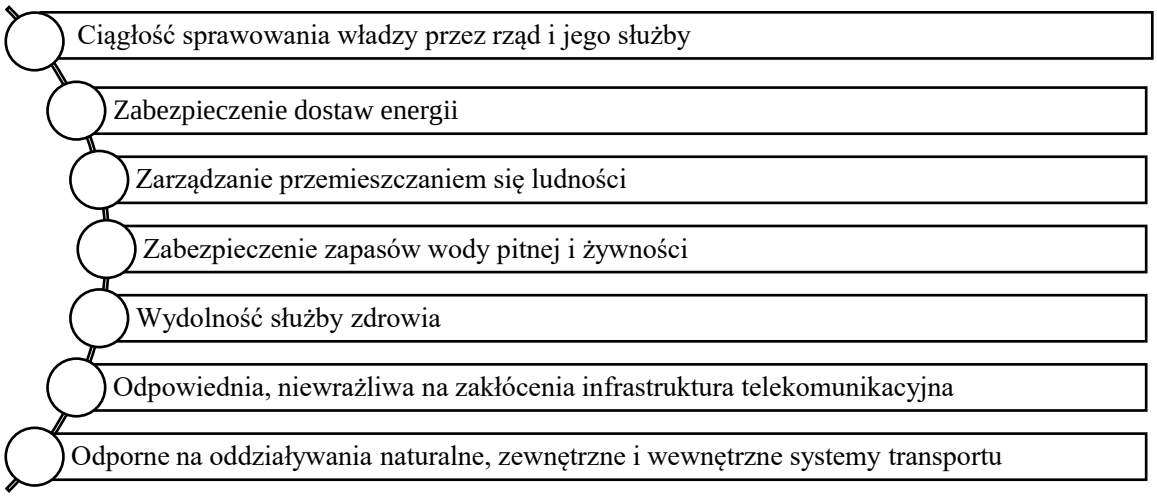
[100] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2016, s. 72-73.

i sposób jego osiągnięcia. Przede wszystkim należy zwrócić uwagę na fakt, że w myśl art. 3 Traktatu Waszyngtońskiego każde państwo jest odpowiedzialne za budowę i utrzymanie własnej odporności. W trakcie szczytu NATO w Wilnie w 2023 roku podkreślono m.in., że to właśnie Sojusz ma odgrywać znaczącą rolę w zakresie poprawy odporności państw członkowskich. Należy przy tym wspomnieć, że już w czasie szczytu NATO w Warszawie w 2016 r. stwierdzono, że to odporność jest niezbędną podstawą wiarygodnego odstraszania i obrony oraz skutecznego wypełniania podstawowych zadań Sojuszu[101]. W trakcie tego szczytu postanowiono zwiększyć odporność NATO na pełne spektrum zagrożeń i kontynuować rozwijanie indywidualnej oraz zbiorowej zdolności do przeciwstawienia się każdej formie ataku zbrojnego. To właśnie wtedy zdecydowano o przyjęciu minimalnych standardów w siedmiu obszarach: gwarancji ciągłości rządów, zabezpieczenia dostaw energii, zarządzania przemieszczaniem się ludności, wydolności służby zdrowia w czasie wojny, zabezpieczenia zapasów żywności i wody, infrastruktury telekomunikacyjnej, transportu (patrz rys. 3.1).

Na szczycie w Brukseli w 2021 r. podjęto dalsze zobowiązania w zakresie wdrażania i monitorowania podjętych zobowiązań oraz rozszerzenia wymienionych obszarów o dywersyfikację łańcuchów dostaw, a także odporności infrastruktury krytycznej (lądowej, morskiej, kosmicznej i cybernetycznej) oraz kluczowych gałęzi przemysłu[102]. Podkreślono także, że odporne państwo to państwo sprawne i bezpieczne, potrafiące sobie poradzić z kryzysami oraz zagrożeniami, które są nieuniknione we współczesnym, zglobalizowanym świecie.

W wydanym oświadczeniu po szczycie NATO w Madrycie w 2022 r. określono m.in., że odporność jest narodową odpowiedzialnością i zbiorowym zobowiązaniem. Podkreślono także, że zostanie ona zwiększona, m.in. poprzez opracowanie na poziomie krajowym celów i planów wdrażania, kierując się celami opracowanymi wspólnie przez Sojusz. Wzmocnione zostanie również bezpieczeństwo energetyczne i zostaną zapewnione niezawodne dostawy energii dla sił zbrojnych. Ponadto za konieczne uznano przyspieszenie adaptacji Sojuszu we wszystkich dziedzinach, co zwiększy odporność na zagrożenia cybernetyczne i hybrydowe oraz wzmocni interoperacyjność[103].

[101] *Commitment to enhance resilience*, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/officialtexts 133180.htm?selected Locale=en, 2016 [dostęp: 27.07.2021].
[102] J. Gotkowska, *NATO 2030: na drodze do nowej strategii*, Ośrodek Studiów Wschodnich, Warszawa 2021.
[103] Por. Deklaracja Szczytu NATO w Madrycie przyjęta przez Szefów Państw i Rządów Sojuszu uczestniczących w sesji Rady Północnoatlantyckiej w Madrycie w dniu 29 czerwca 2022 r., pobrano z lokalizacji:



Rys. 3.1. Kryteria NATO w zakresie odporności państwa

Źródło: opracowanie własne

Biorąc pod uwagę powyższe ustalenia, warto pokusić się o określenie cech, jakimi powinno się charakteryzować odporne państwo. Zdaniem autora należą do nich[104]:

- zapewniona ciągłość rządów oraz pełne i wzajemne zaufanie społeczeństwa do władzy;
- czytelny i trwały system prawny;
- zdolność do absorbowania wstrząsów oraz przekształcania i ukierunkowywania radykalnych zmian lub wyzwań przy jednoczesnym zachowaniu stabilności politycznej oraz zapobieganiu przemocy;
- umiejętność identyfikowania i przezwyciężania kryzysów z minimalnymi stratami i kosztami;
- utrzymanie wysokiego stopnia gotowości cywilnej, czyli stanu zdolności sektora cywilnego do wypełnienia warunków podjęcia i realizacji zadań ciążących na tym sektorze we wszystkich stanach obronności państwa[105];
- zagwarantowane bezpieczeństwo przepływów strategicznych, czyli ruch ludzi, towarów, technologii, wiedzy, informacji, kapitału czy danych; w przypadku ich przerwania umiejętność szybkiego powrotu do stanu poprzedniego;

https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/wystapienia/deklaracja-szczytu-nato-w-madrycie, 56384 [dostęp:19.08.2022].

[104] S. Cieśla, *State Resilience*, dz. cyt, s. 15.

[105] R. Kalinowski, *Od gotowości cywilnej do zarządzania kryzysowego,* [w:] „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa" nr 4, 2013, s. 98, *Civil preparedness*, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/topics_49158.htm,2021 [dostęp 26.07.2021], W. D. Roepke, H. Thankey, *Odporność – pierwsza linia obrony*, NATO Reviev, 2019.

- właściwa ocena ryzyka wystąpienia niekorzystnych zjawisk oraz właściwe zarządzaniem ryzykiem w celu zminimalizowania ich niekorzystnych skutków oraz sprawny i skuteczny system zarządzania kryzysowego;
- umiejętność wyciągania wniosków z doświadczeń wynikających z wcześniejszych sytuacji kryzysowych i doświadczeń innych krajów;
- sprawny, systematycznie rozwijany i testowany narodowy system obrony oraz zapewniony dostęp do infrastruktury krytycznej.

3.4. Ocena stopnia odporności Polski na zagrożenia

Określenie stopnia odporności Polski na zidentyfikowane zagrożenia jest warunkiem koniecznym do zrealizowania założonych celów przez autora niniejszej rozprawy. Oceny dokonano w kontekście odporności państwa w siedmiu obszarach określonych w czasie szczytu NATO w Warszawie w 2016 r., tj. gwarancji ciągłości rządów, zabezpieczenia dostaw energii, zarządzania przemieszczaniem się ludności, wydolności służby zdrowia w czasie wojny, zabezpieczenia zapasów żywności i wody, infrastruktury telekomunikacyjnej oraz transportu. Zdaniem autora ocena odporności Polski w tych właśnie obszarach z jednej strony pozwoli na zrozumienie wymagań stawianych przez NATO krajom członkowskim, natomiast z drugiej – umożliwi przedstawienie propozycji narodowego systemu antydostępowego jako elementu jej wzmocnienia.

Badanie zostało przeprowadzone w grupie składającej się z 35 ekspertów przy wykorzystaniu techniki wywiadu eksperckiego. Dzięki ich szerokiej wiedzy i zaangażowaniu uzyskano wiele interesujących wniosków i spostrzeżeń, które zostały zoperacjonalizowane i przedstawione w dalszej części rozprawy. W procesie badawczym wykorzystano także jedną z podstawowych metod analizy strategicznej, jaką jest analiza SWOT. Możliwość wyartykułowania mocnych i słabych stron organizacji (w tym wypadku państwa polskiego), a także szans i zagrożeń, z którymi może się ona spotkać w przyszłości, jest jedną z głównych zalet tej metody. Co więcej, ta stosunkowo nieskomplikowana metoda może być zastosowana do prawie każdego procesu niezależnie od jego wielkości. Porządkuje informacje, przedstawia rozwiązania, wskazuje przeszkody i podkreśla szanse oraz określa priorytety w zadaniach i działaniach. Ponadto dzięki wykorzystaniu tej metody można rozwinąć pełną świadomość wszystkich czynników, które mogą mieć wpływ na decyzję lub plan. Ilustruje także, jak przekształcić słabości w mocne strony, a zagrożenia w szanse, jak dopasować mocne strony do wykorzystania szans i jak zapobiec sytuacji,

w której zagrożenia staną się słabością. Z drugiej strony należy zwrócić uwagę na możliwość błędnego przedstawienia mocnych stron i słabych stron, szans i zagrożeń w przypadku samodzielnej próby ich identyfikacji bez krytycznego namysłu i analizy. Jednocześnie metoda ta, w przypadku nieumiejętnego posługiwania się nią, może utrudnić przeprowadzenie burzy mózgów i określenie barier, po to by bezkrytycznie bronić wcześniej ustalonych celów lub kierunków działania[106].

3.4.1. Ciągłość sprawowania władzy przez rząd i jego służby

Ciągłość sprawowania władzy przez rząd i podległe mu służby przejawia się w działaniach administracji publicznej na rzecz zapewnienia kluczowych procesów państwa i jest określana jako jeden z warunków zapewnienia gwarancji ciągłości rządów. Dzięki temu gwarantuje się utrzymanie w każdym czasie zdolności do podejmowania decyzji, przekazywania ich i egzekwowania oraz do świadczenia podstawowych usług rządowych na rzecz ludności. Kwestią niezaprzeczalną wydaje się fakt, że działania hybrydowe czy też bezpośredni (konwencjonalny lub inny) atak na struktury organów władzy, jak również zakłócenia procesów przez nie realizowanych, może mieć ogromny wpływ zachowanie ciągłości rządów. W konsekwencji może dojść do poważnych zakłóceń w realizacji wsparcia działań na terenie kraju oraz podważenia zaufania do organów władzy. Istotną kwestią w budowaniu odporności państwa na różnego rodzaju działania (w tym hybrydowe) jest stabilność polityczna, ekonomiczna i społeczna państwa, a przede wszystkim zdolność systemu bezpieczeństwa do rozpoznania zagrożeń, przeciwnika i możliwość podjęcia przez zagrożone państwo działań prewencyjnych[107].

Podczas próby określenia stopnia odporności państwa polskiego w tym obszarze poszczególni eksperci wskazali na wiele czynników wpływających na postrzeganie ciągłości działania administracji i zapewnienia kluczowych procesów państwa. W tabeli 3.1 przedstawiono te najczęściej wymieniane. Warto zwrócić uwagę, że większość specjalistów jako mocne strony państwa wskazała podstawy jego funkcjonowania w oparciu o wartości demokratyczne. Należy jednak wspomnieć, że niektóre kraje autokratyczne (np. Chiny) również są postrzegane jako te, w których ciągłość działania administracji i utrzymanie kluczowych procesów jest w pełni realizowane.

---

[106] *The NATO Alternative Analysis Handbook*, Edition 2, ACT, December 2017.
[107] A. Gasztold, *Zagrożenia hybrydowe dla infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, „Biuletyn Kwartalny", lipiec 2021, s.18.

Tabela 3.1.

Analiza SWOT – czynniki wpływające na ciągłość administracji publicznej i zapewnienia kluczowych procesów państwa

S	**W**
1. Stabilność[108] rządów 2. Spójne akty prawne 3. Ustrój demokratyczny 4. Pluralizm mediów 5. System parlamentarno-gabinetowy 6. Wolność słowa	1. Upartyjnienie struktur państwa i naruszanie praworządności oraz słabość struktur demokratycznych 2. Kontrowersyjny proces legislacyjny 3. Dyskredytacja polityków 4. Polaryzacja społeczna 5. Podatność gospodarki na zakłócenia 6. STRATCOM 7. Zakłócenia systemu gospodarczego państwa 8. Słabość systemu zarządzania kryzysowego 9. Problemy demograficzne
O	**T**
1. Członkostwo w UE i NATO 2. Partnerstwo strategiczne z USA 3. Sojusze regionalne i inne formy współpracy międzynarodowej 4. Współpraca z Chinami	1. Konflikt zbrojny w Europie 2. Rewizjonistyczna polityka Rosji 3. Wywieranie nacisku politycznego (groźba sankcji, embarga, blokad) 4. Podziały wewnętrzne w NATO 5. Konflikt na Pacyfiku 6. Federalizacja UE (Niemcy, Francja) 7. Zmniejszenie znaczenia Zachodu 8. Wroga propaganda i dezinformacja 9. Wzmacnianie lokalnych nacjonalizmów

Źródło: opracowanie własne

Z kolei do słabych stron eksperci zaliczyli przede wszystkim upartyjnienie struktur państwa, polaryzację społeczną (we wszystkich jego wymiarach, np. politycznym, ekonomicznym, itd.) czy też dyskredytację polityków (w wyniku własnej nieostrożności lub w wyniku działania obcych służb).

[108] Stabilność – przymiotnik *stabilis* znaczy m.in.: „trwały", „stały" i „niezmienny". Z kolei rzeczownik *stabilitas* konsekwentnie oznacza: „trwałość", „stałość", „niezmienność", a także „stały porządek". Por. J. Sondel, *Słownik łacińsko-polski dla prawników i historyków*, TAiWPN Universitas, Kraków 2006, s. 897.

Jako istotne szanse z punktu zachowania ciągłości rządów wskazywano przede wszystkim na członkostwo zarówno w Unii Europejskiej, jak i NATO, a także partnerstwo strategiczne z USA[109].

Do najczęściej identyfikowanych zagrożeń dla utrzymania ciągłości rządów zaliczono: możliwość wybuchu konfliktu zbrojnego w Europie, a także rewizjonistyczną i imperialną politykę Rosji[110]. Ponadto wskazywano na ryzyko wystąpienia konfliktu w regionie Indo-Pacyfiku, co w konsekwencji mogłoby przełożyć się na przekierowanie wysiłku militarnego USA (w szczególności) w tamten rejon.

W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron pod kątem ich znaczenia dla zapewnienia ciągłości rządów i ich ogólnych implikacji dla funkcjonowania państwa. Wyniki analizy przedstawiono jako macierz ryzyka zobrzaowaną na rys. 3.2[111]. Wynika z niego, że do najistotniejszych mocnych stron państwa polskiego w analizowanym obszarze zaliczono stabilność rządów (S1), spójne akty prawne (S2) oraz ustrój demokratyczny (S3) będący filarem systemu politycznego kraju. Z kolei jako najbardziej znaczące słabości wskazano upartyjnienie struktur państwa i naruszanie praworządności oraz słabość struktur demokratycznych (W1), możliwość dyskredytacji polityków (W3) oraz polaryzację społeczeństwa (W4).

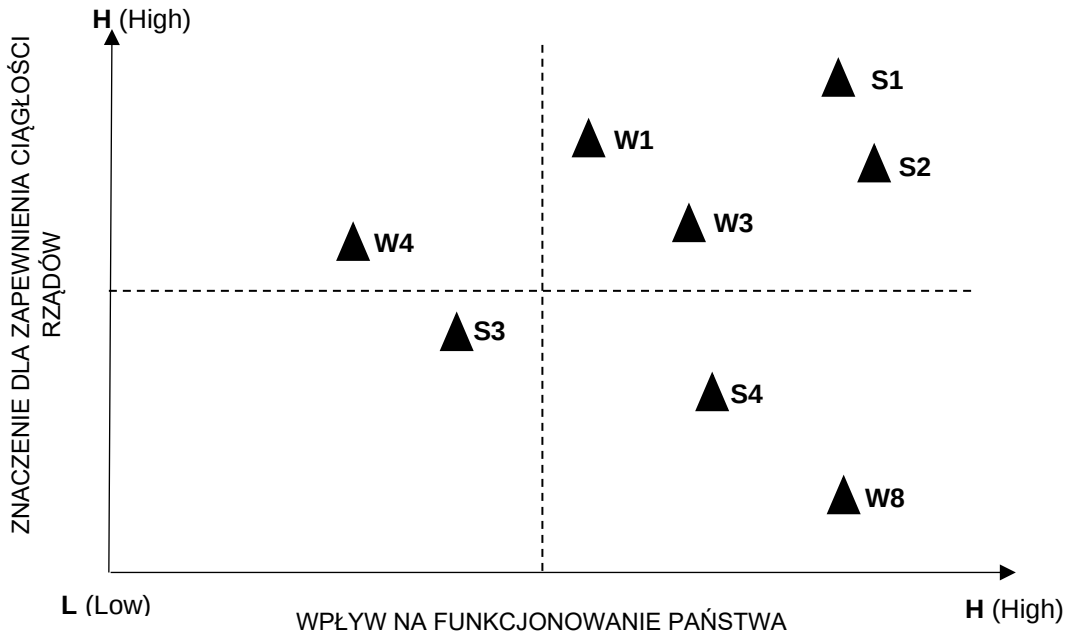
W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na zapewnienie ciągłości rządów pod względem prawdopodobieństwa ich wystąpienia, a ich wyniki zobrazowano na rys. 3.3. Jako najbardziej znaczące szanse w omawianym obszarze wskazano członkostwo w UE i NATO (O1), partnerstwo strategiczne z USA (O2) oraz możliwość uczestnictwa Polski w sojuszach regionalnych i w ramach współpracy międzynarodowej (O3). Do najistotniejszych zagrożeń dla zapewnienia ciągłości rządów zaliczono z kolei konflikt zbrojny w Europie (T1),

[109] W czerwcu 2022 r. poparcie dla Unii Europejskiej wyraziło 92% ankietowanych przy zaledwie 5% przeciwników. Poparcie dla członkostwa w NATO deklaruje natomiast 94% respondentów przy zaledwie 0,5% przeciwników. *Komunikat z badań: Opinie o integracji i działaniach UE,* nr 90/22, CBOS, lipiec 2022, ISBN 2353-5822, s. 1; *Komunikat z badań: Stosunek do NATO i obecności wojsk sojuszniczych w Polsce*, CBOS, nr 40/22, marzec 2022, ISBN 2353-5822, s. 1.

[110] Warto zwrócić uwagę, że przedmiotowe badania były prowadzone październiku i listopadzie 2021 r. Przyp. aut.

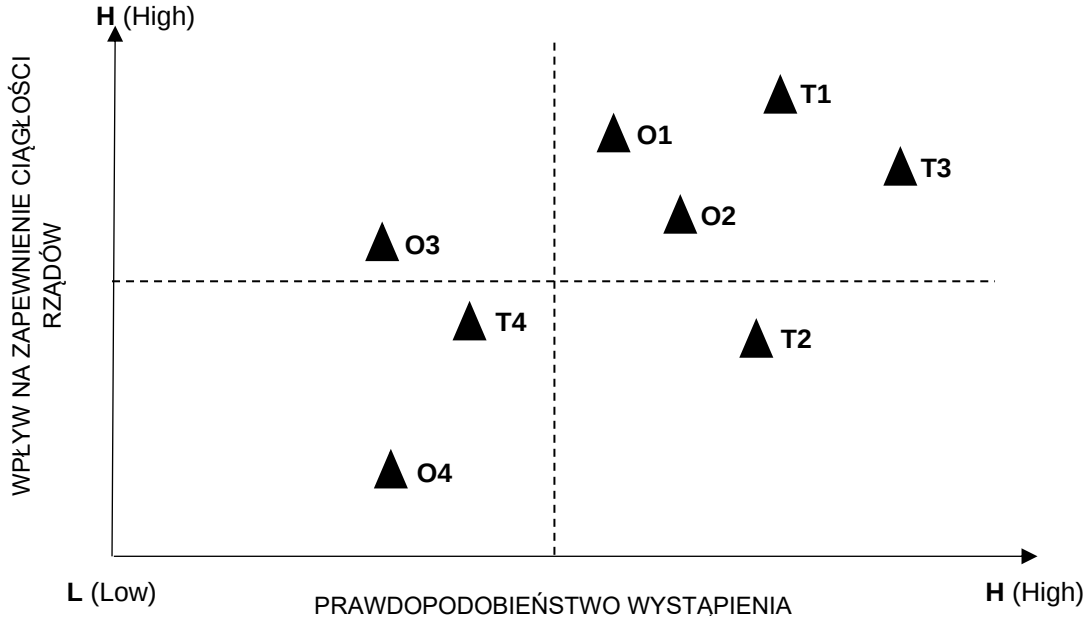
[111] Macierz ryzyka (podobnie jak w analizie pozostałych obszarów odporności państwa) wykorzystano do zidentyfikowania i określenia priorytetów poszczególnych czynników. Każda zidentyfikowana mocna (S) i słaba (W) strona została oceniona pod kątem jej znaczenia dla określonego obszaru odporności oraz jej wpływu na funkcjonowanie państwa. Po drugie, w podobny sposób oceniono szanse (O) i zagrożenia (T) pod względem prawdopodobieństwa ich występowania, a także skutków ich wystąpienia. Przyp. aut.

wywieranie nacisku politycznego (T3) a także zauważalne podziały wewnętrzne NATO (T4).



Rys. 3.2. Uszeregowanie czynników wpływających na ciągłość administracji publicznej i zapewnienie kluczowych procesów państwa pod względem stopnia ważności S/W

Źródło: opracowanie własne



Rys. 3.3. Uszeregowanie czynników zewnętrznych wpływających na ciągłość administracji publicznej i zapewnienie kluczowych procesów państwa pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

W dalszej części analizy poszczególne czynniki zostały uszeregowane zgodnie z ustalonymi w powyższych tabelach miarami ich ważności. Ich wyniki przedstawiono w tabeli 3.2.

Tabela 3.2.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S1 W1 O1 T1
	S2 W3 O2 T3
	S3 W4 O3 T4
Niski	

Źródło: opracowanie własne

Następnie został opracowany szablon matrycy konfrontacji (tabela 3.3) z wykorzystaniem czynników zidentyfikowanych w poprzednich etapach pod względem ich ważności[112]. Wypełniona matryca, pozwoliła na zwizualizowanie czynników, które muszą być wzięte pod uwagę w celu zapewnienia ciągłości rządów.

Tabela 3.3.
Ocena czynników wpływających na zapewnienie ciągłości rządów

	S1	S2	S3	W1	W3	W4
O1	++	+		--	-	-
O2	+		++	--	-	
O3	++	+		-	-	
T1	++	+				--
T3	++	+		-	-	--
T4	+			-		--

Źródło: opracowanie własne

[112] Matrycę konfrontacji (podobnie jak w analizie pozostałych obszarów odporności państwa) wykorzystano do zobrazowania, jakie mocne strony organizacji pozwalają na wykorzystanie pojawiających się szans, a które słabości na to nie pozwalają (lub w znaczniej mierze utrudniają). Z drugiej strony określono, które mocne strony organizacji pozwalają na minimalizowanie zagrożeń (lub skuteczne ich niwelowanie), a które słabości są w tym procesie przeszkodą. Po uszeregowaniu czynników przyznano odpowiednie wartości używając „+" dla pozytywów, które można wykorzystać i „-" dla negatywów, z którymi należy sobie poradzić. Więcej plusów lub minusów w komórce świadczy o silniejszym pozytywnym lub negatywnym problemie, którym powinno się zająć. Przyp. aut.

W wyniku przeprowadzonej analizy, mając na uwadze najistotniejsze (wybrane przez respondentów) czynniki, określono stopień odporności państwa w tym obszarze jako **stosunkowo wysoki**. Zwraca się jednak uwagę na konieczność wzmacniania stabilności rządów[113] poprzez wykorzystanie członkostwa w zarówno w UE, jak i NATO (a zarazem wysokiego poparcia społeczeństwa dla tych organizacji). Ponadto stabilność rządów w Polsce pozwala na czerpanie korzyści z uczestnictwa w wielu sojuszach regionalnych (np. Grupa Wyszehradzka – V4, Bukaresztańska Dziewiątka – B9) i realizację współpracy z podmiotami międzynarodowymi. Ponadto stabilność rządów umożliwia minimalizowanie potencjalnych zagrożeń, takich jak konflikt zbrojny w Europie czy też wywieranie nacisków politycznych na polskie władze ze strony adwersarzy, ale również sojuszników. Rozwinięty system demokratyczny w kraju pozwala z kolei na wykorzystanie profitów z partnerstwa strategicznego z USA w miarę na równych warunkach. W wyniku analizy określono ponadto, że szczególną uwagę należy zwrócić na konieczność podjęcia działań zmierzających do wyeliminowania upartyjnienia struktur państwa, a co się z tym wiąże – słabości struktur demokratycznych. Ta zdefiniowana słabość państwa może w konsekwencji wpłynąć na osłabienie relacji w UE, a także w NATO oraz w ramach partnerstwa z USA. Równie istotną wadą zidentyfikowaną podczas analizy jest polaryzacja społeczna, która może prowadzić do spotęgowania niekorzystnych efektów dla działalności państwa lub konfliktu zbrojnego w Europie. Co więcej, może być jednocześnie podstawą do prób wywierania nacisków politycznych na rządzących oraz wpływać na powstawanie, rozszerzanie się lub brak możliwości reagowania na podziały wewnętrzne w NATO.

3.4.2. Zabezpieczenie dostaw energii

Jednym warunków z niezbędnych do zapewnienia rozwoju państwa jest zaspokojenie jego potrzeb energetycznych[114], utrzymywanie niezawodnych i nieprzerwanych dostaw, a także utrzymanie krajowych sieci energetycznych. Zakłócenia w dostawach zarówno surowców, jak i samej energii mogą mieć zmultiplikowane skutki dla większości sektorów. Dlatego też istotnym problem staje się zapewnienie ochrony infrastruktury energetycznej,

[113] Wzmacnianie stabilności rządu to przede wszystkim zmniejszenie ryzyka niepokojów społecznych, a także ograniczenie niepewności potencjalnych partnerów (krajowych i zagranicznych. Przyp. aut.

[114] W trakcie międzynarodowej konferencji GlobState 2022 szczególną uwagę na konieczność zabezpieczenia dostaw energii zwrócił Szef Sztabu Generalnego WP generał Rajmund T. Andrzejczak. Podobną opinię wyraził Szef Sztabu Generalnego Rumuni gen. Daniel Petrescu. Sytuacja ta świadczy o dużym zrozumieniu wyzwań związanych z bezpieczeństwem energetycznym, także w kręgach wojskowych. Co więcej, problematyka ta jest uwzględniana w grach wojennych prowadzonych zarówno w Polsce, jak i w NATO. Przyp. aut.

w czasie której należy uwzględniać rozbudowane połączenia transgraniczne i rosnącą cyfryzację branży. Ze względu na posiadanie ograniczonych zasobów własnych Polska jest zmuszona do importowania szeregu surowców. W dzisiejszym zglobalizowanym świecie łańcuchy dostaw surowców energetycznych są ze sobą ściśle powiązane, przez co zapewniona jest ich duża wydajność. Z drugiej strony działania niektórych podmiotów na rynku surowców energetycznych (np. wykorzystywanie ich jako swojego rodzaju broni przez Rosję) mogą powodować poważne turbulencje dla bezpieczeństwa państwa.

W czasie prac związanych z analizą stopnia odporności państwa eksperci zaproponowali szereg czynników wpływających na zabezpieczenie potrzeb energetycznych Polski. W tabeli 3.4. zamieszczono najważniejsze z nich. Do najistotniejszych mocnych stron Polski w tym obszarze zaliczono między innymi inicjatywy podejmowane w celu dywersyfikacji dostaw surowców oraz wykorzystania *zielonej energii*[115]. Z kolei do słabych stron zaliczono przede wszystkim uzależnienie od eksportu metali ziem rzadkich[116] oraz uzależnienie od importu ropy naftowej[117] i gazu[118] z Rosji. Jako istotne szanse dla zapewnienia bezpieczeństwa energetycznego wskazano przede wszystkim możliwość dywersyfikacji pozyskiwania zasobów oraz możliwość dekarbonizacji ściśle związanej z wprowadzeniem Europejskiego

[115] Przykładem dokumentu, który przedstawia wizję długoterminowej transformacji energetycznej jest *Polityka energetyczna Polski do 2040 roku*, wydana przez Ministerstwo Klimatu i Środowiska jako załącznik do uchwały nr 22/2021 Rady Ministrów z dnia 2 lutego 2021 r.

[116] Eksperci kanadyjskiej firmy analitycznej SecDev wskazują na fakt, że Europa przygotowywała się do przejścia w 2022 r. na import m.in. litu z Ukrainy, by zastąpić chińskie dostawy. Również przed początkiem rosyjskiej okupacji Krymu, w 2013 r., europejskie firmy szukały ukraińskich partnerów, aby zastąpić nimi chińskich producentów. Oceniają również, że Chiny pozostają źródłem 98% dostaw metali ziem rzadkich dla Europy. Por.: A. Lach, *Surowce na okupowanych przez Rosję terenach Ukrainy warte 12 bln dolarów (Raport)*, Bankier.pl, 11.08.2022., pobrano z lokalizacji: https://www.bankier.pl/wiadomosc/Surowce-na-okupowanych-przez-Rosje-terenach-Ukrainy-warte-12-bln-dolarow-Raport-8388889.html [dostęp: 21.11.2022]. Por. E. Cieślik, *Walka o metale ziem rzadkich*, Forsal.pl, 15.04.2022, pobrano z lokalizacji: https://forsal.pl/gospodarka/artykuly/8400146,walka-o-metale-ziem-rzadkich.html [dostęp: 21.11.2022].

[117] W maju 2022 r. ok. 30% wykorzystywanej ropy pochodziło z Rosji. Por. P. Bednarz, *Czy Polska może odciąć się dziś od ropy? Możliwości są, ale skutki nagłego odcięcia byłyby trudne do zniesienia*, Business Insider, 28.05.2022, pobrano z lokalizacji: https://businessinsider.com.pl/finanse/ odciecie-sie-od-dostaw-rosyjskiej-ropy-jakie-beda-skutki-dla-polski/kc0sdn0 [dostęp: 26.11.2022] oraz A. Bełdowicz, *Eksport rosyjskiej ropy spada, Polska wciąż w pierwszej 10. importerów*, Rzeczpospolita, 16.11.2022, pobrano z lokalizacji: https://klimat.rp.pl/energia/art37426311-eksport-rosyjskiej-ropy-spada-polska-wciaz-w-pierwszej-10-importerow [dostęp: 27.11.2022]. Warto zauważyć, że udział ropy rosyjskiej spadł w portfolio Orlenu z 83% w 2021 roku, do około 60% w 2022 roku, a do 10% w lutym 2023 roku. Por. W. Jakóbik, *Ile jeszcze ropy Polska sprowadza z Rosji? (ANALIZA)*, Biznes Alert, 07.02.2023, pobrano z lokalizacji: https://biznesalert.pl/polska-ile-sprowadza-ropa-rosja-import-sankcje-pkn-orlen/ [dostęp: 30.05.2023].

[118] Podobnie jak w przypadku ropy naftowej, tak również ilość importowanego gazu z Rosji stale się zmniejsza. Por. M. Zaniewicz, *Perspektywy uniezależnienia się UE od rosyjskiego gazu*, PISM, 28.04.2022, pobrano z lokalizacji: https://www.pism.pl/publikacje/perspektywy-uniezaleznienia-sie-ue-od-rosyjskiego-gazu [dostęp: 27.11. 2022] oraz A. Mróz, *Polska nadal importuje tani gaz LPG z Rosji*, Rzeczpospolita, 24.02.2023, pobrano z lokalizacji: https://moto.rp.pl/tu-i-teraz/art38017441-polska-nadal-importuje-tani-gaz-lpg-z-rosji [dostęp: 28.05.2023].

Zielonego Ładu[119]. Natomiast do najczęściej wskazywanych zagrożeń zaliczono postępującą zmianę klimatu, jak również stale utrzymujące się uzależnienie Europy od węglowodorów z Rosji.

W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron ze względu na ich znaczenie dla zapewnienia bezpieczeństwa energetycznego oraz ogólnych implikacji dla funkcjonowania państwa. Wyniki analizy przedstawiono na rys. 3.4. Należy stwierdzić, że do najważniejszych mocnych stron państwa w analizowanym obszarze zaliczono dywersyfikację dostaw surowców energetycznych (S3), rozwój alternatywnych źródeł energii (S5) oraz właściwą eksploatację własnych zapasów surowców energetycznych (S4). Do najbardziej znaczących niedostatków zaliczono uzależnienie od dostaw z Rosji (W3), zależność od eksportu metali ziem rzadkich (W1) oraz wprowadzanie niekorzystnych zmian prawnych implikujących niekorzystne zjawiska w polityce energetycznej (W4).

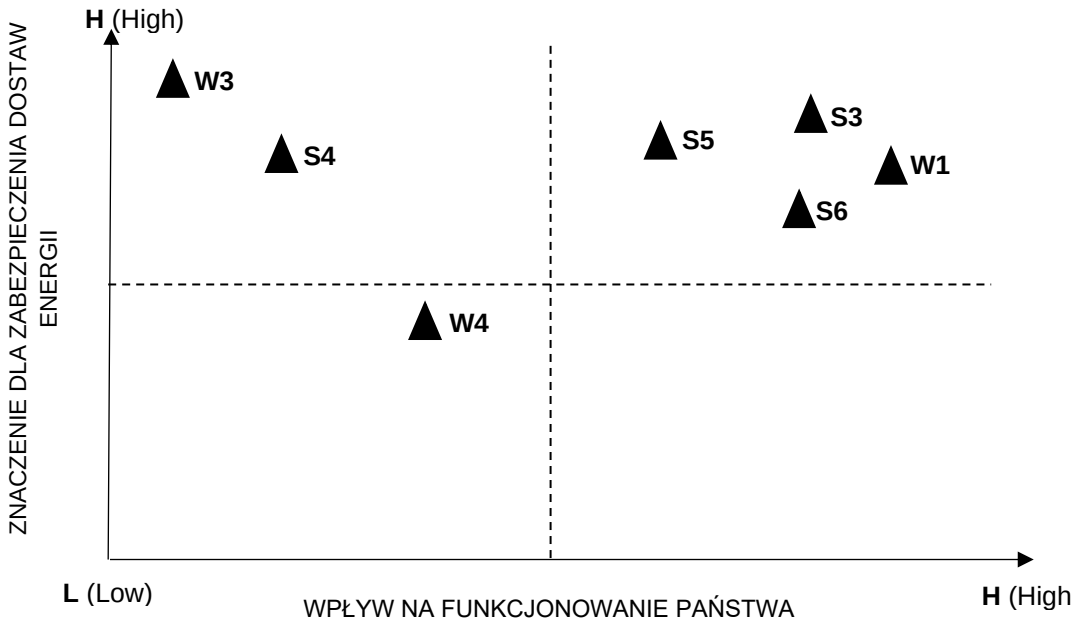
Tabela 3.4.

Analiza SWOT – Czynniki wpływające na zabezpieczenie dostaw energii

S	**W**
1. Polityka energetyczna UE 2. Regulacje prawne 3. Dywersyfikacja dostaw 4. Własne zapasy surowców energetycznych 5. Przyszłość energetyki (elektrownie jądrowe oraz OZE) 6. Baltic Pipe i inne projekty	1. Uzależnienie od eksportu metali ziem rzadkich 2. STRATCOM 3. Uzależnienie od dostaw z Rosji 4. Niekorzystne zmiany prawne np. fotowoltanika, farmy wiatrowe
O	**T**
1. Zielony ład (przeskok generacyjny, odejście od węglowodorów) 2. Dekarbonizacja 3. Dywersyfikacja źródeł surowców 4. Polityka klimatyczna *5.* Inicjatywa *One Road, One Belt*	1. Działalność Rosji – surowce jako rodzaj broni 2. Zmiana klimatu 3. Uzależnienie Europy od węglowodorów z Rosji 4. Metale ziem rzadkich – monopol Chin 5. Polityka klimatyczna

Źródło: opracowanie własne

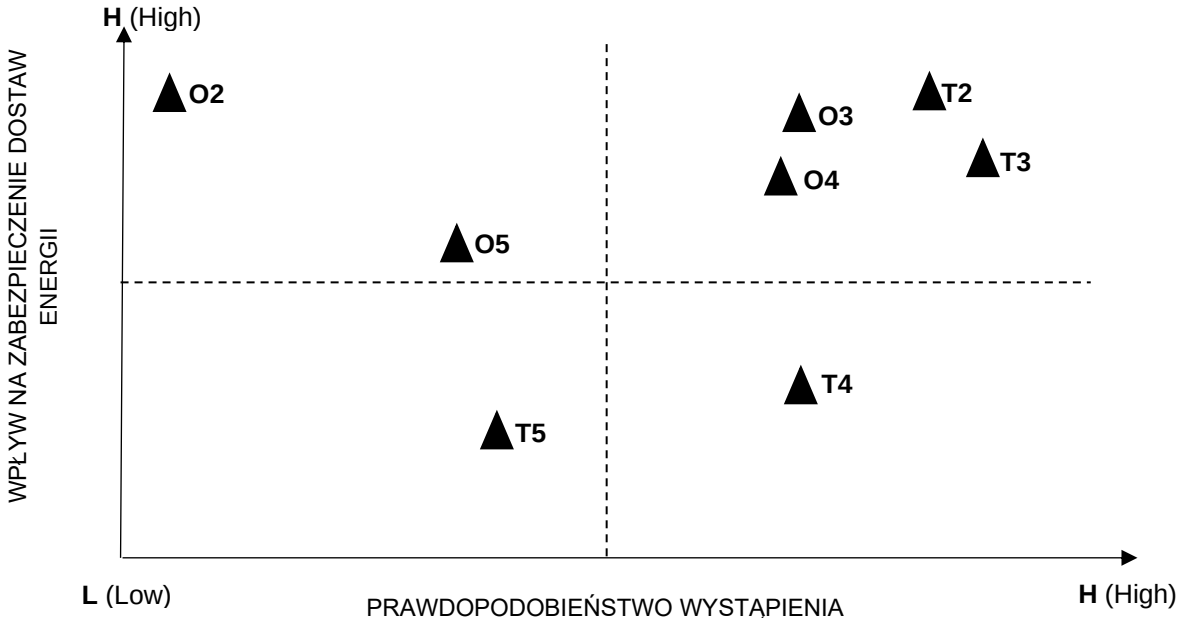
[119] Najważniejszą propozycją Europejskiego Zielonego Ładu jest uchwalenie wiążącego celu neutralności klimatycznej do 2050 roku. Ponadto cel redukcji emisji do 2030 roku obecnie wynosi 40% w porównaniu z poziomem w 1990 roku, ale planuje się jego zwiększenie do 50% lub 55%. Por. P. Wiejski, *Zielony ład dla Europy. Uwarunkowania, narzędzia, perspektywy*, Instytut Spraw Publicznych, Warszawa 2019, s. 2.



Rys. 3.4. Uszeregowanie czynników wpływających na zabezpieczenie dostaw energii pod względem stopnia ważności S/W

Źródło: opracowanie własne

W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na zapewnienie bezpieczeństwa energetycznego pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na rys. 3.5. Jako najbardziej znaczące szanse w omawianym obszarze wskazano dywersyfikację źródeł surowców (O3), *dekarbonizację* Polski (O2) oraz politykę klimatyczną (O4). Do najistotniejszych zagrożeń dla zapewnienia bezpieczeństwa energetycznego zaliczono z kolei postępującą zmianę klimatu (T2), uzależnienie Europy od węglowodorów z Rosji (T3), a także potencjalne zmonopolizowanie rynku metali ziem rzadkich przez Chiny (T4).



Rys. 3.5. Uszeregowanie czynników zewnętrznych wpływających na zabezpieczenie dostaw energii pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

Kolejnym etapem analizy było uszeregowanie poszczególnych czynników zgodnie z ustalonymi miarami ich ważności. Rezultaty przedstawiono w tabeli 3.5.

Tabela 3.5.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S3 W3 O3 T2
	S5 W1 O2 T3
	S4 W4 O4 T4
Niski	

Źródło: opracowanie własne

W dalszej kolejności opracowano i przedstawiono w tabeli 3.6. matrycę konfrontacji, wykorzystując czynniki zidentyfikowane w poprzednich etapach pod względem ich ważności. Dzięki temu możliwe jest zwizualizowanie czynników, które muszą być wzięte pod uwagę w celu określenia odporności państwa w obszarze zabezpieczenia dostaw energii.

Tabela 3.6.
Analiza SWOT – ocena czynników wpływających na zabezpieczenie dostaw energii

	S3	S5	S4	W3	W1	W4
O3	++	+++	+			--
O2	++	+++		--		--
O4	+	++	+	--		--
T2	++	++		---	--	-
T3		++				--
T4	+++	++		--		-

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy stwierdzono, że odporność państwa w obszarze zabezpieczenia dostaw energii jest na stosunkowo **niskim poziomie**. Zauważalna jest jednak tendencja wzrostowa. Wpływ na wzmacnianie odporności w tym zakresie ma paradoksalnie rozpoczęcie przez Rosję wojny w Ukrainie i przyspieszenie procesów uniezależniania się większość państw europejskich od rosyjskich węglowodorów. Oczywiście należy jasno podkreślić fakt, że Polska już od dłuższego czasu prowadziła politykę stopniowego uniezależniania się od dostaw z Rosji. Przejawem tej działalności była i jest między innymi budowa terminali gazowych, Baltic Pipe czy budowanie zbiorników gazu[120]. Kolejnym czynnikiem mogącym pozytywnie wpłynąć na wzmocnienie odporności może być polityka dekarbonizacji powiązana z szerokim wprowadzaniem alternatywnych źródeł energii. Zwraca się przy tym uwagę na pojawiające się zagrożenia związane przede wszystkim ze zmianą klimatu i potencjalnym przejęciem przez Chiny roli monopolisty na rynku dostaw metali ziem rzadkich[121]. Zagrożenia te mogą jednak zostać zminimalizowane poprzez konsekwentne dążenie do wykorzystania posiadanych mocnych stron. Zauważalne są także pewne niekorzystne trendy mogące

[120] Polska w siedmiu obiektach ulokowanych na terenie całego kraju może zgromadzić dokładnie 3 175 mld m^3 paliwa, a zapasy te zapasy stanowią zaledwie 16% rocznego zużycia. Por. P. Ciszak, *Trwa wyścig o gaz. Gigant straszy Europę. „Zagrożenia nie można zlekceważyć"*, money.pl, 23.04.2023, pobrano z lokalizacji: https://www.money.pl/gielda/trwa-wyscig-o-gaz-gigant-straszy-europe-zagrozenia-nie-mozna-zlekcewazyc-6889460731505216a.html [dostęp: 27.05.2023].

[121] Według szacunków Sondażu Geologicznego USA (USGS) w 2021 r. wydobyto na całym świecie 280 tys. ton metali ziem rzadkich, z tego aż 168 tys. w Chinach. Por. H. Kozieł, *Metale ziem rzadkich. Wąskie gardło cywilizacji cyfrowej*, Rzeczypospolita, 18.02.2022, pobrano z lokalizacji: https://www.rp.pl/plus-minus/art35711091-metale-ziem-rzadkich-waskie-gardlo-cywilizacji-cyfrowej [dostęp: 27.11.2022]. Z drugiej strony prowadzone są prace związane z poszukiwaniem nowych źródeł pozyskiwania tych metali jak również określenie metali ziem rzadkich na listę surowców priorytetowych przez Komisję Europejską. Por. A. Sierak, *Polska może mieć zaskakujące źródła metali ziem rzadkich*, wnp.pl, 21.04.2023, pobrano z lokalizacji: https://www.wnp.pl/gornictwo/polska-moze-miec-zaskakujace-zrodla-metali-ziem-rzadkich,701550.html [dostęp: 22.05.2023].

zahamować proces wzmacniania odporności w tym obszarze. Należą do nich przede wszystkim próby zmian w polityce promującej OZE, co w konsekwencji może prowadzić do zmniejszenia zainteresowania jej rozwojem, a także odejście od procesu dywersyfikacji źródeł dostaw. Szczególną uwagę należy zwrócić na możliwość ponownego uzależniania się od tanich rosyjskich surowców w przypadku zakończenia wojny w Ukrainie i powrotu na drogę dialogu z Rosją i realizacji współpracy zgodnie z zasadą *business as usual*.

3.4.3. Zarządzanie przemieszczaniem się ludności

W ostatnich latach wyzwania związane z migracjami stały się zjawiskami powszechnymi. Masowy ruch ludności może doprowadzić do wyczerpania posiadanych zasobów i zdezorganizować świadczenie podstawowych usług. Może również zdestabilizować proces zarządzania na szczeblu centralnym i lokalnym. W przypadku realizacji zadań związanych z reagowaniem na działania przeciwnika istnieje prawdopodobieństwo zmniejszenia ilości zasobów planowanych do udostępnienia przybywającym siłom Sojuszu. Ponadto rozmieszczanie wojsk może zostać zakłócone, zablokowane lub zatrzymane przez jednoczesne przemieszczanie się dużych grup ludzi korzystających z tej samej infrastruktury i szlaków transportowych.

Za początek obecnego kryzysu uznaje się rok 2015, kiedy to po raz pierwszy w UE zarejestrowano 1,25 miliona osób ubiegających się o azyl[122]. Istnieje wiele form przepływów ludności na świecie wywoływanych różnymi przyczynami, do których można zaliczyć: globalizację i procesy integracyjne, tendencje geopolityczne, ponadnarodowość oraz tendencje demograficzne[123].

W trakcie analizy stopnia odporności Polski zaproponowano kilka czynników wpływających na zdolność do reagowania na masowe niekontrolowane migracje, a najistotniejsze z nich umieszczono w tabeli 3.7.

[122] *Odpowiedź UE na wyzwanie migracji,* Parlament Europejski, 17.07.2017, pobrano z lokalizacji: https://www.europarl.europa.eu/news/pl/headlines/society/20170629STO78629/odpowiedz-ue-na-wyzwanie-migracji [dostęp: 27.11.2022].

[123] E. Kacperska, M. Kacprzak, D. Kmieć, A. Król, K. Łukasiewicz, *Migracje międzynarodowe w Europie. Trendy, problemy, wyzwania*, Wydawnictwo SGGW, Warszawa 2019, s. 16.

Tabela 3.7.

Czynniki wpływające na zdolność zarządzania przemieszczaniem się ludności

S 1. Członkostwo w UE i NATO 2. Wolność gospodarcza i polityczna 3. Rozwój gospodarczy 4. Wzrost produktywności	**W** 1. Uprzedzenia do migrantów 2. Niesprawdzony program integracji 3. Niedoświadczona i niewydolna administracja samorządowa 4. STRATCOM 5. Uzależnienie gospodarki od migrantów 6. System kontroli migrantów
O 1. Niwelacja niekorzystnych trendów demograficznych 2. Źródła siły roboczej spośród migrantów 3. Wzmocnienie potencjału intelektualnego 4. Łatwa integracja migrantów z Europy Wschodniej 5. Wzmocnienie gospodarki 6. Integracja społeczna 7. Wspólna polityka UE	**T** 1. Konflikty zbrojne 2. Polityka państw trzecich 3. Zmiana klimatu 4. Wzrost polaryzacji w Europie 5. Obciążenie systemu socjalnego państwa 6. Zagrożenia wywiadowcze i terrorystyczne 7. Nieszczelna granica zewnętrzna UE 8. Społeczeństwa równoległe

Źródło: opracowanie własne

Zdaniem ekspertów do mocnych stron w tym obszarze można przyporządkować między innymi członkostwo w Unii Europejskiej i NATO, przez co Polska jest traktowana jako kraj bezpieczny do życia, o stosunkowo wysokim wzroście gospodarczym, przyczyniającym się do powstawania nowych miejsc pracy[124]. Z kolei do słabych stron zaliczono przede wszystkim silne uprzedzenia do migrantów oraz uzależnienie gospodarki od migrantów w niektórych obszarach[125]. Ciekawym przykładem jest wskazany jako słabość

[124] Z danych upublicznionych Główny Urząd Statystyczny PKB Polski w I kwartale 2023 r. PKB wyrównany sezonowo (w cenach stałych przy roku odniesienia 2015) zwiększył się realnie o 3,8% w porównaniu z poprzednim kwartałem i pozostał na zbliżonym poziomie do notowanego w analogicznym okresie roku poprzedniego. Z kolei PKB niewyrównany sezonowo (w cenach stałych średniorocznych roku poprzedniego) zmniejszył się realnie o 0,3% w porównaniu z 1 kwartałem roku poprzedniego. Por. Główny Urząd Statystyczny, *Wstępny szacunek produktu krajowego brutto 31.05.2023 r. w 1 kwartale 2023 r.*, 31.05.2023, pobrano z lokalizacji: https://stat.gov.pl/obszary-tematyczne/rachunki-narodowe/kwartalne-rachunki-narodowe/wstepny-szacunek-produktu-krajowego-brutto-w-1-kwartale-2023-roku,3,83.html [dostęp: 31.05. 2023].

[125] Według prof. Jacka Męciny z Uniwersytetu Warszawskiego i eksperta Konfederacji Lewiatan sektory takie jak rolnictwo, hotelarstwo, budownictwo, przetwórstwo spożywczo-przemysłowe, opieka społeczna nie mogą już sprawnie funkcjonować bez imigrantów. Źródło: Z. Gajewski (opr.), *Migranci ekonomiczni w Polsce. Fakty i mity*, [w:] „Magazyn THINKTANK", nr 36, Warszawa 2020.

niesprawdzony program integracji. Obecny stan wiedzy pozwala na stwierdzenie, że system został sprawdzony w trakcie organizowania pomocy dla uchodźców z Ukrainy. Z drugiej strony należy zwrócić uwagę, że system pomocy był początkowo, w dużym stopniu, organizowany oddolnie, przez osoby prywatne oraz samorządy. W miarę rozwoju sytuacji nastąpiło przejęcie odpowiedzialności przez państwo. Może to świadczyć z jednej strony o nieprzygotowaniu systemu integracji, a z drugiej strony o zdolności do adaptacji przez odpowiedzialne ministerstwa i służby[126].

W przedmiotowym obszarze zgodzono się, że istnieje wiele możliwości, które przy odpowiednim ich wykorzystaniu mogą korzystnie wpłynąć na rozwój gospodarczy kraju. Jako najbardziej istotne wskazano przede wszystkim na możliwości odwrócenia niekorzystnych trendów demograficznych oraz wzmocnienie potencjału intelektualnego[127].

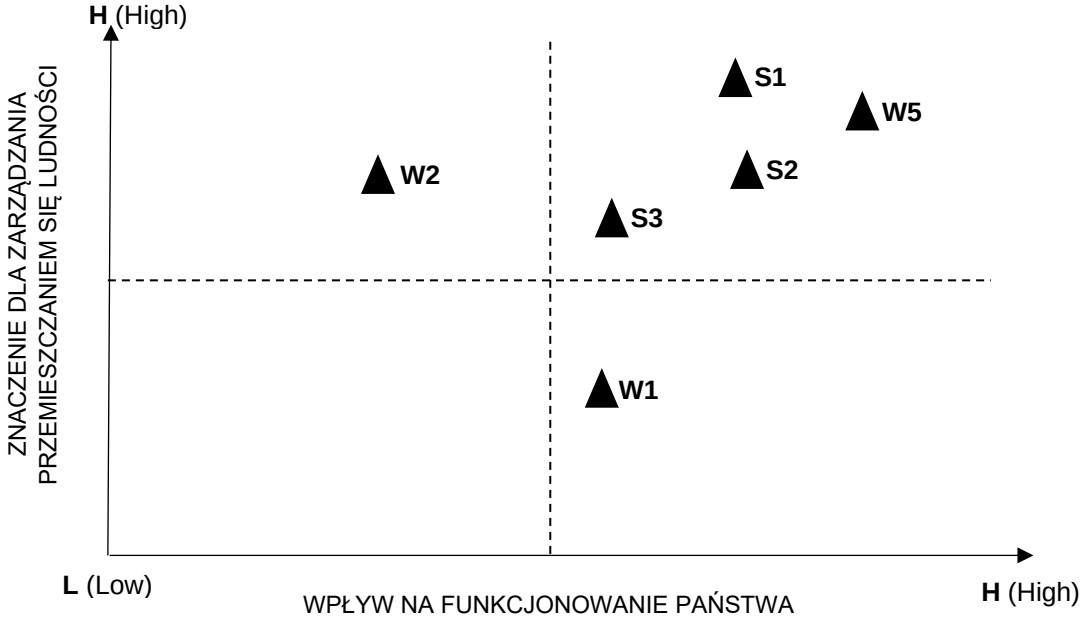
Do najczęściej wskazywanych zagrożeń zaliczono postępującą konflikty zbrojne, konfrontacyjną politykę państw trzecich (kryzys graniczny wywołany przez Białoruś w 2021 r.), obciążenie systemu socjalnego państwa, a także zagrożenia terrorystyczne i wywiadowcze[128] czy też zmianę klimatu[129].

[126] Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, Dz.U. z 2022 r., poz. 583.

[127] Populacja Polski w 2023 r. zmaleje o 90 000 i osiągnie 37 391 000 ludzi w 2024 roku. Migracja ludności zmniejszyła populację o 10 000 ludzi rocznie przy uwzględnieniu emigracji i imigracji. Od 1980 r. gęstość zaludnienia Polski uległa zmianie z 116,1 na 123,6 w 2021 r., pobrano z lokalizacji: https://www.populationof.net/pl/poland/ [dostęp: 30.05.2023].

[128] Zatrudnianie cudzoziemców w obiektach infrastruktury krytycznej oraz podmiotach realizujących usługi na ich rzecz może generować zarówno zagrożenia wywiadowcze, jak i terrorystyczne. Zagrożenia terrorystyczne i kontrwywiadowcze mogą być także powodowane realizacją, przez firmy zewnętrzne zatrudniające cudzoziemców, w tym migrantów z państw podwyższonego ryzyka, zadań zleconych na rzecz obiektów strategicznych, np. baz wojskowych i strategicznych spółek skarbu państwa. Źródło: Departament Analiz i Polityki Migracyjnej MSWiA, *Polityka migracyjna Polski – diagnoza stanu wyjściowego*, Warszawa, 15.12.2020, s. 16, pobrano z lokalizacji: https://www.gov.pl/attachment/2a65e5d4-52c5-40ac-ada9-3b3f988f86b9 [dostęp: 27.11.2022].

[129] Autorzy publikacji *Global Trends 2040* oceniają, że zmieniające się globalne trendy demograficzne na pewno pogłębią różnice w możliwościach ekonomicznych i politycznych poszczególnych krajów oraz między nimi. Ponadto nadwerężą system rządów i zwiększą presję globalnej migracji w ciągu najbliższych 20 lat. Przewiduje się także, że jednym z elementów wpływających na taką sytuację będzie zmiana klimatu. Skutki tych zmian, a w konsekwencji degradacja środowiska, prawdopodobnie przyczynią się do braku bezpieczeństwa żywnościowego i wodnego w krajach ubogich oraz zwiększenia migracji itd. Por. *Global Trends 2040*. *A more contested World*, The National Intelligence Council, March 2021.



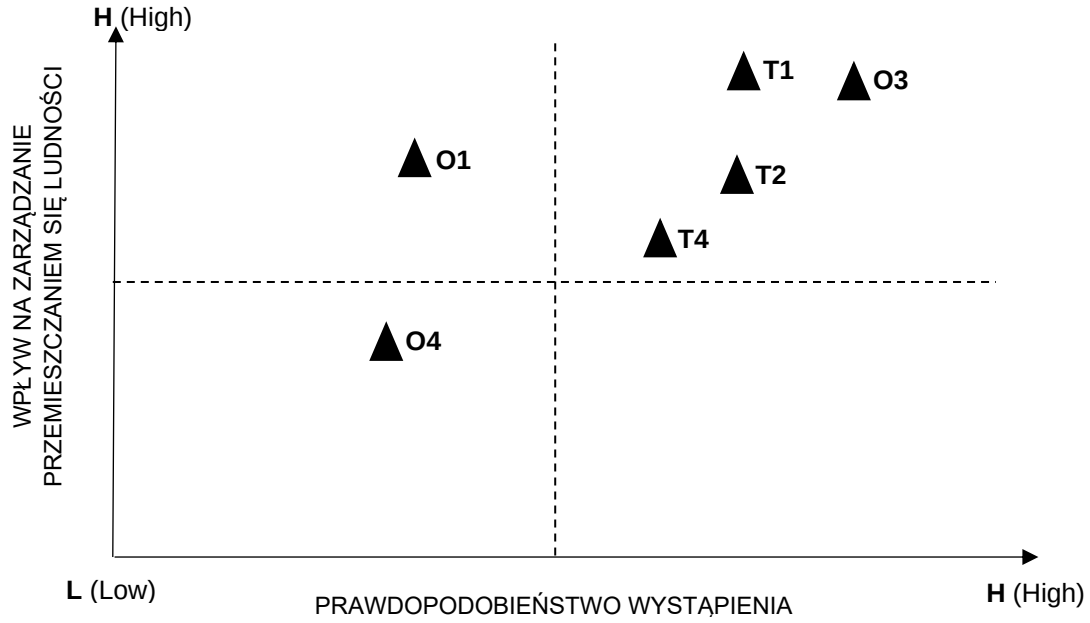
Rys. 3.6. Uszeregowanie czynników wpływających na zarządzanie się przemieszczaniem ludności pod względem stopnia ważności S/W

Źródło: opracowanie własne

Następnie określono mocne (S) i słabe (W) strony państwa w obszarze reagowania na masowe niekontrolowane migracje pod względem ich znaczenia dla zarządzania przemieszczaniem ludności i ich ogólnych implikacji dla funkcjonowania państwa. Wyniki analizy przedstawiono na rysunku 3.6. Wynika z niego, że do najważniejszych mocnych stron państwa w analizowanym obszarze zaliczono: członkostwo Polski w UE i NATO (S1), wolność gospodarczą i polityczną (S2) oraz rozwój gospodarczy (S4). Jako najistotniejsze słabe strony uznano: uzależnienie gospodarki od migrantów (W5), niesprawdzony program integracji (W2) oraz głęboko zakorzenione u części społeczeństwa uprzedzenia do migrantów (W4).

W kolejnej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na zarządzanie przemieszczaniem ludności pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na rysunku 3.7. Jako najbardziej znaczące szanse w omawianym obszarze wskazano: wzmocnienie potencjału intelektualnego (O3), zminimalizowanie niekorzystnych trendów demograficznych (O1) oraz możliwość łatwej integracji migrantów z Europy Wschodniej (O4). Do najistotniejszych zagrożeń dla zarządzania przemieszczaniem ludności zaliczono z kolei:

konflikty zbrojne (T1), politykę państw trzecich (T2) a także wzrost polaryzacji w Europie (T4).



Rys. 3.7. Uszeregowanie czynników zewnętrznych wpływających na zarządzanie przemieszczanie się ludności pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

Kolejnym etapem analizy było uszeregowanie poszczególnych czynników zgodnie z ustalonymi w powyższych wykresach miarami ich ważności. Rezultaty przedstawiono w tabeli 3.8.

Tabela 3.8.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S1 W5 O3 T1
	S2 W2 O1 T2
	S3 W1 O4 T4
Niski	

Źródło: opracowanie własne

Tabela 3.9. przedstawia matrycę konfrontacji, w której zwizualizowano zidentyfikowane w poprzednich etapach czynniki ze względu na ich stopień ważności, co w konsekwencji pozwoliło na określenie odporności państwa w obszarze zarządzania przemieszczaniem ludności.

Tabela 3.9.

Ocena czynników wpływających na zarządzanie przemieszczaniem się ludności

	S1	S2	S3	W5	W2	W1
O3	++	++	++		-	--
O1	++	+			--	--
O4	+		+			-
T1	+++	+		--		-
T2	++	+	+	--	--	--
T4	+				--	--

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy, po wzięciu pod uwagę najistotniejszych, wybranych przez ankietowanych czynników, określono stopień odporności państwa w tym obszarze jako **niski z tendencją wzrostową**[130]. Należy dążyć do wykorzystania naszego członkostwa w zarówno w UE, jak i NATO, a także rozwoju gospodarczego do wzmocnienia potencjału intelektualnego i zminimalizowania niekorzystnych skutków niżu demograficznego poprzez możliwość przyciągnięcia migrantów. Co więcej, członkostwo w tych organizacjach umożliwia współpracę związaną z zarządzaniem przemieszczaniem migrantów i ich późniejszą relokacją. Ponadto właściwa współpraca w ramach UE i NATO pozwala na minimalizowanie skutków konfliktów zbrojnych lub działalności państw trzecich (Białoruś w 2021 r.) w obszarze reagowania na migracje. W trakcie analizy stwierdzono uzależnienie polskiej gospodarki od obecności uchodźców, szczególnie w warunkach konfliktu zbrojnego lub celowej działalności państw trzecich. Ta zdefiniowana słabość państwa może w konsekwencji wpłynąć na masowy odpływ pracujących w kraju migrantów, czego skutkiem może być brak siły roboczej, a w konsekwencji spadek gospodarczy. Kolejną istotną wadą zidentyfikowaną podczas analizy jest uprzedzenie części

[130] Należy zwrócić uwagę na fakt, że badania przeprowadzono w październiku i listopadzie 2020 r. Po rozpoczęciu wojny w Ukrainie i pojawieniu się milionów uchodźców na wschodniej granicy sytuacja uległa zmianie. Dotychczasowe zaniedbania, szczególnie w regulacjach prawnych, zostały w szybki sposób poprawione. W przyszłości warto zwrócić uwagę na wcześniejsze przeprowadzenie niezbędnych analiz i przygotowanie odpowiednich scenariuszy działania przy budowaniu (wzmacnianiu) odporności Polski. Przyp. aut.

społeczeństwa do migrantów[131], które może prowadzić do spotęgowania polaryzacji społecznej.

3.4.4. Wydolność służby zdrowia

Zdolność do radzenia sobie ze zdarzeniami z dużą liczbą ofiar i innymi problemami związanymi z kwestią zdrowotną miała kluczowe znaczenie podczas pandemii wirusa Covid-19, jak również w trakcie trwającej agresji rosyjskiej w Ukrainie. Takie zdarzenia, jeśli nie są odpowiednio koordynowane, mogą podważyć zaufanie publiczne, przeciążyć krajowe zdolności reagowania kryzysowego oraz osłabić jakość i ciągłość świadczeń, a w tym cywilnego wsparcia dla wojska. Dlatego też istotne jest zapewnienie, że systemy opieki zdrowotnej będą w stanie poradzić sobie nawet w bardzo wymagających sytuacjach, gdy może wystąpić jednoczesna presja na cywilne i wojskowe możliwości opieki zdrowotnej[132]. Znaczące, utrzymujące się wyzwania w zakresie wojskowych zdolności wsparcia medycznego podkreślają potrzebę bardziej samowystarczalnego, odpornego cywilnego systemu medycznego, zwłaszcza w przypadku, gdy wydarzenia w znacznym stopniu przetestują zarówno cywilne, jak i wojskowe zdolności medyczne.

W NATO przyjmuje się, że aby system był odporny, średni wskaźnik łóżek szpitalnych powinien wynosić 4,8 na 1 000 obywateli, pielęgniarek 8,2, a lekarzy 3,8[133].

---

[131] W lutym 2016 r. zaledwie 39% badanych zgadzało się na pomoc migrantom. Spośród nich tylko 4% opowiadało się za przyjmowaniem uchodźców i zezwalaniem na ich osiedlanie się w Polsce, a 35% aprobowało pomoc tymczasową – do czasu, kiedy uchodźcy będą mogli wrócić do swoich krajów pochodzenia. Aż 57% ankietowanych uważało, że uchodźców nie powinniśmy przyjmować wcale. W miarę pogłębiania się tzw. kryzysu migracyjnego wskaźnik spadał do coraz niższego poziomu, a postawy polskich ankietowanych stawały się coraz bardziej wrogie. Poparcie dla przyjęcia uchodźców spadło do 26%, a sprzeciw wzrósł do 67%. Por. K. Głowiak, *Stosunek Polaków do przyjmowania uchodźców przed i w warunkach europejskiego kryzysu migracyjnego*, „Historia i Polityka", nr 35(42)/2021, s. 155.

Dla porównania, zdecydowana większość badanych (84%) popiera przyjmowanie ukraińskich uchodźców przez Polskę i wynik ten stanowi łagodne przełamanie tendencji spadkowej, jaka była obserwowana od kwietnia. Bezpośrednio po rozpoczęciu rosyjskiej inwazji na Ukrainę odsetek ten sięgnął 94%, później spadał co miesiąc o kilka punktów procentowych, by wzrosnąć o dwa punkty (z 82% w czerwcu do 84% w lipcu). Tylko co dziewiąty badany (11%) wyraża sprzeciw wobec przyjmowania ukraińskich uchodźców. Por. *Komunikat z badań: Polacy wobec wojny na Ukrainie i ukraińskich uchodźców*, CBOS, nr 101/22, sierpień 2022, ISSN 2353-5822, s. 5 oraz I. Kacprzak, *Sondaż: Polacy chcą, by uchodźcy wojenni partycypowali w kosztach życia*, Rzeczpospolita, 25.11.2022, pobrano z lokalizacji: https://www.rp.pl/spoleczenstwo/art37484871-sondaz-polacy-chca-by-uchodzcy-wojenni-partycypowali-w-kosztach-zycia [dostęp: 29.11.2022].

[132] L. Meyer-Minnemann, *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience*, [w:] D. Hamilton (red), *Forward Resilience Protecting Society in an Interconnected World*, Johns Hopkins University, Waszyngton 2016, s. 93.

[133] Materiały własne autora pozyskane w ramach działalności służbowej w ACT.

Z przeanalizowanych danych wynika, że w Polsce stan ten kształtuje się odpowiednio: liczba łóżek – 4,38, pielęgniarek – 5,1 a lekarzy – 2,38[134].

Zdarzenie masowe jest zdarzeniem z dużą liczbą poszkodowanych, w wyniku którego określone w procesie segregacji poszkodowanych zapotrzebowanie na kwalifikowaną pierwszą pomoc i medyczne czynności ratunkowe, realizowane w trybie natychmiastowym przekracza możliwości sił i środków podmiotów ratowniczych obecnych na miejscu zdarzenia w danej fazie działań ratowniczych[135]. Należy zwrócić uwagę, że do takich zdarzeń dochodzi przede wszystkim w pokojowym okresie funkcjonowania państwa i w pierwszej kolejności reagować na nie będą podmioty cywilnej służby zdrowia, wzmacniane w razie konieczności przez pozostałe resorty.

W trakcie analizy odporności Polski w przedmiotowym obszarze zaproponowano szereg czynników, a najistotniejsze z nich umieszczono w tabeli 3.10. Do najważniejszych mocnych stron zaliczono m.in.: opracowane akty prawne w obszarze reagowania na zdarzenia z dużą liczbą ofiar, rozbudowaną infrastrukturę medyczną[136] oraz możliwość wsparcia cywilnej służby zdrowia przez wojskową[137].

[134] Por. *Zdrowie i ochrona zdrowia w 2020 r*., Główny Urząd Statystyczny, Warszawa, Kraków 2021 oraz dane OECD (Organizacji Współpracy Gospodarczej i Rozwoju) opublikowane 23 sierpnia 2021, pobrano z lokalizacji: https://www.oecd.org/coronavirus/en/data-insights/number-of-medical-doctors-and-nurses?utm_term=PAC&utm_medium=social &utm_source=twitter&utm_content= [dostęp: 20.09.2021].

[135] *Procedura postępowania na wypadek wystąpienia zdarzenia z dużą liczbą poszkodowanych*, Ministerstwo Zdrowia, Warszawa, 04.09.2020 r.

[136] W Polsce na koniec 2020 r. funkcjonowało 898 stacjonarnych szpitali ogólnych oraz 208 szpitali dziennych (tzw. szpitali jednego dnia). Dysponowały one łącznie 167,8 tys. łóżek (stan w dniu 31 grudnia). Wskaźnik liczby łóżek w szpitalach stacjonarnych na 10 tys. ludności kraju wyniósł 43,8 łóżka (stan w dniu 31 grudnia), co oznacza że na jedno łóżko przypadało przeciętnie 228 mieszkańców. Por. *Zdrowie i ochrona zdrowia w 2020 r*., wyd.cyt., str.62.

[137] Ministerstwu Obrony Narodowej podlega 110 podmiotów medycznych, w tym 22 szpitale, 29 specjalistycznych przychodni, pracownie psychologiczne, ośrodki medycyny prewencyjnej oraz stacje krwiodawstwa i krwiolecznictwa. Wojskowa służba zdrowia zatrudnia w sumie ponad 17 tys. pracowników, w tym ponad 4 tys. lekarzy (w tym 331 lekarzy wojskowych), ponad 4,5 tys. pielęgniarek i położnych, 250 ratowników medycznych i blisko 200 psychologów. W podmiotach leczniczych resortu obrony narodowej przygotowane jest ponad 5,5 tys. łóżek. Por. K. Lisowska, *MON o wojskowej służbie zdrowia: tworzymy plan także na wypadek wojny*, Puls Medycyny, 27.10.2022, pobrano z lokalizacji: https://pulsmedycyny.pl/ mon-o-wojskowej-sluzbie-zdrowia-tworzymy-plan-takze-na-wypadek-wojny-1167938 [dostęp: 24.11.2022].

Jako słabe strony w tym obszarze wskazano niewystarczającą liczbę pracowników służby zdrowia[138], a także ich zaawansowany wiek[139] oraz permanentne niedofinansowanie tego resortu[140].

Tabela 3.10.

Czynniki wpływające na wydolność służby zdrowia

S 1. Akty prawne, procedury 2. Infrastruktura medyczna 3. System ratownictwa 4. Wsparcie cywilnej służby zdrowia przez służby mundurowe	**W** 1. Liczba pracowników służby zdrowia i ich wiek 2. Odpływ kadry medycznej za granicę 3. Niedofinansowanie służby zdrowia
O 1. Imigracja personelu medycznego 2. Służba zdrowia w państwach ościennych 3. Regulacje UE 4. Nowe technologie 5. Telemedycyna	**T** 1. Epidemie, pandemie 2. Konglomerat nowych zagrożeń (wirusy, bakterie jeszcze niezidentyfikowane) 3. Terroryzm (w tym bioterroryzm) 4. BMR 5. Luki w zabezpieczeniu elektrowni jądrowych

Źródło: opracowanie własne

[138] Zgodnie z rejestrami prowadzonymi przez izby lekarskie, izby pielęgniarek i położnych, izby aptekarskie oraz izby diagnostów laboratoryjnych w roku 2020 prawo wykonywania zawodu posiadało 153,5 tys. lekarzy, 43,3 tys. lekarzy dentystów, 303,2 tys. pielęgniarek, 39,8 tys. położnych, 36,5 tys. farmaceutów i 17,1 tys. diagnostów laboratoryjnych. Por. *Zdrowie i ochrona zdrowia w 2020 r*., dz. cyt, s. 49.

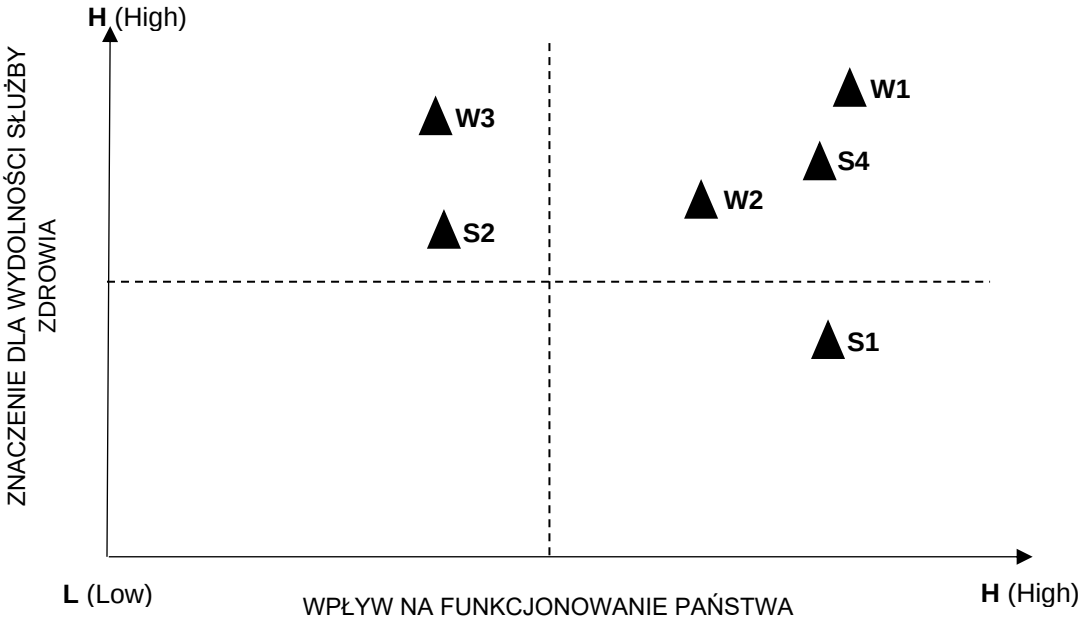
Według opublikowanych 23 sierpnia 2021 r. danych OECD Polska zajmuje 29. (przed Meksykiem, Turcją i Kolumbią) na 32 miejsca pod względem liczby lekarzy i pielęgniarek na tysiąc mieszkańców. Por. https://www.oecd.org/coronavirus/en/data-insights/number-of-medical-doctors-and-nurses?utm_term=PAC&utm_medium=social&utm_source=twitter&utm_content= [dostęp: 29.09.2021]; oraz M. Fidziński, *Ilu mamy lekarzy w Polsce (oprócz tego, że za mało)? Odpowiedź nie jest prosta*, Gazeta,pl, 27.08.2021, pobrano z lokalizacji: https://next.gazeta.pl/next/7,151003,27500831,ilu-mamy-lekarzy-w-polsce-oprocz-tego-ze-za-malo-odpowiedz.html [dostęp: 23.11.2022].

[139] W roku 2021 średnia wieku dla pielęgniarek to 53 lata i 51 lat dla położnych a 18% lekarzy przekroczyło 65 rok życia. Por. J. Friediger, *HCC 2021: brakuje lekarzy specjalistów? A może mamy za dużo specjalizacji?*, rynekzdrowia.pl, 12.06.2021, pobrano z lokalizacji: https://www.rynekzdrowia.pl/Nauka/HCC-2021-brakuje-lekarzy-specjalistow-A-moze-mamy-za-duzo-specjalizacji,222357,9.html [dostęp: 29.09.2021] oraz J. Przybytek-Pawlik, *Średnia wieku pielęgniarek to 53 lata. Szefowa NIPiP alarmuje: „Pielęgniarka idzie na emeryturę i umiera”*, rynekzdrowia.pl, 25.10.2021, pobrano z lokalizacji: https://www.rynekzdrowia.pl/Polityka-zdrowotna/Srednia-wieku-pielegniarek-to-53-lata-Szefowa-NIPiP-alarmuje-quot-Pielegniarka-idzie-na-emeryture-i-umiera-quot-Polityka-zdrowot,2260 26,14.html [dostęp: 17.08.2022].

[140] W finansowaniu systemu ochrony zdrowia NIK wskazuje na niskie, w porównaniu z innymi krajami UE, nakłady publiczne na ochronę zdrowia, przy jednoczesnym wysokim współudziale nakładów ponoszonych ze środków prywatnych. Por. *Raport: System ochrony zdrowia w Polsce – stan obecny i pożądane kierunki zmian*, Najwyższa Izba Kontroli, 14 maja 2019 r. oraz *Służba zdrowia potrzebuje zastrzyku finansowego. Dorzucimy się wszyscy*, Money.pl, 22.04.2021, pobrano z lokalizacji: https://www.money.pl/ gospodarka/sluzba-zdrowia-potrzebuje-zastrzyku-finansowego-dorzucimy-sie-wszyscy-6631700437547968a.html [dostęp: 02.10.2022].

Do najczęściej wskazywanych szans należą przede wszystkim: poszukujący miejsc zatrudnienia przedstawiciele zawodów medycznych emigrujący z innych krajów, regulacje Unii Europejskiej oraz rozwój nowych technologii i telemedycyny[141]. Z kolei za zagrożenia uznano m.in.: epidemie, terroryzm oraz użycie broni masowego rażenia (BMR).

W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron pod względem ich znaczenia dla wydolności służby zdrowia i ich ogólnych implikacji dla funkcjonowania państwa. Wyniki analizy przedstawiono na rysunku 3.8. Stwierdzono, że do najistotniejszych mocnych stron państwa polskiego w analizowanym obszarze należą: określona ramami prawnymi możliwość wsparcia cywilnej służby zdrowia przez służby mundurowe (S4), rozbudowana infrastruktura medyczna (S2) oraz spójne akty prawne i wprowadzone procedury normujące zasady reagowania (S1). Z kolei jako najbardziej znaczące słabości wskazano: niewystarczającą liczbę pracowników służby zdrowia i ich stosunkowo zaawansowany wiek (W1), niedofinansowanie służby zdrowia (W3) oraz odpływ kadry medycznej za granicę (W2).

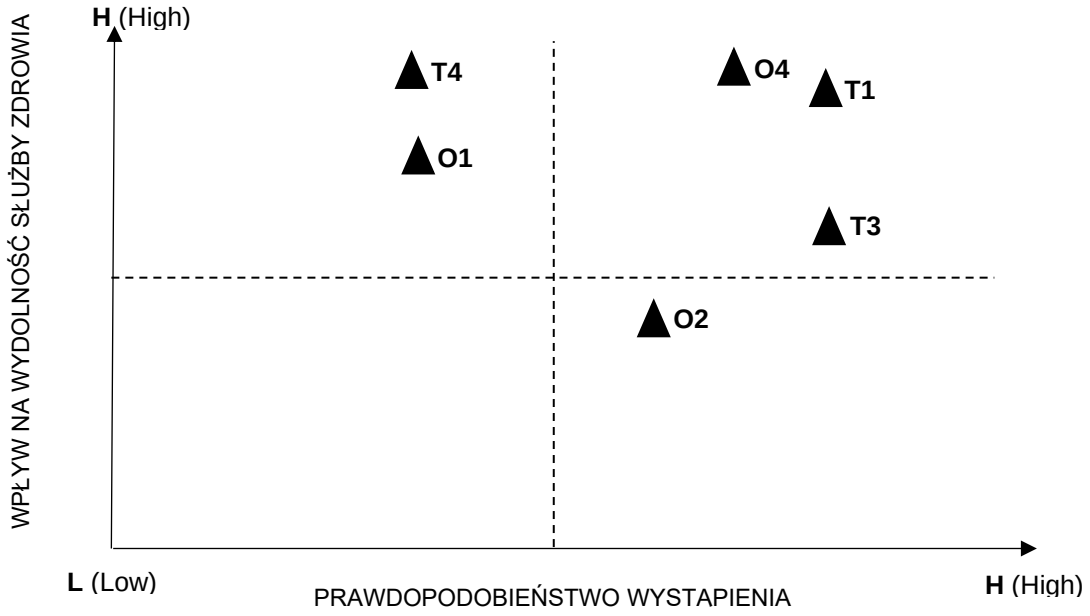


Rys. 3.8. Uszeregowanie czynników wpływających na wydolność służby zdrowia pod względem stopnia ważności S/W

Źródło: opracowanie własne

[141] O telemedycynie jako szansie na poprawę jakości systemu służby zdrowia wspomina także raport NIK, w którym pada zalecenie rozwijania i upowszechniania stosowania tego rodzaju świadczenia. Por. *Raport: System ochrony zdrowia,* dz. cyt., s. 21, 103.

W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) oraz zagrożeń (T) mających wpływ na wydolność służby zdrowia pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na rys. 3.9. Jako najbardziej znaczące szanse w omawianym obszarze wskazano: wykorzystanie nowych technologii (O4), imigrację personelu medycznego (O1) oraz możliwość korzystania ze wsparcia organów służby zdrowia w państwach ościennych (O2). Do najistotniejszych zagrożeń dla wydolności służby zdrowia zaliczono z kolei: wysoce prawdopodobne wykorzystanie broni masowego rażenia w Polsce lub kraju sąsiednim (T4), pojawiające się epidemie oraz pandemie (T1), a także terroryzm, w tym bioterroryzm (T3).



Rys. 3.9. Uszeregowanie czynników zewnętrznych wpływających na wydolność służby zdrowia pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

W dalszej części analizy poszczególne czynniki zostały uszeregowane zgodnie z ustalonymi miarami ich ważności. Ich wyniki przedstawiono w tabeli 3.11.

Tabela 3.11.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S4 W1 O4 T4
	S2 W3 O1 T1
	S1 W2 O2 T3
Niski	

Źródło: opracowanie własne

Następnie został opracowany szablon matrycy konfrontacji przy wykorzystaniu czynników zidentyfikowanych w poprzednich etapach pod względem ich ważności. Przedstawiono go w tabeli 3.12. Wypełniona matryca, pozwoliła na zwizualizowanie czynników, które muszą być wzięte pod uwagę, aby móc określić zdolności do reagowania na zdarzenia z dużą liczbą ofiar.

Tabela 3.12.
Ocena czynników wpływających na wydolność służby zdrowia

	S4	S2	S1	W1	W3	W2
O4		+	+	-	--	-
O1	+	+	++		--	
O2			+			-
T4	++	+		-	-	-
T1	++	+	+	--	--	--
T3	++	+		--	--	--

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy, po wzięciu pod uwagę najistotniejszych (wybranych przez ankietowanych) czynników, określono stopień odporności państwa w tym obszarze jako **stosunkowo niski**. Zwraca się uwagę na potrzebę dostosowania aktów prawnych i procedur normujących zasady reagowania na zdarzenia z dużą liczbą ofiar w celu zachęcenia i umożliwienia wykonywania pracy personelowi medycznemu emigrującemu z innych państw do Polski. Ponadto możliwość wsparcia cywilnej służby zdrowia przez służby mundurowe w Polsce pozwala na zminimalizowanie potencjalnych zagrożeń, takich jak: użycie broni masowego rażenia, pojawiające się epidemie oraz pandemie, a także działania terrorystyczne. W wyniku analizy stwierdzono, że szczególną uwagę należy zwrócić na konieczność podjęcia działań w celu stworzenia warunków do zmniejszenia niedoborów wśród pracowników służby zdrowia oraz zahamowania odpływu kadry medycznej za granicę[142]. Te dwie słabości mogą znacznie utrudnić działania w przypadku zdarzeń związanych z wybuchem epidemii czy działaniami terrorystycznymi. Eksperci zwrócili także uwagę na konieczność podjęcia działań związanych z niedofinansowaniem służby zdrowia. Ta zdefiniowana słabość państwa może w konsekwencji rzutować na brak możliwości pozyskania i wykorzystania nowych technologii (O4). Może ona także wpłynąć na brak wykorzystania potencjału, jaki stanowi emigrujący do Polski personel medyczny z innych krajów.

3.4.5. Zbezpieczenie zapasów wody pitnej i żywności

Jednym z niezbędnych warunków do zapewnienia bytu ludności jest zapewnienie ciągłości zaopatrzenia w wodę i żywność. Zakłócenia bezpieczeństwa dostaw żywności i wody lub ich skażenie może doprowadzić do masowych ofiar, niedoborów produktów żywnościowych prowadzących do panicznych zakupów i gromadzenia zapasów, przemieszczenia ludności itd. Dodatkowe wyzwania w zakresie bezpieczeństwa w tym

[142] Aktualne dane dotyczące emigracji opierają się tylko na liczbie zaświadczeń wydawanych przez izby zawodowe, które potwierdzają prawo wykonywania zawodu w państwach członkowskich UE. Dane te mają jedynie charakter szacunkowy i nie oddają w pełni rzeczywistej emigracji pracowników ochrony zdrowia. Ponadto nie prowadzi się ilościowych badań dotyczących emigracji polskich profesjonalistów medycznych, co sprawia, że zagadnienie emigracji polskiej kadry medycznej jest wciąż niedostatecznie zbadane. Dane uzyskane z krajowych izb zawodowych pokazują, że o zaświadczenia potwierdzające prawo do wykonywania zawodu w innych krajach Unii Europejskiej (od przystąpienia do niej Polski w 2004) ubiegało się 7–9% praktykujących lekarzy i pielęgniarek. Całkiem duża liczba certyfikatów (ok. 300 w skali roku) została także wydana fizjoterapeutom, co jest szczególnie niepokojące, biorąc pod uwagę, że jest to grupa zawodowa, której funkcjonowanie zostało uregulowane ustawowo dopiero stosunkowo niedawno. Por. A. Domagała, M. Kautsch, A.Kulbat, K. Parzonka, *Exploration of Estimated Emigration Trends of Polish Health Professionals*, [w:] „International Journal of Environmental Research and Public Health", 19(2)/2022, Oxford Academic, 2022.

sektorze obejmują wzrost cen żywności i dostaw wody, co będzie miało wpływ na ich dostępność. Problemy związane z zaopatrzeniem w żywność i wodę mogą być dodatkowo spotęgowane przez wstrząsy w produkcji podstawowych towarów, ze względu na zależność od środków produkcji, jak również przez zakłócenia w łańcuchach rolno-spożywczych. Co więcej, zakłócenia i wyzwania w zakresie bezpieczeństwa dostaw, mogą wpłynąć ujemnie na zdolność do zapewnienia wsparcia cywilnego i utrzymania rozmieszczonych sił wojskowych NATO, w tym w ramach *Host Nation Support*[143].

Przyjmując, że Polska jest samowystarczalna pod względem produkcji żywności warto jednak zwrócić uwagę na potrzebę przygotowania odpowiednich jej zapasów[144]. Należy także stwierdzić, że Polska jest klasyfikowana dopiero na 24 miejscu w Unii Europejskiej pod względem odnawialnych zasobów słodkiej wody przypadających na jednego mieszkańca[145].

W czasie prac związanych z analizą stopnia odporności państwa eksperci zaproponowali kilka istotnych czynników mających wpływ na zabezpieczenie żywności i wody. W tabeli 3.13. zamieszczono najważniejsze (zdaniem ekspertów) z nich. Do najistotniejszych mocnych stron Polski w tym obszarze zaliczono między innymi: ekonomiczną dostępność żywności[146], posiadanie rezerw strategicznych czy samowystarczalność żywnościową. Z kolei jako słabe strony wskazano przede wszystkim: przestarzałe i awaryjne sieci wodociągowe[147], niewystarczający stopień zabezpieczenia dostaw wody na wypadek braku możliwości korzystania z sieci wodociągowych[148].

---

[143] Wsparcie przez państwo-gospodarza (HNS) – cywilna i wojskowa pomoc udzielana przez państwo-gospodarza w czasie pokoju, kryzysu i w czasie wojny sojuszniczym siłom zbrojnym i organizacjom, które są rozmieszczane, wykonują zadanie lub przemieszczają się przez terytorium państwa-gospodarza. Źródło: *Wsparcie przez państwo-gospodarza* – DD-4.5(B) wer. 2, wyd. elektroniczne, CDiS SZ, Bydgoszcz 2019, s. 137.

[144] Polska jest samowystarczalna w produkcji zbóż, części rodzajów mięsa, cukru i nabiału. Natomiast świeże owoce, nasiona i owoce oleiste, miód, tłuszcze i oleje roślinne nie są produkowane w wystarczających ilościach. Por. K. Szałaj, *Czy Polska jest rzeczywiście samowystarczalna żywnościowo? Sprawdzamy!*, Tygodnik Poradnik Rolniczy, 17.03.2022, pobrano z lokalizacji: https://www.tygodnik-rolniczy.pl/articles/wojna-w-ukrainie-rolnictwo/czy-polska-jest-samowystarczalna-zywnosciowo-sprawdzamy-czego-nam-brakuje/ [dostęp: 19.11.2022].

[145] Por. P. Paulewicz-Bazała, *Las w obliczu zagrożenia suszą*, Wodne Sprawy, 13.07.2023, pobrano z lokalizacji: https://wodnesprawy.pl/las-w-obliczu-zagrozenia-susza-kryzys-klimatyczny-p/ [dostęp: 16.08. 2023].

[146] Dostępność ekonomiczna wiąże się z możliwością nabycia żywności przez wszystkie grupy społeczne i w Polsce oceniana jest na poziomie dobrym. Por. M. Kozłowska-Burdziak, *Warunki bezpieczeństwa żywnościowego Polski (ze szczególnym uwzględnieniem województwa podlaskiego)*, „Optimum. Economic Studies", nr 3(97) 2019, s. 40.

[147] *Raport: Utrzymanie i eksploatacja sieci wodociągowych w miastach*, Najwyższa Izba Kontroli, 29.05.2018 r., s. 7.

[148] *Raport: Zapewnienie bezpieczeństwa zaopatrzenia w wodę dużych aglomeracji miejskich na wypadek wystąpienia sytuacji kryzysowych*, Najwyższa Izba Kontroli, 27.07.2017 r., s. 10.

Jako istotne szanse dla zapewnienia zabezpieczenia w wodę i żywność wymieniono przede wszystkim rozwinięte globalne i regionalne łańcuchy dostaw czy wprowadzane i dostępne innowacyjne rozwiązania w systemach zarządzania[149]. Do najczęściej wskazywanych zagrożeń zaliczono postępującą zmianę klimatu, jak również celową działalność przeciwnika (państwowego i niepaństwowego).

Tabela 3.13.

Czynniki wpływające na zabezpieczenie zapasów żywności i wody

S 1. Akty prawne 2. Ekonomiczna dostępność żywności 3. Rezerwy strategiczne 4. Bezpieczeństwo żywnościowe (samowystarczalność) 5. Zapasy żywnościowe	**W** 1. Jakość sieci wodociągowych 2. Stopień zabezpieczenia dostaw wody na wypadek braku możliwości korzystania z sieci wodociągowych (np. po skażeniu) 3. Urządzenia hydrotechniczne 4. Gospodarka wodna
O 1. Globalne i regionalne łańcuchy dostaw 2. Współpraca gospodarcza UE i formuły regionalne 3. Innowacje z zarządzaniu łańcuchami dostaw	**T** 1. Terroryzm (ekoterroryzm) 2. Zmiana klimatu (powodzie, susze) 3. Zakłócenia globalnych łańcuchów dostaw 4. Celowa działalność przeciwnika

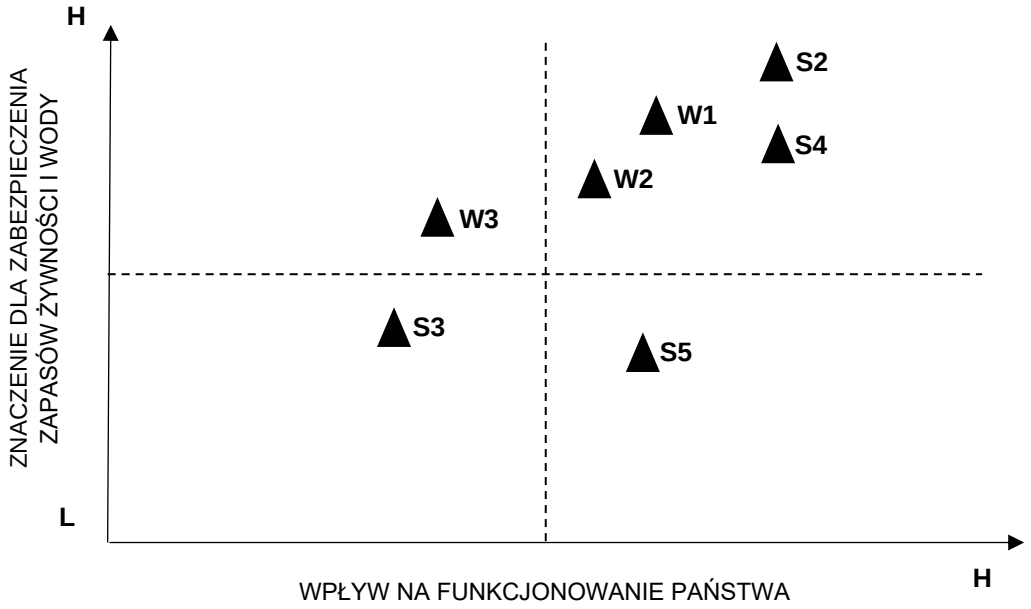
Źródło: opracowanie własne

W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron ze względu na ich znaczenie dla zaopatrzenia w wodę i żywność i ich ogólnych implikacji dla funkcjonowania państwa. Wyniki analizy przedstawiono na rysunku 3.10. Stwierdzono, że do najważniejszych mocnych stron państwa w analizowanym obszarze należą: ekonomiczna dostępność żywności (S2), samowystarczalność żywnościowa (S4) oraz posiadanie rezerw strategicznych[150] (S3). Do najbardziej znaczących wad zaliczono: niską jakość sieci

[149] Por. M. Juchniewicz, *Innowacje w logistyce łańcucha dostaw żywności*, [w:] „Zeszyty naukowe Uniwersytetu Szczecińskiego", nr 875. Problemy Zarządzania, Finansów i Marketingu, nr 41, t. 2, 2015.

[150] Rezerwy żywnościowe są utrzymywane w grupach asortymentowych, np. zboża i produkty zbożowe, mięso i przetwory mięsne, tłuszcze roślinne i zwierzęce, produkty mleczne, inne (np. woda pitna mineralna, cukier). W ramach tych grup asortymentowych utrzymywane są surowce, półprodukty i produkty gotowe, które mogą być udostępniane w celu niwelowania negatywnych skutków wystąpienia różnego rodzaju sytuacji kryzysowych. Przeznaczenie udostępnianych rezerw jest każdorazowo określane w decyzji ministra właściwego ds. energii. Zarówno asortyment rezerw, jak i ich ilość, a także rozmieszczenie w kraju określa Rządowy Program Rezerw Strategicznych, który jest ustalany na okres pięciu lat i jest dokumentem niejawnym. Por. strona internetowa Rządowej Agencji Rezerw Strategicznych, https://www.rars.gov.pl/?dz=rezerwy-zywnosciowe [dostęp 05.12.2022] oraz K. Bartman, *Polsce nie grozi głód, ale potrzebne są rezerwy żywności. Takie, które nie "wyparują" z magazynów*, Money.pl, 28.03.2022, pobrano

wodociągowych (W1), niewystarczający stopień zabezpieczenia dostaw wody na wypadek braku możliwości korzystania z sieci wodociągowych (W2) oraz stan urządzeń hydrotechnicznych[151] (W3).



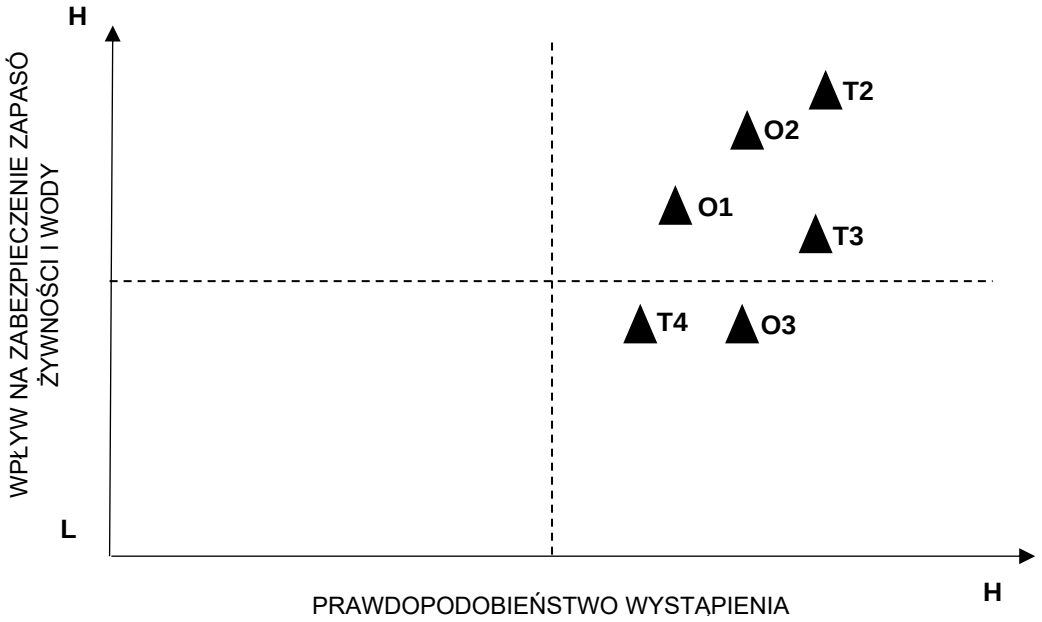
Rys. 3.10. Uszeregowanie czynników wpływających na zabezpieczenie zapasów żywności i wody pod względem stopnia ważności S/W

Źródło: opracowanie własne

W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na zaopatrzenie w wodę i żywność, pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na wykresie 3.11.

z lokalizacji: https://www.money.pl/gospodarka/polsce-nie-grozi-glod-ale-potrzebne-sa-rezerwy-zywnosci-takie-ktore-nie-wyparuja-z-magazynow-6750665549720480a.html [dostęp: 05.12.2022].

[151] I. Świderska, P. Lebiecki, *Stan bezpieczeństwa budowli piętrzących wodę w Polsce na koniec 2009 roku*, Materiał z XXV Konferencji Naukowo-Technicznej, Międzyzdroje 24-27.05.2011 r. oraz *Raport: Nadzór nad stanem technicznym i stanem bezpieczeństwa wodnych budowli piętrzących*, Najwyższa Izba Kontroli, 02.02.2016 r.



Rys. 3.11. Uszeregowanie czynników zewnętrznych wpływających na zabezpieczenie zapasów żywności i wody pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

Jako najbardziej znaczące szanse w omawianym obszarze wskazano: współpracę gospodarczą w ramach UE i formuły współpracy regionalnej (O2), wykorzystanie globalnych i regionalnych łańcuchów dostaw (O1) oraz wprowadzanie innowacyjnych rozwiązań do zarządzania łańcuchami dostaw (O3). Do najistotniejszych zagrożeń dla zapewnienia zaopatrzenia w wodę i żywność zaliczono z kolei: postępującą zmianę klimatu (T2), wywołane różnymi przyczynami zakłócenia globalnych łańcuchów dostaw (T3), a także celową działalność przeciwnika (T4).

Kolejnym etapem analizy na tym etapie było uszeregowanie poszczególnych czynników zgodnie z ustalonymi miarami ich ważności. Ich rezultaty przedstawiono w tabeli 3.14.

Tabela 3.14.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S2 W1 O2 T2
	S4 W2 O1 T3
	S3 W3 O3 T4
Niski	

Źródło: opracowanie własne

W dalszej kolejności opracowano i przedstawiono w tabeli 3.15. matrycę konfrontacji, wykorzystując czynniki zidentyfikowane w poprzednich etapach pod względem ich ważności. Dzięki temu zwizualizowano czynniki, które muszą być wzięte pod uwagę, aby określić odporność państwa w obszarze zaopatrzenia w wodę i żywność.

Tabela 3.15.
Ocena czynników wpływających na zabezpieczenie zapasów żywności i wody

	S2	S4	S3	W1	W2	W3
O2		+	+			-
O1	++	+	+			
O3			+			
T2				--		-
T3		++	+		--	
T4		+	++	-	-	--

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy stwierdzono, że odporność państwa w obszarze zabezpieczenia zapasów żywności i wody jest na **średnim poziomie**. Wysoko oceniany poziom ekonomicznej dostępności żywności świadczy o wyeliminowaniu zagrożenia niedostatku w tym obszarze. Wykorzystanie dostępu do rynków światowych i regionalnych może przyczynić się do zwiększenia dostępnych cenowo produktów na rynku krajowym, jak również do tworzenia niezbędnych rezerw. Samowystarczalność żywnościowa (w głównych asortymentach) jest czynnikiem, który może odegrać pozytywną rolę w sytuacji zakłóceń globalnych łańcuchów dostaw, ich przerwania czy też celowej działalności przeciwnika (np. niedobór zboża na rynkach światowych jako efekt działalności

Rosji w Ukrainie). Także posiadanie przez Polskę odpowiednich rezerw strategicznych może osłabić niekorzystne oddziaływanie powyższych zagrożeń, a tym samym wpływa na wzmacnianie odporności. Zauważalne są również pewne niekorzystne trendy mogące zahamować proces wzmacniania odporności w obszarze zabezpieczenia dostaw wody i żywności. Należy zwrócić uwagę na niski stopień przygotowania sieci wodociągowych do warunków zmieniającego się klimatu oraz niewystarczający stopień zabezpieczenia dostaw wody na wypadek braku możliwości korzystania z sieci wodociągowych. Ponadto ww. słabości systemu mogą przyczynić się do powstania niekorzystnej sytuacji w przypadku celowej działalności przeciwnika.

3.4.6. Odporność infrastruktury telekomunikacyjnej

Systemy i usługi łączności mają kluczowe znaczenie dla odporności państwa. Ich zakłócenie, uszkodzenie lub wyeliminowanie będzie miało bezpośredni i destrukcyjny wpływ na inne sektory, potencjalnie zagrażając ciągłości funkcjonowania państwa, a także utrudniając wsparcie przez siły Sojuszu.

Sektor łączności podlega szybkiej i ciągłej ewolucji technologicznej. Ponadto rosnąca zależność od komunikacji rozproszonej i usług internetowych zwiększyła zależność od krytycznej infrastruktury komunikacyjnej, wzmacniając wymóg ciągłej dostępności oraz zapewnienia dostępu do niezawodnych, bezpiecznych i solidnych usług komunikacyjnych. Infrastruktura ta może być narażona na cyberataki, wtargnięcia lub inne formy, które mogą zakłócić działanie sieci, usług i sprzętu czy obejmować niewykryte zaawansowane i trwałe zagrożenia w celu monitorowania i nadzoru lub kradzieży poufnych danych klientów. Ryzyko to może wzrosnąć w wyniku potencjalnego uzależnienia od sprzedawców wysokiego ryzyka lub poprzez zagraniczną własność, kontrolę lub bezpośrednie inwestycje w krytyczną architekturę komunikacyjną, systemy i łańcuchy dostaw.

W trakcie analizy stopnia odporności Polski zaproponowano szereg czynników wpływających na zdolność do zabezpieczenia infrastruktury komunikacyjnej i umieszczono je w tabeli 3.16. Zdaniem ekspertów do mocnych stron w tym obszarze można zaliczyć między innymi rozwiniętą sieć 5G z możliwością jej dalszej rozbudowy[152] oraz potencjał naukowo-badawczy. Z kolei jako słabe strony wskazano m.in. stan jakościowy sieci teleinformatycznych[153] czy też podatność na zakłócenia cybernetyczne.

Tabela 3.16.

Czynniki wpływające na zapewnienie łączności

S 1. Akty prawne 2. Sieć teleinformatyczna 3. Rozwinięta sieć 5G z możliwością jej dalszej rozbudowy 4. Kolejowa sieć łączności 5. Potencjał naukowo-badawczy	**W** 1. Podatność na zakłócenia cybernetyczne 2. Stosunki własnościowe[154] 3. Współpraca pomiędzy podmiotami będącymi właścicielami 4. Jakość sieci teleinformatycznej
O 1. Członkostwo w UE i NATO i regulacje prawne 2. Współpraca podmiotów gospodarczych w środowisku międzynarodowym 3. Współpraca w ramach agencji kosmicznych 4. Umowy bilateralne w zakresie wykorzystania systemu satelitarnego (np. Polska–Włochy)	**T** 1. Ograniczenia dostępu do nowych technologii 2. Polityka państw trzecich 3. Wrogie działania w cyberprzestrzeni 4. Metale ziem rzadkich – ich dostępność 5. Rywalizacja w kosmosie 6. Zagrożenia naturalne i cywilizacyjne

Źródło: opracowanie własne

W przedmiotowym obszarze zgodzono się, że istnieje wiele możliwości, które przy odpowiednim ich wykorzystaniu mogą korzystnie wpłynąć na rozwój gospodarczy kraju.

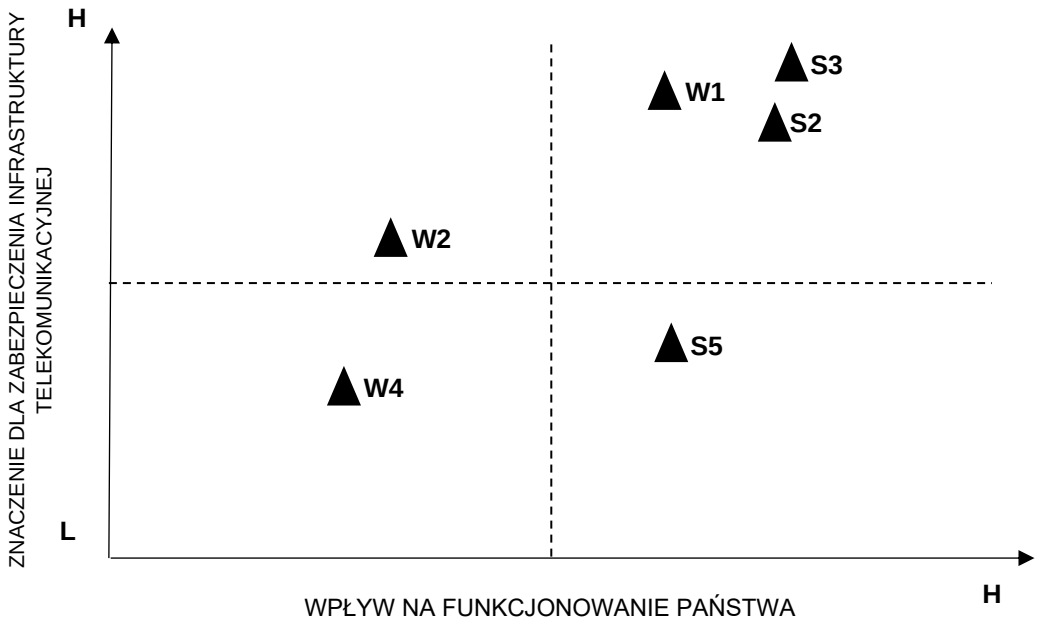
[152] Bardzo ważną zaletą sieci 5G jest dużo wyższy poziom bezpieczeństwa dla danych użytkownika niż w przypadku korzystania z publicznych sieci Wi-Fi. Sieć 5G daje o wiele szybsze, stabilniejsze połączenia i o wiele krótsze czasy reakcji sieci niż obecne rozwiązania. Pozwoli podłączyć do sieci miliony inteligentnych urządzeń, które mogą usprawnić wiele obszarów funkcjonowania państwa. Por. *Strategia 5G dla Polski*, Ministerstwo Cyfryzacji, Warszawa 2018 oraz *5G: sieci telekomunikacyjne nowej generacji*, gov.pl, 17.04.2017, pobrano z lokalizacji: https://www.gov.pl/web/5g/korzysci [dostęp: 06.12.2022].

[153] Eksperci zaliczyli stan sieci teleinformatycznych zarówno do silnych, jak i słabych stron państwa. Wpływ na taką decyzję miało przede wszystkim obecne (ciągle jeszcze nierówny dostęp) niedoskonałości, a z drugiej strony ciągły rozwój tych sieci. Por. *Raport o stanie rynku telekomunikacyjnego w Polsce w 2021 r.*, Urząd Komunikacji Elektronicznej, Warszawa, czerwiec 2022 r.

[154] Np. mające wpływ na współpracę przedsiębiorcy telekomunikacyjnego z zarządcami dróg i przedsiębiorstwami elektroenergetycznymi. Przyp. autora.

Jako najbardziej istotne wskazano przede wszystkim na członkostwo zarówno w UE, jak i NATO oraz współpracę agencji kosmicznych w celu rozwoju telekomunikacji[155]. Do najczęściej wskazywanych zagrożeń zaliczono ograniczenia w dostępie do niektórych technologii, a także zagrożenia naturalne i cywilizacyjne.

W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron pod względem ich znaczenia dla funkcjonowania państwa w przedmiotowym obszarze. Wyniki analizy przedstawiono na rysunku 3.12. Stwierdzono, że do najistotniejszych mocnych stron państwa polskiego w analizowanym obszarze należy zaliczyć: rozwiniętą sieć 5G z możliwością jej dalszej rozbudowy (S3), konsekwentnie rozbudowywaną sieć teleinformatyczną (S2) oraz potencjał naukowo-badawczy (S5). Z kolei jako najbardziej znaczące słabości wskazano podatność na zakłócenia cybernetyczne (W1), dostępność metali ziem rzadkich (W4) oraz stosunki własnościowe podmiotów odpowiadających za rozwój w obszarze infrastruktury teleinformatycznej (W2).

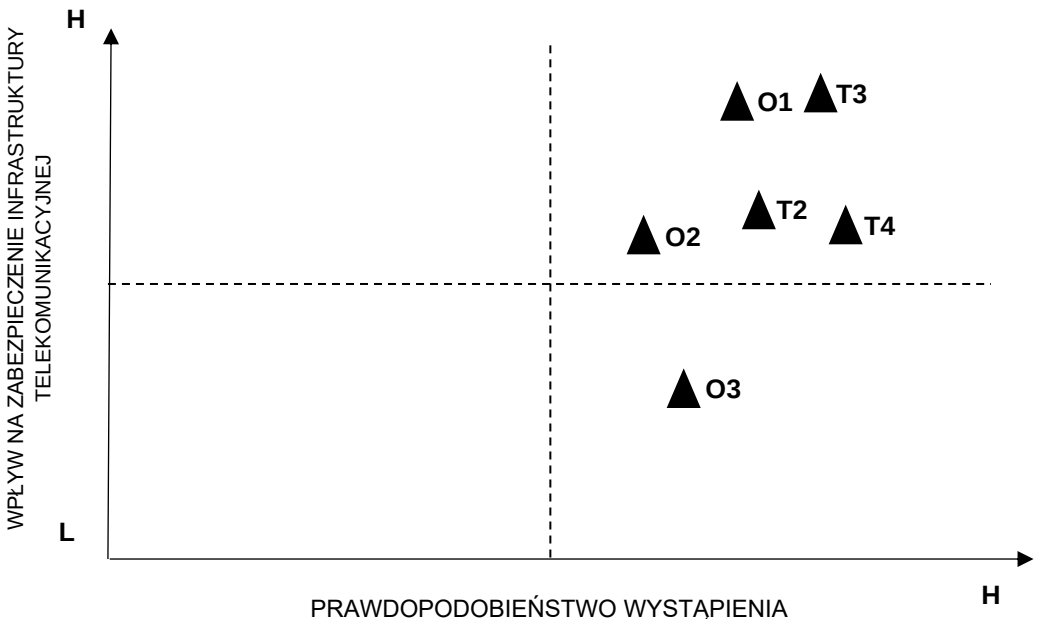


Rys. 3.12. Uszeregowanie czynników wpływających na zabezpieczenie infrastruktury teleinformatycznej pod względem stopnia ważności S/W

Źródło: opracowanie własne

[155] Ważnym aspektem działalności Polskiej Agencji Kosmicznej jest promowanie rozwoju technologii satelitarnej, którą można wykorzystać w życiu codziennym, w tym w komunikacji, nawigacji, monitoringu środowiska i prognozowaniu pogody. Por. *Ocena stanu rozwoju badań i użytkowania przestrzeni kosmicznej – raport za 2021 rok*, Polska Agencja Kosmiczna, Gdańsk 2022.

W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na zabezpieczenie infrastruktury teleinformatycznej pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na rysunku 3.13. Jako najbardziej znaczące szanse w omawianym obszarze wskazano na: członkostwo w UE i NATO i czytelne regulacje prawne (O1), współpracę podmiotów gospodarczych w środowisku międzynarodowym (O2) oraz współpracę w ramach agencji kosmicznych (O3). Jako najistotniejsze zagrożenia wskazano z kolei: wrogie działania w cyberprzestrzeni (T3), konfrontacyjną politykę państw trzecich (T2), a także ograniczoną dostępność metali ziem rzadkich (T4).



Rys. 3.13. Uszeregowanie czynników zewnętrznych wpływających na zabezpieczenie infrastruktury teleinformatycznej pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

Kolejnym etapem analizy w tym etapie było uszeregowanie poszczególnych czynników zgodnie z ustalonymi miarami ich ważności. Rezultaty przedstawiono w tabeli 3.17.

Tabela 3.17.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S3 W1 O1 T3
	S2 W4 O2 T2
	S5 W2 O3 T4
Niski	

Źródło: opracowanie własne

Tabela 3.18. zawiera matrycę konfrontacji, w której zwizualizowano zidentyfikowane w poprzednich etapach czynniki ze względu na ich stopień ważności, co w konsekwencji pozwoliło na określenie odporności państwa w obszarze zabezpieczenia infrastruktury komunikacyjnej.

Tabela 3.18.
Ocena czynników wpływających na zabezpieczenie infrastruktury teleinformatycznej

	S4	S2	S5	W1	W4	W2
O1			+			-
O2	++	++	+	--	--	-
O3	+		+	-	-	
T3	+	+	++	--	--	
T2	+	+		---	--	--
T4			+			

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy, po wzięciu pod uwagę najistotniejszych, wybranych przez ankietowanych, czynników, określono stopień odporności państwa w tym obszarze jako **średni z tendencją wzrostową**. Należy dążyć do dalszej rozbudowy sieci teleinformatycznych wykorzystując członkostwo w UE i NATO. Co więcej, współpraca w ramach projektów międzynarodowych oraz z zagranicznymi przedsiębiorstwami pozwoli na rozbudowę ww. sieci oraz na wykorzystanie najnowszych zdobyczy technologii. Posiadany potencjał naukowy-badawczy, a przede wszystkim wykształcony i doświadczony potencjał ludzki, przy właściwym ukierunkowaniu może stać się nieocenionym zasobem do tworzenia linii obrony przed wrogimi działaniami

w cyberprzestrzeni. W trakcie analizy zwrócono uwagę na podatność systemu na zagrożenia cybernetyczne, które mogą utrudnić lub wręcz uniemożliwić korzystną współpracę podmiotów gospodarczych w środowisku krajowym i międzynarodowym, szczególnie w warunkach celowego działania przeciwnika. Uzależnienie od importu metali ziem rzadkich może, w warunkach celowej działalności państw trzecich, doprowadzić w konsekwencji do zmniejszenia poziomu inwestycji związanych z rozwojem infrastruktury teleinformatycznej.

3.4.7. Odporność systemów transportu

Cywilny system transportowy odgrywa zasadniczą rolę w zapewnieniu usług, które umożliwiają zarówno szybkie rozmieszczenie oraz utrzymanie sił wojskowych Sojuszu, jak i zaspokojenie potrzeb ludności i gospodarki w czasie pokoju, kryzysu i konfliktu[156]. Dlatego też warunkiem niezbędnym jest zapewnienie, że siły NATO mogą szybko przemieszczać się po terytorium kraju, a cywilne sieci transportowe pozostają funkcjonalne i efektywne, aby w sposób ciągły wspierać działania zarówno cywilne, jak i wojskowe. W trakcie pandemii Covid-19 uwidoczniły się problemy związane z globalnym łańcuchem dostaw, co z kolei pokazało, że krajowe łańcuchy dostaw mogą być i są często pod silnym wpływem innych państw, które mogą mieć całkowicie różne interesy, często odległe od celów Polski.

Podczas próby określenia stopnia odporności państwa polskiego w tym obszarze poszczególni eksperci wskazali na wiele czynników wpływających na postrzeganie możliwości infrastruktury transportowej. W tabeli 3.19. przedstawiono te najczęściej podawane. Większość specjalistów zalicza do mocnych stron państwa dotychczasowe inwestycje w poprawę infrastruktury transportowej oraz potencjał naukowo-badawczy.

Z kolei do słabych stron eksperci zaliczyli przede wszystkim słabą drogową dostępność regionalną, stan techniczny dróg powiatowych czy niską przepustowość odcinków. Jako istotne szanse wskazywano przede wszystkim rozwój nowoczesnych technologii i powiazania z europejskim oraz światowym systemem transportowym. Do najczęściej występujących zagrożeń dla infrastruktury transportowej zaliczono niewystarczającą przepustowość sieci drogowej w przypadku zagrożeń militarnych czy możliwość blokady szlaków komunikacyjnych przez państwa trzecie lub organizacje terrorystyczne.

[156] Por. *Strategia Zrównoważonego Rozwoju Transportu do 2030 roku*, Ministerstwo Infrastruktury, Warszawa 2019.

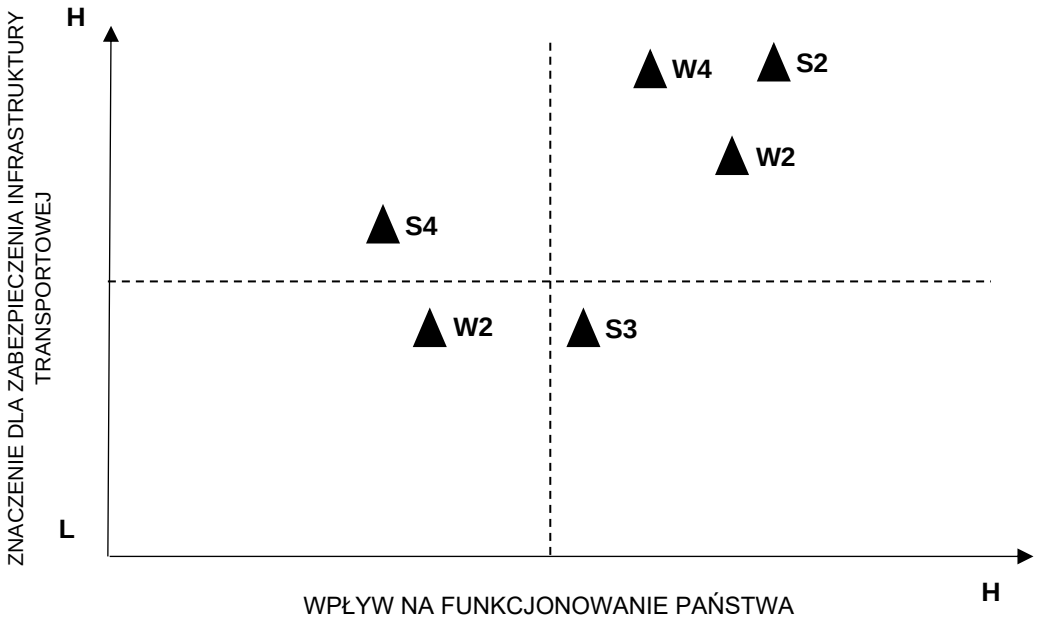
Tabela 3.19.

Czynniki wpływające na zabezpieczenie infrastruktury transportowej

S 1. Akty prawne 2. Inwestycje w poprawę infrastruktury 3. Nowoczesna infrastruktura transportu lotniczego 4. Potencjał naukowo-badawczy	**W** 1. Brak pełnego dostępu do sieci dróg szybkiego ruchu na wschodzie kraju 2. Słaba drogowa dostępność regionalna w części północno-wschodniej i wschodniej, jak również na Pomorzu Środkowym 3. Finansowanie dróg powiatowych i gminnych i ich stan techniczny 4. Brak spójnej sieci autostrad i dróg ekspresowych pomiędzy ośrodkami aglomeracyjnymi i niewystarczające powiązania z pozostałymi gałęziami transportu lądowego (drogowym, wodnym śródlądowym) 5. Niska przepustowość odcinków (w tym łączących porty morskie)
O 1. Powiązanie z europejskim i globalnym systemem transportowym 2. Nowoczesne technologie, w tym inteligentne systemy transportowe 3. Inicjatywy międzynarodowe	**T** 1. Możliwość blokady szlaków komunikacyjnych (np. cieśniny duńskie) 2. Zagrożenia naturalne 3. Niewystarczająca przepustowość sieci drogowej w przypadku zagrożeń militarnych

Źródło: opracowanie własne

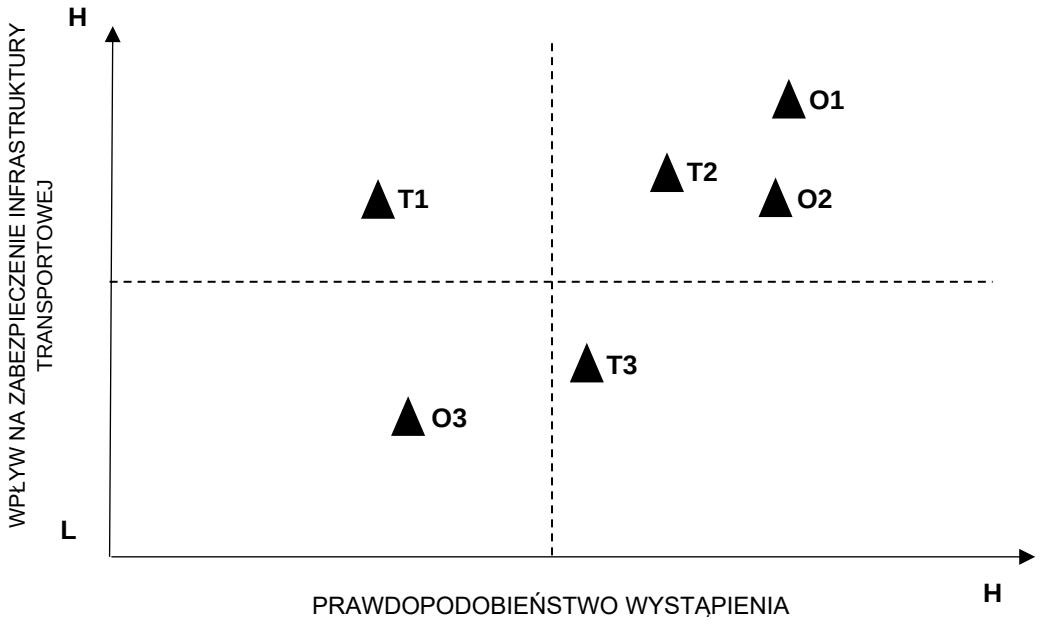
W następnej kolejności podjęto próbę określenia mocnych (S) i słabych (W) stron pod kątem ich znaczenia dla zapewnienia sprawności infrastruktury transportowej. Wyniki analizy przedstawiono na rysunku 3.14. Stwierdzono, że do najistotniejszych mocnych stron państwa polskiego w analizowanym obszarze zaliczyć należy: inwestycje w poprawę infrastruktury (S2), potencjał naukowo-badawczy (S4) oraz nowoczesną infrastrukturę transportu lotniczego (S3). Z kolei jako najbardziej znaczące słabości wskazano: brak spójnej sieci autostrad i dróg ekspresowych pomiędzy ośrodkami aglomeracyjnymi i niewystarczające powiązania z pozostałymi gałęziami transportu lądowego (drogowym, wodnym śródlądowym) (W4), niską przepustowość odcinków (w tym łączących porty morskie) (W5) oraz słabą drogową dostępność regionalną w części północno-wschodniej i wschodniej, jak również na Pomorzu Środkowym (W2).



Rys. 3.14. Uszeregowanie czynników wpływających na zabezpieczenie infrastruktury transportowej pod względem stopnia ważności S/W

Źródło: opracowanie własne

W dalszej części analizy podjęto próbę oceny i uszeregowania szans (O) i zagrożeń (T) mających wpływ na infrastrukturę transportową pod względem prawdopodobieństwa ich wystąpienia. Wyniki zobrazowano na rysunku 3.15. Jako najbardziej znaczące szanse w omawianym obszarze wskazano: powiązanie z europejskim i globalnym systemem transportowym (O1), nowoczesne technologie, w tym inteligentne systemy transportowe (O2) oraz inicjatywy międzynarodowe zmierzające do poprawy wykorzystania elementów infrastruktury (O3). Do najistotniejszych zagrożeń dla infrastruktury transportowej zaliczono z kolei: możliwość blokady szlaków komunikacyjnych (T1), zagrożenia naturalne (T2), a także niewystarczająca przepustowość sieci drogowej w przypadku zagrożeń militarnych (T4).



Rys. 3.15. Uszeregowanie czynników zewnętrznych wpływających na zabezpieczenie infrastruktury transportowej pod względem wpływu i prawdopodobieństwa ich wystąpienia

Źródło: opracowanie własne

W dalszej części analizy poszczególne czynniki uszeregowane zostały zgodnie z miarami ich ważności. Ich wyniki przedstawiono w tabeli 3.20.

Tabela 3.20.
Priorytetyzacja zidentyfikowanych czynników

Wysoki	
PRIORYTET	S2 W4 O1 T1
	S4 W5 O2 T2
	S3 W2 O3 T4
Niski	

Źródło: opracowanie własne

W opracowanej matrycy konfrontacji (tabela 3.21.) zwizualizowano zidentyfikowane w poprzednich etapach czynniki ze względu na ich stopień ważności, co w konsekwencji pozwoliło na określenie odporności państwa w obszarze zabezpieczenia infrastruktury transportowej.

Tabela 3.21.
Ocena czynników wpływających na zabezpieczenie infrastruktury transportowej

	S2	S4	S3	W4	W5	W2
O1			+			-
O2	++	++	+	--	--	-
O3	+		+	-	-	
T1	+	+	++	--	--	
T2	+	+		---	--	--
T3			+			

Źródło: opracowanie własne

W wyniku przeprowadzonej analizy, po wzięciu pod uwagę najistotniejszych (wybranych przez ankietowanych) czynników, określono stopień odporności państwa w tym obszarze jako **średni**. Wysokie inwestycje w poprawę infrastruktury transportowej oraz posiadany potencjał naukowo-badawczy pozwalają na efektywne wykorzystanie zdobyczy technologicznych w projektowaniu oraz realizacji zaplanowanych inwestycji. W konsekwencji elementy tej infrastruktury mogą przyczynić się do rozwoju istniejącej sieci połączeń globalnych i regionalnych. Z kolei nowoczesna infrastruktura transportu lotniczego może umożliwić zachowanie ciągłości łańcuchów dostaw w wypadku zagrożeń związanych z blokadą pozostałych szlaków komunikacyjnych. W wyniku analizy określono ponadto, że należy zwrócić szczególną uwagę na konieczność podjęcia działań zmierzających do utworzenia spójnej sieci autostrad i dróg ekspresowych pomiędzy ośrodkami aglomeracyjnymi oraz powiązań z pozostałymi gałęziami transportu lądowego (drogowym, wodnym śródlądowym). Ta zdefiniowana słabość może w konsekwencji wpłynąć na brak możliwości prowadzenia dostaw oraz zachowania swobody manewru w sytuacji blokady linii komunikacyjnych w wyniku działalności przeciwnika czy też z przyczyn naturalnych. Zagrożenia mogą zostać spotęgowane poprzez niską przepustowość odcinków (w tym łączących porty morskie) oraz słabą drogową dostępność regionalną.

3.5. Konkluzje

Prace związane z określeniem stanu odporności Polski związane były z koniecznością zidentyfikowania różnorodnych obszarów i czynników wpływających na jej budowę i utrzymanie. Podjęta próba zobrazowania stanu odporności została odzwierciedlona w tabeli 3.22.

Tabela 3.22.
Graficzne zobrazowanie stanu odporności Polski

OBSZAR ODPORNOŚCI	STOPIEŃ ODPORNOŚCI
Gwarancja ciągłości rządów	
Zabezpieczenie dostaw energii	↗
Zarządzanie przemieszczaniem się ludności	↗
Wydolność służby zdrowia	
Zabezpieczenie zapasów żywności i wody	
Zabezpieczenie infrastruktury telekomunikacyjnej	↗
Zabezpieczenie infrastruktury transportowej	

Źródło: opracowanie własne

W wyniku prowadzonych badań można zaryzykować stwierdzenie, że odporność Polski kształtuje się na średnim poziomie. Najlepszą sytuację można zaobserwować w obszarze zapewnienia ciągłości rządów, co jest związane z przestrzeganiem demokratycznych reguł rządzenia państwem i członkostwem zarówno w NATO, jak i UE. Z kolei na średnim poziomie kształtuje się odporność w obszarach zabezpieczenia zapasów żywności i wody, infrastruktury telekomunikacyjnej oraz transportowej. Warto także zaznaczyć, że zaobserwowano pozytywny trend wzrostu poziomu odporności w obszarze zabezpieczenia infrastruktury telekomunikacyjnej. Jako najmniej odporne obszary zidentyfikowano: poziom zabezpieczenia dostaw energii, zarządzanie przemieszczaniem się ludności oraz wydolność służby zdrowia. Warto nadmienić, że o ile w dwóch pierwszych obszarach zauważalny jest trend wzrostu, to w obszarze wydolności służby zdrowia sytuacja wymaga podjęcia zdecydowanych działań w zakresie zwiększenia jej efektywności.

Uzasadnione wydaje się stwierdzenie, że występowanie stosunkowo wysokiego lub przynajmniej średniego poziomu odporności w tych obszarach, w których państwo polskie może prowadzić samodzielne działania, jest uzależnione przede wszystkim od czynników wewnętrznych. Z kolei w obszarach, w których Polska jest uzależniona od czynników zewnętrznych (np. dostawy surowców energetycznych, migracje), zaobserwowano stosunkowo niski stan odporności. Wyjątek stanowi poziom służby zdrowia, który wynika z wieloletnich zaniedbań i wymaga zdecydowanych, systemowych działań. Pozytywnie konkludując: jako państwo posiadamy zdolność do kształtowania właściwego poziomu odporności w obszarach, które są zależne od nas samych.

Rozpatrując kwestię odporności, należy zwrócić uwagę, że prace związane z jej wzmacnianiem czy wręcz budową wymagają skoordynowanych wysiłków wszystkich podmiotów odpowiedzialnych za bezpieczeństwo państwa. Analizując z kolei liczne definicje określające odporność, można dojść do wniosku, że jest ona przeciwieństwem niestabilności. Upraszczając, zapewnienie stabilności przyczynia się do zapewnienia odporności. Aby jednak taka sytuacja miała miejsce, konieczne jest jasne zdefiniowanie, jakimi cechami odporne państwo powinno się charakteryzować.

W przedmiotowym opracowaniu podjęto próbę określenia takich uwarunkowań. Dzięki identyfikacji tych cech można było w dalszej kolejności pokusić się o wyspecyfikowanie zagrożeń dla odporności. W niniejszym opracowaniu podjęto także próbę zwrócenia uwagi na wzajemne przenikanie się zagrożeń w poszczególnych obszarach. Zniwelowanie ryzyka wystąpienia zagrożenia w jednym sektorze z dużym prawdopodobieństwem wpłynie na zwiększenie odporności w innych. Z kolei sytuacja odwrotna może doprowadzić do wystąpienia niestabilności w znacznie większym zakresie. Dlatego też problematyka budowania czy też wzmacniania odporności powinna być traktowana holistycznie. Nie można skupiać się tylko na rozwijaniu stabilności we własnych sektorach. W związku z powyższym celowe wydaje się przeprowadzanie okresowych przeglądów stanu odporności, identyfikacja jej słabych punktów w celu konsekwentnego jej rozwijania.

Na szczycie w Madrycie w 2022 roku NATO ustanowiło nowy poziom odniesienia dla swojej postawy odstraszania i obrony zgodnie z podejściem 360 stopni w domenach lądowej, powietrznej, morskiej, cybernetycznej i kosmicznej oraz wobec wszystkich innych zagrożeń i wyzwań. Integralną częścią postawy Sojuszu jest wzmocnienie odporności narodowej i zbiorowej, w tym poprzez utrzymanie i zwiększenie bezpieczeństwa

infrastruktury krytycznej, kluczowych gałęzi przemysłu, łańcuchów dostaw i sieci przesyłu informacji[157]. Podkreśla się, że budowanie i umacnianie odporności jest kluczowym aspektem działań w zakresie wzmocnienia zdolności do odstraszania, zwiększenia gotowości do obrony, dostosowania do coraz większego wykorzystania nowoczesnych technologii i zmian klimatu. Istotną kwestią w tej sferze jest zwiększanie zdolności społeczeństwa do przygotowania się, reagowania, odzyskiwania sił i adaptacji do pełnego zakresu wyzwań i zagrożeń. Trwająca wojna w Ukrainie, Covid-19, rosnąca rywalizacja geopolityczna itd. wskazują na znaczenie odporności budowanej w odpowiedzi na wszelkie zagrożenia (np. związane z cyberatakami, incydentami chemicznymi, biologicznymi, radiologicznymi i nuklearnymi, terroryzmem, pandemiami czy też klęskami naturalnymi) i opartej na całym społeczeństwie. Można stwierdzić, że odporność jest istotnym czynnikiem odstraszania – stworzenie u przeciwnika przekonania, że atak nie osiągnie zamierzonych celów.

Oczywiste jest, że budowa i umacnianie odporności wymaga ścisłej współpracy cywilno-wojskowej. Szczególnego wymiaru współpraca ta nabiera w przypadku konfliktu zbrojnego na terytorium Polski przy jednoczesnym wejściu sił sojuszniczych. Tworzy się wówczas potrzeba zabezpieczenia nie tylko bytu ludności cywilnej, ale i również wchodzących wojsk NATO.

Członkostwo Polski w NATO i Unii Europejskiej jest uważane za czynnik mający wpływ na zwiększanie narodowej odporności, a jednocześnie jest ogromną szansą na dalszy jej rozwój. Biorąc pod uwagę fakt, że Unia Europejska została uznana za strategicznego partnera NATO, zasadne jest dążenie do pełnego wykorzystania możliwości jakie te dwie organizacje oferują.

Właściwe wykorzystanie posiadanego potencjału naukowo-badawczego może przyczynić się do rozwoju odporności w większości zidentyfikowanych obszarów poprzez planowanie budowy nowoczesnych − trudnych do zakłócenia i łatwych do odbudowy (naprawy) − sieci. Szczególnego znaczenia nabiera fakt posiadania zdolności do implementacji nowych technologii, które z jednej strony są wrażliwe na oddziaływanie, z drugiej jednak pozwalają na budowanie nowoczesnych systemów zwiększających odporność i bezpieczeństwo. Holistyczne traktowanie szans i wyzwań związanych z nowymi

[157] Por. *NATO 2022 Strategic Concept*, NATO, 29.06.2022, pobrano z lokalizacji: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [dostęp: 27.07.2022].

technologiami z całą pewnością pozwoli zbudować odporność we wszystkich zidentyfikowanych obszarach.

Szczególnego wymiaru nabiera, na co wskazują doświadczenia z Ukrainy, ochrona infrastruktury krytycznej. Jej trwałość i odporność pozwalają na realizację zadań związanych z bezpieczeństwem ludności cywilnej oraz zapewnieniem swobody działań sił zbrojnych Polski i Sojuszu. Paradoksalnie wojna w Ukrainie, a także pandemia Covid-19 i płynące z nich wnioski pozwoliły, i wciąż pozwalają, na podjęcie niezbędnych działań zwiększających poziom bezpieczeństwa narodowego, a tym samym odporności.

Nie ulega wątpliwości, że każdy z analizowanych obszarów odporności państwa wpływa na gotowość cywilną oraz na system militarny. Jednym z najlepszych sposobów sprawdzenia przygotowania do realizacji zadań związanych z zapewnieniem bezpieczeństwa dla mieszkańców oraz funkcjonowania infrastruktury krytycznej jest przeprowadzenie ćwiczeń obejmujących swym zakresem zarówno system niemilitarny, jak i militarny. Realistyczne ćwiczenia umożliwiają przede wszystkim zweryfikowanie przygotowanych uprzednio planów, procedur oraz odpowiednie zgranie wszystkich elementów.

ROZDZIAŁ IV

CHARAKTERYSTYKA SYSTEMÓW ANTYDOSTĘPOWYCH WYBRANYCH PAŃSTW

W poprzednim rozdziale dokonano analizy odporności Polski na podstawie siedmiu obszarów wskazanych w czasie szczytu NATO w Warszawie, które są systematycznie sprawdzane i oceniane[158]. Jednym z komponentów składających się na zdolność do obrony państwa lub też części jego terytorium jest rozbudowany system antydostępowy. Taki system może być traktowany jednocześnie jako jeden z elementów odstraszania (ang. *deterrence*), jak i również odporności. Posiadanie zdolności do uniemożliwienia lub chociażby utrudnienia wejścia na terytorium kraju oraz uświadomienie przeciwnikowi faktu ich posiadania sprawia, że stworzony został dylemat na poziomie strategicznym lub operacyjnym. Z drugiej strony system antydostępowy w poważnym stopniu może przyczynić się do utrzymania odporności (np. poprzez osłonę elementów infrastruktury krytycznej, a poprzez to zachowanie jej zdolności do dalszego funkcjonowania).

Aby oddziaływać na przeciwnika na całej głębokości i we wszystkich domenach, celowe jest, aby system antydostępowy charakteryzował się takimi zdolnościami, wykorzystując do tego zarówno podsystem militarny, jak i niemilitarny. Zaangażowanie każdego z tych podsystemów umożliwi zachowanie ciągłości funkcjonowania państwa, zapewnienie bytu ludności, a także może się przyczynić do zadania znaczących strat przeciwnikowi i opóźnienia lub zatrzymania jego działań, stworzenia warunków do wykonania zwrotów zaczepnych lub umożliwienia przybycia sił wzmocnienia NATO. Należy zauważyć, że posiadanie zdolności antydostępowych jest ściśle związane z pełnym wykorzystaniem czynników operacyjnych: czasu, siły i przestrzeni z integralną rolą informacji jako czynnika krytycznego. Zwrócił na to uwagę Milan Vego, który stwierdził, że „...bez zdolności do prowadzenia ruchów na dużą skalę na lądzie, na morzu i w powietrzu, prowadzenie operacji jest w zasadzie pustą ideą. Sukces każdej większej operacji lub kampanii zależy od swobodnego przemieszczania się swoich sił w teatrze[159]".

Celem niniejszego rozdziału jest przedstawienie istoty koncepcji antydostępowej oraz wskazanie elementów wchodzących w skład systemów A2/AD (ang. *Anti-Access/Area Denial*). Ponadto podjęto próbę opisania dwóch najbardziej reprezentatywnych sposobów

[158] W 2022 roku dokonano kolejnej takiej oceny na podstawie wytycznych *Resilience Committee*. Przyp. aut.
[159] M. Vego, *Joint Operational Warfare: Theory and practice*, Naval War College, 2007, s. III-7.

rozbudowy takich systemów, zrealizowanych przez Chiny i Rosję. Zwrócono uwagę na podstawowe różnice w sposobie ich budowy, a przede wszystkim na odmienne podejście do określenia celów, które stały u podstaw ich tworzenia.

4.1. Pojęcie i geneza systemów antydostępowych

Jak wspomniano w rozdziale I, koncepcje czy też rozwiązania typu *zakaz dostępu* nie są odkryciem XXI wieku, a raczej swoistym rozwinięciem idei prowadzenia takich działań w przestrzeni powietrznej i kosmicznej, na lądzie i morzu, a także w cyberprzestrzeni. Należy podkreślić, że chociaż część z omawianych pojęć jest stosunkowo nowa, to siły zbrojne w ramach prowadzenia działań stawały w obliczu poważnych wyzwań związanych ze wzbranianiem dostępu do określonych obszarów. Oznacza to, że takie podejście (koncepcja) nie jest zupełnie nowym sposobem prowadzenia walk, a jedynie wynikiem ewoluowania tych stosowanych w przeszłości na wyższy poziom technicznego zaawansowania, zmiany ilościowej i jakościowej sprzętu wojskowego (SpW) oraz zmiany, która zaszła w taktyce i technice wykorzystania posiadanego potencjału (bardzo często nieszablonowego, niekonwencjonalnego lub hybrydowego)[160].

Należy zwrócić uwagę, że A2/AD jest pojęciem funkcjonującym w zachodniej przestrzeni pojęć wojskowych, co oznacza, że nie musi być w ten sposób nazywana w Rosji czy Chinach. Budowa przez te państwa własnych zdolności antydostępowych spowodowała konieczność zmian w koncepcjach prowadzenia działań, zarówno w Europie, jak i na Dalekim Wschodzie, przez USA oraz NATO[161]. Taka sytuacja wynika przede wszystkim z faktu, że podstawą działania sił Sojuszu, a Stanów Zjednoczonych w szczególności, jest utrzymanie swobody przerzutu i przemieszczenia własnych wojsk, sił i środków zaopatrzenia oraz uzupełnień na teatr/y prowadzenia działań dla samodzielnego prowadzenia operacji lub dla wsparcia sił sojusznika/koalicjanta. Wiąże się z tym

[160] Zachodzące zmiany w ładzie globalnym wskazują na działania hybrydowe jako te, które wymagają ciągłych analiz w celu ustalenia ich znaczenia w procesie umacniania władzy i wpływów podmiotów państwowych i niepaństwowych na przyszłe środowisko bezpieczeństwa. Szerzej zobacz analizy CDiS SZ: *Analiza raportu Sojuszniczego Dowództwa Transformacji (ACT) pt. Strategic Foresight Analysis (SFA) 2017* (pol. *Raport z 2017 roku – analizy strategiczne środowiska bezpieczeństwa*), Bydgoszcz 2017, rozdział 2.; *Analiza dokumentu pt. „Framework for Future Alliance Operations – FFAO (2015)"* (pol. *Założenia do przyszłych operacji Sojuszu – 2015*), Bydgoszcz 2016, rozdział 2.5; *Analiza dokumentu pt. „Global Strategic Trends – Out To 2045"* (pol. *Strategiczne Trendy Globalne do 2045 roku*), Bydgoszcz 2015, rozdział 5. i 6.

[161] Por.: J. Bartosiak, *Koncepcja operacyjna wojny powietrzno-morskiej na zachodnim Pacyfiku*, analiza Fundacji Republikańskiej, Warszawa 2012; *Joint Operational Access Concept (JOAC)*, U.S. Department of Defense, Waszyngton 2012.

konieczność zdobycia i utrzymania określonego stopnia kontroli przestrzeni powietrznej oraz panowania na morzu[162].

Aby w pełni zrozumieć tę koncepcję, należy zacząć od wyjaśnienia jej podstaw, tak by poznać wyzwania, które można napotykać w czasie przełamywania systemu A2/AD. Działania podejmowane w ramach **A2** (przeciwdziałanie dostępowi) zapobiegają atakom lub pogarszają zdolności atakujących sił w zakresie wejścia w broniony obszar[163]. W działaniach tych wykorzystuje się ukształtowanie terenu lub rozbudowę inżynieryjną, a także posiadane zdolności operacyjne lub dyplomatyczne[164]. Przykładem wykorzystania warunków terenowych (geograficznych) może być zmuszenie przeciwnika do prowadzenia działań w dużej odległości od baz morskich czy też użytecznych lotnisk. To również umiejętne wykorzystanie naturalnych warunków terenowych danego państwa (np. Finlandia, Szwajcaria). Z kolei przykładem zastosowania kwestii dyplomatycznych lub politycznych (w ramach działań A2) może być sytuacja, gdy jeden lub więcej krajów w regionie, gdzie będzie prowadzona operacja, wzbrania lub ogranicza zdolności wojsk do rozmieszczania sił na ich suwerennym terytorium lub przemieszczenia sił przez jego terytorium, dokonania przelotu przez jego przestrzeń powietrzną[165]. Dobrymi przykładami tego typu działań może być przemieszczanie wojsk (w tym SZ RP) w ramach operacji koalicyjnych i sojuszniczych w Iraku i Afganistanie oraz wykorzystanie sił powietrznych koalicji w Syrii w ramach operacji przeciwko państwu islamskiemu[166]. Z kolei **AD** (pozbawienie swobody działania) sprowadza się do ograniczenia swobody działania na zajmowanym przez przeciwnika terenie. W ten sposób doprowadza się do obniżenia zdolności sił rozmieszczonych na

[162] Panowanie na morzu – swoboda w zakresie wykorzystania obszarów morskich i uniemożliwienie ich wykorzystania przez przeciwnika w środowisku podwodnym, nawodnym i nadwodnym, AAP-6, *Słownik terminów i definicji NATO,* NSO, Bruksela 2017, s. 112.

[163] Do tego celu wykorzystywane są przede wszystkim środki rażenia dalekiego zasięgu. Przyp. autora.

[164]*Gaining and Maintaining Access: An Army–Marine Corps Concept*, U.S. Army and U.S. Marine Corps, version 1.0, Fort Eustis 2012, s. 3.

[165] Przykładem może być koalicyjna operacja Iracka Wolność (ang. *Iraqi Freedom*) prowadzona na terenie Iraku, gdzie niezbędne było wykorzystanie terenu i przestrzeni powietrznej sąsiedniego Kuwejtu oraz uzyskanie wszelkich niezbędnych zgód dyplomatycznych celem zapewnienia bezpieczeństwa przelatującym i stacjonującym wojskom koalicji lub przemieszczenie przez terytorium Pakistanu wydzielonych do operacji ISAF sił i środków SZ RP. Przyp. aut.

[166] Na podstawie porozumienia między Rosją a Syrią oraz zgody Rady Federacji (izby wyższej rosyjskiego parlamentu) Naczelny Dowódca Sił Zbrojnych Federacji Rosyjskiej wydał rozkaz o utworzeniu i rozmieszczeniu w Syrii z dniem 30.09.2015 r. komponentu powietrznego Sił Powietrzno-Kosmicznych FR. Przemieszczenie statków powietrznych rozpoczęło się od samolotów Su-30SM. Szerzej zobacz analiza: R. Reczkowski, *Implikacje geopolityczne i wojskowe dla Polski i SZ RP z zaangażowania Federacji Rosyjskiej (FR) w konflikt domowy w Syrii*, CDiS SZ, E-Biblioteka, Bydgoszcz 2016.

obszarze operacyjnym[167] i wchodzących na ten obszar. Istotne znaczenie przy rozpatrywaniu zagadnień związanych z A2 oraz AD ma fakt, że dosyć trudno jest określić różnice pomiędzy nimi, gdyż są one stosunkowo względne[168]. Należy zwrócić uwagę na fakt, że używane środki mają charakter asymetryczny i bardzo często są wykorzystywane przez podmioty potencjalnie słabsze, korzystające z przewagi wynikającej z działania na własnym terytorium (lub w jego pobliżu).

Należy także stwierdzić, że działania w ramach A2/AD obejmują również możliwości prowadzenia operacji w przestrzeni kosmicznej (np. zakłócanie i niszczenie satelitów komunikacyjnych[169], systemów nawigacji satelitarnej np. GPS/GLONASS) czy w cyberprzestrzeni. Oznacza to, że efektywne wykorzystanie koncepcji A2/AD zapewnia przewagę w obronie i stanowi równocześnie wsparcie do rozpoczęcia oraz prowadzenia z powodzeniem lądowych działań zaczepnych na tych samych kierunkach.

Dla kontrastu warto również zapoznać się ze stanowiskiem niektórych amerykańskich ekspertów, którzy definiują termin A2/AD jako zbiór zdolności wykorzystywanych do zapobiegania lub ograniczania przeciwnikowi możliwości rozmieszczania swoich sił oraz swobody ich manewru na określonym obszarze[170]. Zwracają oni przy tym uwagę, że A2/AD jest wyzwaniem tylko dla komponentu powietrznego, który ma być odpowiedzialny za „rozwiązanie" tego problemu. Między innymi z tego powodu Marynarka Wojenna USA zaprzestała używania terminu A2/AD. Jak to wyjaśnił admirał John M. Richardson[171]: „Problem z A2/AD polega na tym, że koncepcja ta łączy strategię z taktyką w sposób, który lekceważy niemilitarne aspekty działań w ramach A2, minimalizuje rolę odstraszania oraz skupia się na analizach taktycznych, w jaki sposób systemy uzbrojenia przeciwnika będą działać"[172]. Ponadto admirał skrytykował koncepcję A2/AD w zakresie trzech głównych

[167] W opinii analityków amerykańskich nie każdy przeciwnik dysponuje znaczącymi możliwościami w zakresie A2, natomiast praktycznie każdy może w znaczący sposób utrudnić lub wręcz pozbawić swobody manewru. Przykładem może być sytuacja po przemieszczeniu sił koalicji do Afganistanu, gdzie nie spotkały się one ze znaczącym zagrożeniem w zakresie A2 (z wyjątkiem czynników dyplomatycznych i geograficznych). W zakresie AD natomiast napotkały szereg poważnych zagrożeń dla własnej swobody działania (np. powszechne użycie improwizowanych urządzeń wybuchowych). Przyp. aut.

[168] Okręt podwodny działający na dalekich rubieżach, realizując zadania kontroli morza i uniemożliwienia korzystania z akwenu w ramach AD, może tym samym utrudniać lub ograniczać siłom morskim przeciwnika dostęp do prowadzenia operacji połączonych w ramach A2. Przyp. aut.

[169] Pozyskiwane dane rozpoznawcze (nawet te ze źródeł otwartych) wskazują na dynamiczny rozwój tego typu środków, głównie w siłach zbrojnych Federacji Rosyjskiej. Przyp. aut.

[170] L. Simon, *Demysttifying the A2/AD Buzz, War on the Rocks*, 04.01.2017, pobrano z lokalizacji: https://warontherocks.com/ 2017/ 01/demystifying-the-a2ad-buzz/ [dostęp: 24.07.2021].

[171] Admirał John. M. Richardson od 18 września 2015 r. do sierpnia 2019 r. był szefem operacji morskich Marynarki Wojennej USA (ang. *Chief of Naval Operation* – CNO). Przyp. autora.

[172] Por. W. A. Perkins, *Component Integration Challenges presented by Advanced Layered Defence Systems (A2/AD)*, [w:] „The Three Swords Magazine", nr 33/2018, Stavanger 2018 oraz Sam LaGrone, *CNO*

kwestii. Po pierwsze zauważył, że z różnymi teatrami działań związane są różne wyzwania, a uniwersalna koncepcja, taka jak A2/AD, powoduje raczej zamieszanie, a nie przejrzystość[173]. Po drugie Richardson przypomniał, że w A2/AD nie ma nic nowego, gdyż rywalizacja wojskowa zawsze opierała się na uniemożliwieniu dostępu potencjalnemu przeciwnikowi oraz utrudnieniu mu przemieszczania się. Na koniec skupił się na koncepcji działań powstrzymujących, twierdząc, że są one zbyt często brane za fakt dokonany, gdy w rzeczywistości stanowią one raczej dążenie (aspirację).

4.2. Kluczowe elementy systemów antydostępowych

Myśląc o koncepcji antydostępowej, należy drobiazgowo rozpatrywać wzajemne zależności potrzeb i możliwości, technologii oraz ekonomii, które zadecydują o własnych zdolnościach A2/AD i możliwościach odstraszania oraz zwalczania sił przeciwnika. Takie myślenie pozwoli odpowiedzieć na pytanie, dlaczego przeciwdziałanie systemom A2/AD jest tak trudne do osiągnięcia i kosztowne. Analizując zagadnienia związane z tworzeniem zdolności antydostępowych, można dojść do wniosku, że głównym motywem jej rozwoju jest obawa przed użyciem siły przez potencjalnego przeciwnika. Drugim powodem może być chęć dokonania własnej projekcji siły w pobliżu swoich granic i powstrzymanie w ten sposób agresji. Obecnie podmioty dysponujące znacznym potencjałem ofensywnym (np. USA, Rosja, Chiny) muszą liczyć się z tym, że spodziewane koszty będą przewyższać spodziewane korzyści płynące z interwencji. Ryzyko to może wzrosnąć poprzez wzbronienie im łatwego dostępu i ograniczenie swobody działania. Paradoksalnie te dwie wspomniane motywacje nie wykluczają się[174]. Rozpatrując czynnik (słabe i mocne strony oraz szanse i zagrożenia) projekcji siły[175], w porównaniu z potencjałem i podstawowymi korzyściami płynącymi z prowadzenia działań antydostępowych, należy z wysokim prawdopodobieństwem przyjąć, że:

Richardson: Navy Shelving A2/AD Acronym, USNI News, 03.10.2016, pobrano z lokalizacji: https://news.usni.org/ 2016/10/03/cno-richardson-navy-shelving-a2ad-acronym [dostęp: 25.07.2021].

[173] W myśl tego Siły Zbrojne USA powinny pominąć koncepcje ogólne, takie jak A2/AD, a skoncentrować się na konkretnych strategiach i zdolnościach odpowiednich dla konkretnych przeciwników w kontekście uwarunkowań geograficznych, koncepcji oraz technologii. Przyp. aut.

[174] Należy zauważyć, że potencjalny napastnik może być podatny na zdolności, które, choć nie są A2/AD *per se*, są jednak częścią ogólnych zdolności odstraszania, z których A2/AD jest szczególnym typem. Międzykontynentalne pociski uzbrojone w broń jądrową, pociski konwencjonalne wystrzeliwane z okrętów podwodnych, sponsorowany przez państwo terroryzm, nieregularne działania wojenne i zdolności do działania cyberprzestrzeni, mogą być atrakcyjne dla wrogich państw w odstraszaniu lub reagowaniu na projekcje sił. Przyp. aut.

[175] Należy jednak przy tym pamiętać o jednoczesnym zachowaniu wysokiego poziomu ochrony i obrony własnego potencjału. Przyp. aut.

1) Siły przewidziane do użycia w operacji muszą zdobyć przewagę i kontrolować działania w sposób pozwalający im na utrzymanie swobody działania, tak aby finalnie odnieść zwycięstwo. W przeciwieństwie do tych założeń A2/AD wymaga potencjału wystarczającego do zwalczania lub powstrzymania ataku – wysiłek ten z założenia powinien być mniejszy.
2) Nowoczesne technologie potrzebne do lokalizowania (namierzania), śledzenia i kierowania nowoczesnych platform, takich jak okręty oraz samoloty, są coraz bardziej dostępne, stosunkowo tanie i łatwe do pozyskania.
3) Siły i środki A2/AD zwykle są rozmieszczane na obszarze należącym do obrońcy i na jego wodach terytorialnych[176] (ich zasięg wykrycia i rażenia środków przeciwnika jest wielokrotnie większy niż tylko własny obszar), podczas gdy działania ofensywne wymagają przemieszczania się platform (często na bardzo dużych dystansach) na bronionym obszarze. W związku z tym siły i środki zaangażowane w prowadzenie działań antydostępowych mają większą zdolność do absorpcji strat (uzupełniania) i wykorzystują do tego sieci wewnętrznych linii komunikacyjnych, a zarazem utrzymują lub łatwo przemieszczają siły na wyznaczone pozycje[177].
4) Prowadzenie działań *stricte* antydostępowych jest relatywnie „tańsze”[178] niż prowadzenie działań ofensywnych opartych na wysoko mobilnych platformach. Koszty systemów uzbrojenia wykorzystywanego w A2/AD wynoszą średnio niewielką część kosztów zwalczanych platform. Szczególnie mocno to widać na przykładzie kosztów jednostkowych pocisków rakietowych, których cena jest tylko ułamkiem sumy wydanej na zakup statku powietrznego lub okrętu, który te pociski może zniszczyć. Jak wskazują wyniki światowych badań, w przypadku działań ofensywnych ta niekorzystna sytuacja wzrasta. Koszty pozyskania coraz

[176] Pas wód morskich przyległych do wybrzeża lub wód wewnętrznych, stanowiących integralną część terytorium państwa. Zwykle to 12 mil morskich. Pobrano z lokalizacji: http://encyklopedia.pwn.pl/szukaj/wody terytorialne.html [dostęp: 20.09.2018].
[177] W wypadku działań sił Sojuszu (np. prowadzenie działań antyterrorystycznych lub wynikających z art. 5. traktatu) zarówno wojska operacyjne, jak i logistyka oraz platformy transportowe będą zwykle działać, jak pokazuje historia, z odległości od kilkuset do kilku tysięcy kilometrów (w wypadku operacji w Europie prowadzonych przez wojska amerykańskie) od baz zaopatrzeniowych lub głównych baz operacyjnych. Przyp. aut.
[178] Efekt ekonomiczny w tym wypadku należy rozumieć po pierwsze poprzez pryzmat finansowy zakupu środków walki, koszt ich utrzymania i wykorzystania oraz nieodwracalnego wykorzystania uzbrojenia, po drugie również poprzez koszt wysiłku, jaki należy włożyć w samo planowanie i prowadzenie działań przez sztaby wojskowe. Przyp. aut.

nowocześniejszych okrętów i samolotów rosną szybciej niż koszty defensywnych systemów antydostępowych. Ta tendencja jasno wyskazuje, dlaczego możliwości potencjalnego przeciwnika dysponującego środkami A2/AD stale rosną w stosunku do możliwości ofensywnego prowadzenia działań. Można to zauważyć, porównując koszty konkretnych systemów A2/AD i koszty środków projekcji siły, które mogą je pokonać (lub zneutralizować). Przy wyłączeniu użycia pocisków samosterujących przeciwko okrętom nawodnym (ponieważ przechyla to szalę jeszcze bardziej na korzyść A2/AD) średni ich koszt to około jednej piątej kosztu zdolności projekcji siły. W tabeli 4.1. zawarto szacunkowe koszty tego typu działań.

W związku z powyższym celowe jest stwierdzenie, że funkcjonalność systemów A2/AD polega głównie na sprzężeniu zdolności wykrywania, zakłócania elektronicznego systemów naprowadzających, orientacji przestrzennej i komunikacji oraz niszczenia środków przeciwnika, w tym samolotów, pocisków manewrujących, okrętów itp.

Tabela 4.1.
Porównanie kosztów poniesionych na środki projekcji siły z kosztami systemów antydostępowych

A2/AD		**Projekcja siły**		**Proporcje**	
Zdolność lub jednostka A2/AD	**Koszt w mln. USD**	**Zdolność lub jednostka projekcji siły**	**Koszt w mln USD**	**Zaangażowanie A2/AD:FP**	**Koszty A2/AD:FP**
Środki obrony powietrznej (SA-20)	1	samolot wielozadaniowy F-35	140	10:1	1:14
ASBM[179] (DF-21D)	11	lotniskowiec o napędzie nuklearnym, niszczyciel rakietowy	13 000 1 700	5:1	1:230 1:30
Pocisk manewrujący (C803)	1	lotniskowiec o napędzie nuklearnym, niszczyciel rakietowy	13 000 1 700	5:1	1:2 500 1:350
Okręt podwodny (Yuan)	500	lotniskowiec o napędzie nuklearnym, niszczyciel rakietowy	13 000 1 700	2:1	1:10 1:2
Myśliwiec zdolny do przenoszenia broni antysatelitarnej (ASAT)	20	satelita rozpoznawczy	3 000	2:1	1:75
Podstawowe rakiety balistyczne krótkiego zasięgu[180]	1	rakiety systemu Patriot	3	1:3	1:9

Źródło: opracowanie własne na podstawie: T.K. Kelly, D.C. Gompert, D. Long, *Smarter Power, Stronger Partners*, the RAND Corporation, Santa Monica, Calif., s. 91-92.

[179] Pocisk (ang. *anti-ship ballistic missile* – ASBM). Przyp. aut.
[180] *Short-Range Ballistic Missile* – SRBM (ang.). Przyp. aut.

Do kluczowych zdolności A2 (*anti-access*), szczególnie w zakresie dalekiego zasięgu, mających na celu zapobieganie przedostawaniu się siły przeciwnika na broniony obszar, zalicza się przede wszystkim:

- pociski balistyczne i manewrujące wystrzeliwane z powierzchni (ziemi, wody), powietrza i okrętów podwodnych, zdolne do precyzyjnego rażenia wysuniętych baz i rozmieszczonych sił oraz wspierającej ich logistyki na odległościach przekraczających 1 500 km;
- systemy rozpoznania i nadzoru dalekiego zasięgu, które zapewniają niezbędne informacje dotyczące celu, w tym satelity, samoloty oraz systemy radarowe;
- kinetyczną i niekinetyczną broń ASAT[181], która może unieszkodliwić systemy satelitarne niezbędne w realizacji projekcji siły;
- okręty podwodne, które są w stanie powstrzymywać przemieszczanie wojsk i stwarzać zagrożenie dla jednostek morskich zarówno na wodach terytorialnych, jak i międzynarodowych;
- działania w cyberprzestrzeni przewidziane między innymi do zakłócania systemów dowodzenia i kontroli oraz infrastruktury krytycznej, zarówno cywilnej, jak i wojskowej;

[181] Broń antysatelitarna – ASAT (ang. *Anti-satellite weapon*) broń służąca do zwalczania (uszkadzania bądź niszczenia) obiektów przeciwnika rozmieszczonych w kosmosie – zwłaszcza sztucznych satelitów. Zobacz szerzej: *Office of Technology Assessment: Ballistic Missile Defense Technologies,* University Press of Pacific, Honolulu 2002, s. 187. ASAT może być w pełnej gotowości operacyjnej nawet tuż po 2020 roku. Dyrektor Narodowego Wywiadu (*Director of National Intelligence*) Dan Coats w maju 2017 r. zwracał uwagę na zmianę doktryny rosyjskiej i chińskiej, która zakłada obecnie również atak przeprowadzony na cywilne i wojskowe systemy satelitarne. Obecnie zagrożone są przede wszystkim systemy satelitarne na niskiej orbicie okołoziemskiej (LEO), a więc satelity poruszające się w odległości od 180 km do 2 000 km (100 do 1 242 mil). Takich obiektów w 2016 r. było około 780 i należały one do 43 krajów. Pomiędzy nimi są głównie satelity obserwacji Ziemi, które zapewniają większość informacji potrzebnych wojskowym do przygotowania i realizowania operacji na całym świecie – zarówno w czasie kryzysu, jak i wojny. LEO są dodatkowo wykorzystywane przez satelity komunikacyjne i meteorologiczne (np. Iridium, Globalstar i Orbcomm). Należy zwrócić uwagę, że Rosjanie i Chińczycy działają przy tym dwutorowo. Pierwszym celem jest zbudowanie samego systemu ASAT, który dodatkowo byłby stosunkowo tani i łatwy w użyciu. Nie chodzi więc już tylko o spowodowanie wielkiego wybuchu jądrowego na wybranej wysokości orbitalnej. Po drugie Rosja i Chiny chcą wspólnie doprowadzić do wprowadzenia takich międzynarodowych porozumień, by ograniczyć Amerykanom możliwość bronienia się w kosmosie przed uzbrojeniem antysatelitarnym. Zagrożone chińskimi i rosyjskimi systemami uzbrojenia są również obiekty kosmiczne krążące na orbitach silnie eliptycznych HEO (*Highly Elliptical Orbits*) – czyli przede wszystkim wojskowe satelity łączności i rozpoznania strategicznego. Są one tylko pozornie bezpieczne, ponieważ poruszają się po elipsie. I o ile w apogeum (najdalej wysuniętym punktem orbity w odległości powyżej 35 786 km) znajdują się jeszcze poza zasięgiem systemów niszczących, to 37 satelitów HEO w perygeum (najbliżej położonym punkcie orbity – leżącym w odległości 500 – 1 000 km) wchodzi już w strefę rażenia uzbrojenia opracowywanego i podobno wdrażanego przez Chińczyków i Rosjan. Przyp. aut.

- działania terrorystyczne;
- siły specjalne zdolne do niekonwencjonalnych działań bojowych na podejściach do obszaru operacyjnego[182].

Należy zwrócić uwagę, że posiadanie ww. zdolności pozwoli na oddziaływanie na dużych obszarach, co oznacza, że nawet siły i środki znajdujące się w obszarach tyłowych mogą stać się celem ataku.

Do kluczowych zdolności AD (*area-denial*) o mniejszym zasięgu, mających na celu ograniczenie swobody działania w obszarze operacyjnym, należą:

- siły powietrzne oraz systemy obrony powietrznej, zarówno stacjonarne, jak i mobilne, zaprojektowane tak, by wzbraniać lokalnej przewagi powietrznej;
- rakietowe pociski przeciwokrętowe krótkiego zasięgu i okręty podwodne ograniczające działalność morską przeciwnika w konkretnym obszarze;
- rakiety, artyleria, pociski i moździerze przeznaczone do atakowania celów powierzchniowych;
- broń chemiczna i biologiczna wzbraniająca wykorzystania wybranych obszarów;
- komputerowe i elektroniczne ataki w celu zredukowania, zneutralizowania lub zniszczenia systemu C2 w obszarze operacyjnym;
- liczne lądowe pola i morskie zagrody minowe służące do szybkiego zamknięcia cieśnin morskich, przełęczy lądowych, długich odcinków linii brzegowej lub lotnisk;
- uzbrojone i wypełnione materiałami wybuchowymi małe łodzie i statki na wodach przybrzeżnych i w cieśninach morskich[183];
- manewrowe siły lądowe;
- siły specjalne zdolne do niekonwencjonalnych działań bojowych na podejściach do obszaru operacyjnego;
- systemy bezzałogowe, takie jak bezzałogowe statki powietrzne i bezzałogowe pojazdy podwodne, przeznaczone do gromadzenia danych wywiadowczych lub rażenia celów na określonym obszarze[184].

[182] Na podstawie *Joint Operational Access Concept (JOAC)*, dz. cyt., s. 18.
[183] Wody przybrzeżne obejmują obszar wód powierzchniowych od linii brzegu, których zewnętrzną granicę wyznacza odległość jednej mili morskiej po stronie w kierunku morza, licząc od linii podstawowej. Prawo wodne, Dz.U. 2017 poz 1566. Ustawa z dnia 20 lipca 2017 r.
[184] Na podstawie *Joint Operational Access Concept (JOAC)*, dz. cyt., s. 19.

Powyższe zdolności, dostępne niegdyś tylko dla mocarstw, stają się coraz łatwiej osiągalne dla wielu państw, a nawet dla podmiotów niepaństwowych. Niektóre podmioty będą mieć ograniczoną liczbę tych zdolności, a inne będą wdrażać w pełni zintegrowane i warstwowe zaawansowane systemy A2/AD obejmujące siły powietrzne, morskie, lądowe, kosmiczne i cybernetyczne sterowane przez pojedynczy system dowodzenia i kontroli oraz wzajemnie się wspierające.

4.3. Rosyjski system antydostępowy jako wyzwanie dla Polski i NATO

Po przeanalizowaniu doktryny wojskowej Federacji Rosyjskiej z 26 grudnia 2014 r. można dostrzec, że za jedno z najistotniejszych zagrożeń uznaje się zwiększanie potencjału militarnego państw NATO oraz zbliżanie ich infrastruktury wojskowej do rosyjskich granic. Duże zaniepokojenie budzi także stworzenie oraz rozwijanie systemów strategicznej obrony przeciwrakietowej przez państwa NATO, co wg Kremla narusza globalną stabilność oraz ukształtowany stosunek sił w sferze rakietowo-jądrowej. We wspomnianym dokumencie pokuszono się o określenie charakterystycznych cech i właściwości współczesnych konfliktów. Zaliczono do nich m.in.:

- kompleksowe wykorzystanie siły militarnej oraz politycznych, ekonomicznych, informacyjnych i innych środków o charakterze pozamilitarnym;
- zmasowane wykorzystanie systemów uzbrojenia oraz sprzętu wojskowego;
- wzmocnienie centralizacji i automatyzacji zarządzania wojskiem i uzbrojeniem;
- stworzenie na terytoriach skonfliktowanych stron stałej aktywnej strefy działań wojennych;
- udział w działaniach wojennych nieregularnych formacji zbrojnych oraz prywatnych formacji wojskowych;
- zastosowanie niebezpośrednich i asymetrycznych sposobów działania;
- wykorzystanie broni jądrowej jako czynnika odstraszania.

W związku z tak zdefiniowanymi zagrożeniami oraz właściwościami konfrontacji przyjęto, że polityka militarna Federacji Rosyjskiej będzie skierowana na zapobieganie konfliktom wojennym, doskonalenie organizacji oraz form i metod wykorzystania sił zbrojnych. Równie istotnym przedsięwzięciem będzie przeciwdziałanie próbom uzyskania przewagi militarnej poszczególnych państw (grup państw) poprzez tworzenie systemów strategicznej obrony antyrakietowej, wyniesienia broni do przestrzeni kosmicznej, rozwijania strategicznych konwencjonalnych systemów rodzajów broni precyzyjnego rażenia[185].

Rys. 4.1. Rosyjskie strefy A2/AD

Źródło: opracowanie własne na podstawie: M. Gawęda, *Rosyjskie bastiony A2/AD (analiza)*, Defence 24, 29.07.2018 r. [dostęp: 20.05.2023][186]. Mapę pobrano z openstreetmap.org

[185] Pobrano z lokalizacji: https://www.bbn.gov.pl/ftp/dok/01/DoktrynaFederacjiRosyjskiej.pdf, s. 5-11 [dostęp: 04.10.2021 r.].

[186] Dla określenia sił stacjonujących w poszczególnych rejonach wykorzystano: J. Ciślak, *Armia rosyjska – armia agresora: Wojsko w Obwodzie Kaliningradzkim [RAPORT]*, Defence24, 30.04.2022, pobrano z lokalizacji: https://defence24.pl/sily-zbrojne/armia-rosyjska-armia-agresora-wojsko-w-obwodzie-kaliningradzkim-raport [dostęp: 04.05.2022]; S. Wills, *Kaliningrad: Impregnable Fortress or „Russian Alamo"?*, CNA, 15.05.2023, pobrano z lokalizacji: https://www.cna.org/our-media/indepth/2023/05/kaliningrad-impregnable-fortress-or-russian-alamo [dostęp: 25.06.2023]; M. Dura, *Rosyjskie rakietowe baterie nadbrzeżne: do obrony i szantażu politycznego [KOMENTARZ]*, Defence24, 20.01.2022, pobrano z lokalizacji: https://defence24.pl/sily-zbrojne/rosyjskie-rakietowe-baterie-nadbrzezne-do-obrony-i-szantazu-politycznego-komentarz [dostęp: 04.05.2022], M. Boulègue, *Russia's Military Posture in the Arctic Managing Hard Power in a 'Low Tension' Environment*, Chatham House, czerwiec 2019, pobrano z lokalizacji: https://www.chathamhouse.org/sites/default/files/2019-06-28-Russia-Military-Arctic_0.pdf

Również szef Sztabu Generalnego SZ FR gen. armii Witalij Gierasimow przedstawił swoją wizję przyszłych konfliktów zbrojnych, określając je jako coraz bardziej dynamiczne, aktywne i efektywne wojskowe działania. Zgodnie z jego założeniami nowe technologie informacyjne pozwolą znacząco zmniejszyć przestrzenny, czasowy i informacyjny dystans między wojskiem a organami władzy. Co więcej, starcia wielkich zgrupowań wojsk na poziomie strategicznym i operacyjnym staną się przeszłością. Zasadniczym sposobem osiągnięcia celów walki stanie się bezkontaktowe oddziaływanie na przeciwnika na dużych odległościach[187].

Koncepcje, które zostały przedstawione zarówno w doktrynie wojskowej Federacji Rosyjskiej, jak również w wystąpieniu gen. Gierasimowa, zaczęto przekuwać w czyny. Należy także zwrócić uwagę, że w żadnym z powyższych nie znajdzie się terminu A2/AD czy też wyrażenia *systemy antydostępowe*. Jednak realne działania jak najbardziej wpisują się w ich definicję. Od pewnego czasu Federacja Rosyjska koncentruje siły i środki oraz rozbudowuje infrastrukturę wojskową w newralgicznych punktach swojej strefy wpływów[188], które mają zapewnić jej militarną lub polityczno-wojskową obecność w regionie, co zostało przedstawione na rysunku 4.1.

Z drugiej strony takie działania doskonale wpisują się w budowę zdolności do uniemożliwienia, a przynajmniej znacznego utrudnienia, siłom Sojuszu realizacji wsparcia państwom leżącym na wschodniej granicy NATO w przypadku rosyjskiej agresji. W szczególności zwraca się uwagę na rozmieszczenie i skoncentrowanie rosyjskich systemów obrony powietrznej (systemy S-400, S-300) i przeciwokrętowej (systemy Bastion-P), rakiet balistycznych (Iskander) i pocisków manewrujących, a także środków walki radioelektronicznej (np. Krasucha, Murmańsk-BN) i działań w cyberprzestrzeni[189]. Zasięgi tych środków rażenia zostały przedstawione na rysunku 4.2.

[dostęp: 04.05.2022]; C. Wall, N. Wegge, *The Russian Arctic Threat. Consequences of the Ukrainian War*, CSIS, styczeń 2023, pobrano z lokalizacji: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230125_Wall_RussianArcticThreat_0.pdf?VersionId=e8h73TdoOUjdJO3Y4nOTc4 [dostęp: 21.02.2023].

[187] Wystąpienie szefa SG SZ FR z 26 stycznia 2013 roku do członków rosyjskiej Akademii Nauk Wojskowych na posiedzeniu podsumowującym prace Akademii w 2012 roku. Przyp. aut.

[188] Warto zwrócić uwagę, że około 2/3 posiadanych zasobów niektórych środków rakietowych mogło zostać wykorzystanych w walkach w Ukrainie. Por. Focus 2023, *The Norwegian Intelligence Service's assessment of current security challenges*, Norwegian Intelligence Service, Oslo 2023.

[189] Już w czasie zimnej wojny Związek Radziecki planował użycie pocisków rakietowych wystrzeliwanych z powietrza i okrętów, aby utrzymać zachodnie lotniskowce z dala od przyległych wód i budował tak zwane bastiony, aby chronić swoje bazy morskie i strategiczne okręty podwodne (na podstawie M. Vego, *Soviet Naval Tactics*, Naval Institute Press, Annapolis, 1992, Ch. 1, 20.

Rys. 4.2. Zasięgi rosyjskich systemów A2/AD

Źródło: Opracowanie własne na podstawie: B. Perry, *Entering the Bear's Lair: Russia's A2/AD Bubble in the Baltic Sea*, The National Interest, 20 September 2016 [dostęp: 09.10.2021]. Mapę pobrano z openstreetmap.org

4.4. System antydostępowy Chińskiej Republiki Ludowej w kontekście bezpieczeństwa globalnego

Zdaniem wielu ekspertów naturalnym kierunkiem ekspansji dla Chin jest obszar Azji Południowo-Wschodniej, w którym wzmacniają swoją rangę, a jednocześnie obniżają pozycję USA. To rozszerzanie własnych wpływów napotyka jednak szereg barier, do których m.in. należą wzajemne roszczenia Chin, Tajwanu, Filipin, Wietnamu, Malezji i Brunei o zlokalizowane na Morzu Południowochińskim (tzw. linia dziewięciu kresek[190]) Wyspy Paracelskie, Spratly[191] i inne[192]. Co więcej, priorytetem wydaje się utrzymanie obecnego systemu rządów i zachowanie integralności terytorialnej państwa. Jako główne

[190] *Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*, U.S. Department of Defense, Waszyngton 2019, s. 8.
[191] Zajęcie przez Chiny spornych Wysp Spratly i innych wysp umożliwiło im stworzenie swoistych „stacjonarnych lotniskowców" i militarne wzmocnienie ich roszczeń do całego Morza Południowochińskiego (por. R. Sawyer, *Chinese Strategic Power: Myths, Intent, and Projections*, [w:] „Journal of Military and Strategic Studies", vol. 9, nr 2, 1 styczeń 2007, s. 21).
[192] Por. Ł. Jureńczyk, *Polityczno-wojskowy wymiar rywalizacji między Chińską Republiką Ludową a Stanami Zjednoczonymi Ameryki w XX i XXI wieku,* „Annales, Sectio K. Politologia" 2017, vol. 24, nr 2, s. 19-20.

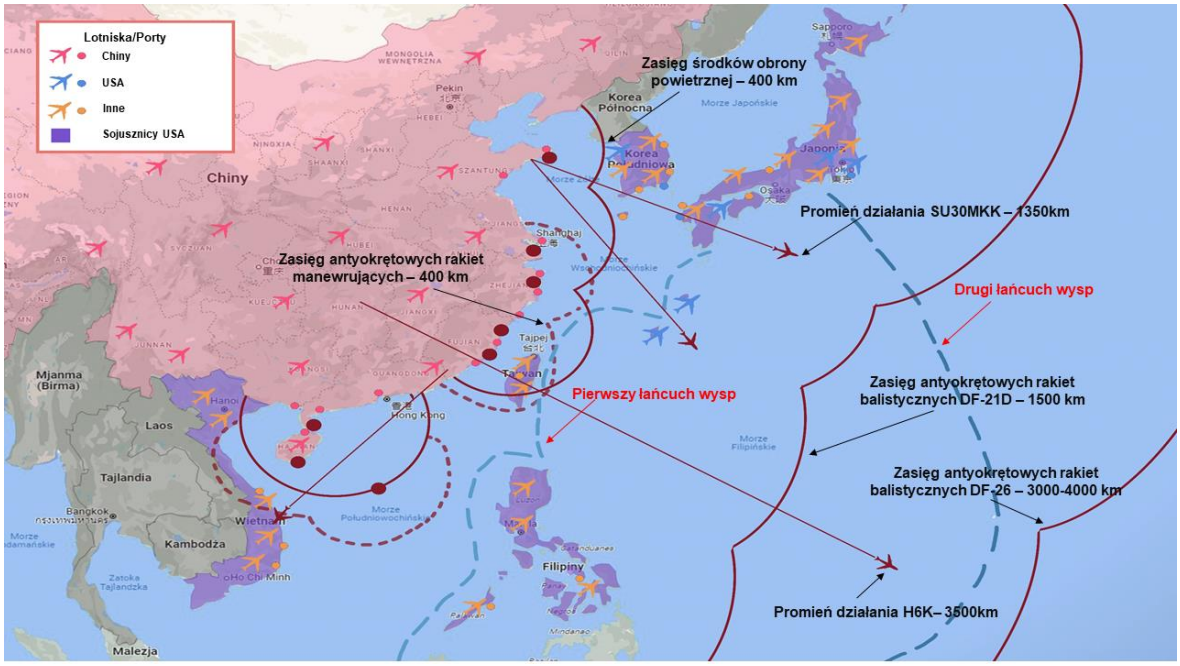
zagrożenie identyfikowane są wszelkie tendencje o charakterze odśrodkowym i autonomicznym. Wśród nich za szczególnie niebezpieczne uważane są wszelkie ruchy prodemokratyczne oraz istnienie na mapie świata Tajwanu jako niezależnego państwa.

W lipcu 2019 r. Chiny opublikowały kolejną białą księgę o polityce obronnej jako swoistą odpowiedź na podobne roszczenia i rosnące zaangażowanie Stanów Zjednoczonych w Azji i ich politykę wobec ChRL. W dokumencie tym można się doszukać prób zmiany własnego wizerunku, pokazania pokojowych zamiarów i określenia granic, których przekroczenie spotka się ze zdecydowaną reakcją państwa. W przedmiotowej publikacji jako główne zagrożenie definiuje się postępującą rywalizację mocarstw, której głównym sprawcą są Stany Zjednoczone. Ponadto wskazuje się na zagrożenia związane z naruszaniem ich kluczowych interesów, które choć niezdefiniowane, to z kontekstu można wywnioskować, że dotyczą Tajwanu, Hongkongu, Makau, Tybetu, Sinkiangu oraz spornych obszarów na Morzu Południowo- i Wschodniochińskim[193]. Dla zniwelowania tych zagrożeń rozwijane są kompleksowe zdolności Chińskiej Armii Ludowo-Wyzwoleńczej[194] (ChALW), w tym tzw. strategii aktywnej obrony, zgodnie z którą budowane są zdolności do odstraszania, odpierania, zakłócania i opóźniania rozmieszczenia sił USA[195], graficznie zobrazowanych na rysunku 4.3.

Chiny rozwijają potencjał skoncentrowany na koncepcji przeciwstawienia się interwencji opartej na zintegrowanym użyciu środków rakietowych, powietrznych oraz okrętów, w wielu przypadkach wykorzystując sztucznie zbudowane wyspy[196]. Intencją tej koncepcji jest przede wszystkim odstraszenie przeciwnika, a w dalszej kolejności obniżenie jego zdolności do dalszego prowadzenia działań. Biorąc pod uwagę odległość dzielącą dwóch głównych antagonistów, można stwierdzić, że prowadzenie działań zgodnie z tą koncepcją (nazywaną czasem koncepcją kontrinterwencji) spowoduje zwiększenie kosztów interwencji ze strony Stanów Zjednoczonych. Ponadto amerykańscy analitycy zwracają uwagę na fakt posiadania przez ChALW zdolności do szybkiego przejęcia inicjatywy

[193] J. Szczudlik, *„Nowa era" w polityce obronnej Chin*, [w:] „Biuletyn PISM", nr 122 (1870), Warszawa 2019.
[194] Por. T. Smura, *Modernizacja Chińskiej Armii Ludowo-Wyzwoleńczej*, [w:] „Pułaski Policy Paper", nr 3, 24.03.2021, Warszawa 2021.
[195] Dla osiągnięcia tych celów wykorzystuje się słabości USA – odległość od Chin oraz wrażliwość społeczną. Pierwsza kwestia ma ogromne znaczenie przy przerzucie wojsk w rejon działań, druga zaś dotyczy awersji opinii publicznej do ponoszenia masowych ofiar i szeroko pojętych negatywnych rozstrzygnięć. Przyp. autora.
[196] Aby przeciwdziałać takiemu potencjałowi, planuje się zwiększenie inwestycji w zintegrowane systemy obrony przeciwlotniczej i przeciwrakietowej (por. See Sam LaGrone, *Pacific Commander Davidson Asks Congress to Fund 'Regain the Advantage' Plan Aimed at China*, USNI News, 18.04.2019, pobrano z lokalizacji: https://news.usni.org/2019/04/18/pacific-commander-davidson-asks-congress-to-fund-regain-the-advantage-plan-aimed-at-china [dostęp: 14.11.2021].

i wykonania uderzenia na siły przeciwnika z dystansu w celu uzyskania pewności, że przeciwnik nie będzie w stanie przeszkodzić im w osiągnięciu swoich celów[197]. Należy zauważyć, że choć władze Chin nigdy oficjalnie nie potwierdziły istnienia takiej koncepcji, to jej założenia sprawiają, że można określić ją mianem A2/AD.



Rys. 4.3. Chińskie zdolności A2/AD

Źródło: opracowanie własne na podstawie: B. Köylüoğlu, *Modern Dunyanin Jeopolitik Faylari*, https://www.stratejivefinans.com/modern-dunyanin-jeopolitik-faylari/, 18.04.2021 [dostęp: 30.12.2021]. Mapę pobrano z openstreetmap.org

Chińską strategię antydostępową można scharakteryzować jako cztery powiązane filary[198]:

1) geograficzny – zwiększanie dystansu i czasu niezbędnego na dotarcie przeciwnika do teatru działań oraz jednoczesne stworzenie maksymalnego zagrożenia, a także osiągnięcie w tym czasie własnych celów militarnych i politycznych;
2) kinetyczny – obniżanie zdolności penetracyjnych przeciwnika oraz jednoczesne zwiększanie własnych zdolności uderzeniowych;

[197] *PLA Aerospace Power: A primer on trends in China's Military Air, Space, and Missile Forces*, US Air University, Montgomery 2017, s. 7.
[198] Zobacz szerzej: O. S. Mastro *China Anti-access/Area Denial (A2AD) Capabilities: Is the U.S. Rebalancing Enough?* [w:] W. H. Natter, J. Brooks, *American Strategy and Purpose: Reflections on Foreign Policy and National Security in an Era of Change*, Createspace Independent Publishing Platform, 2014, s. 118-140.

3) polityczny – wykorzystywanie presji politycznej, militarnej i ekonomicznej w dążeniu do osłabienia sojuszy i paktów przeciwnika oraz rozszerzania swoich wpływów[199];
4) odstraszania – działania zastraszające czyniące zaangażowanie przeciwnika zbyt kosztownym, co skutkuje jego wycofaniem lub ograniczeniem działań.

Próbując scharakteryzować strategię A2/AD zgodnie z definicją obowiązującą w NATO, działania ChRL zmierzające do przeciwdziałania dostępowi (A2) polegają na opóźnianiu tranzytu, dotarcia i rozmieszczenia sił przeciwnika na teatrze działań oraz na utrzymywaniu ich w dystansie od newralgicznych pozycji, lub ich operowaniu w dużej odległości od rejonu działań. Dla przykładu efekt taki można osiągnąć, stosując zaawansowane uzbrojenie antysatelitarne i cyberataki, skutkujące wyłączeniem lub zakłóceniem działania sieci komunikacyjnych będących fundamentem świadomości sytuacyjnej, mobilności i skutecznego rażenia przez siły ekspedycyjne USA. Z kolei przedmiotem pozbawienia swobody działania (AD) przez ChALW ma być szeroko pojęte zakłócanie zmierzające do zmuszenia przeciwnika do pożądanych zachowań poprzez spowodowanie poważnych ograniczeń w swobodzie działania. Taki cel Chiny mogą osiągnąć poprzez zastosowanie zintegrowanej obrony rakietowej, okrętów podwodnych czy szybkich okrętów patrolowych zdolnych do zadania znaczących strat amerykańskim siłom operującym w obrębie pierwszego łańcucha wysp[200].

4.5. Konkluzje

Idea tworzenia systemów czy też stref, które utrudniałyby lub wręcz uniemożliwiały dostęp do bronionego obszaru, było istotnym elementem sztuki wojennej już od niepamiętnych czasów. Umiejętność właściwego wykorzystania warunków geograficznych, posiadanych środków, potencjału intelektualnego, ekonomicznego itp. pozwalała na prowadzenie skutecznej obrony własnego terytorium, ale również na bezpieczne przeprowadzenie koncentracji własnych wojsk w celu przygotowania ich do działań ofensywnych i zdobycia terenu przeciwnika. Można stwierdzić, że takie wykorzystanie

[199] Por. A. Chatzky, J. McBride, *China's Massive Belt and Road Initiative*, Council on Foreign Relations. January 28, 2020 [dostęp: 24.11.2021].
[200] Pierwszy łańcuch wysp tworzą Kuryle, Wyspy Japońskie, Tajwan, Filipiny i zachodni brzeg Borneo. Wyznaczony w ten sposób obszar obejmuje akweny bezpośrednio przylegające do chińskich wybrzeży, na których położone są sporne archipelagi Senaku, Spratly i Paracele. Por. P. Behrendt, *Chińska flota zielonych wód*, Nowa Konfederacja, 06.06.2017, pobrano z lokalizacji: http://www.nowakonfederacja.pl/chinska-flota-zielonych-wod [dostęp: 21.10.2021].

posiadanego potencjału było naczelną zasadą prowadzenia działań wojennych. Dlatego współczesna koncepcja A2/AD nie jest swoistym *novum*, ale stanowi rozwinięcie dotychczas stosowanych zasad z wykorzystaniem nowoczesnej technologii.

Przytoczone wyżej przykłady sposobów budowania zdolności A2/AD, zarówno przez Rosję, jak i Chiny, mają wiele cech wspólnych, np. systemy uzbrojenia, koncepcja ich użycia itp. Analizując założenia doktrynalne, będące podstawą realizacji koncepcji antydostępowej, można pokusić się o wyspecyfikowanie pewnych różnic. Rosyjskie systemy uniemożliwiające wtargnięcie w głąb terytorium kraju były rozwijane wokół jego granic już w czasach Związku Radzieckiego[201]. Rosyjska koncepcja w dalszym ciągu ma na celu zapewnienie obrony własnego terytorium oraz uniemożliwienie (utrudnienie) przeciwnikowi przekroczenia granic. Nową ideą jest stworzenie warunków do projekcji siły, zakłócenia przemieszczenia się sił wsparcia Sojuszu (w przypadku ataku Rosji), a także ograniczenie lub zablokowanie dostępu do portów bałtyckich. Z kolei Chiny rozbudowują swój potencjał antydostępowy przede wszystkim jako swoiste zabezpieczenie swoich interesów politycznych i gospodarczych. Gospodarka skoncentrowana na eksporcie, a uzależniona od importu surowców, opiera się przede wszystkim na swobodnym korzystaniu z dróg morskich. Dlatego też niezmiernie istotna jest stała obecność Chin w Azji Południowo-Wschodniej. Chińska koncepcja opiera się na wykorzystaniu wyspecjalizowanych środków militarnych skoncentrowanych w wybranych rejonach (np. sztuczne wyspy) pozwalających na izolowanie i utrzymywanie potencjalnych sił morskich przeciwnika (w zamyśle sił amerykańskich) na dużych odległościach od ich kontynentalnych granic[202].

Zwraca się uwagę, że po aneksji Krymu przez Rosję społeczeństwa zachodnie zostały wręcz zasypane informacjami o możliwościach rosyjskich systemów rakietowych, ich rozmieszczeniu w strefach tworzących swoiste obszary zakazu rzędu 400 km od Kaliningradu lub wysp na Bałtyku, a tym samym odcięcia tego regionu od zachodnich samolotów i okrętów[203]. Działania wojenne w Ukrainie w zasadzie potwierdziły te zamiary. Nie można jednak rozpatrywać efektywności tych systemów na podstawie działań na

[201] Porównując elementy rozwinięte w ramach systemu obrony powietrznej ZSRR z obecnymi bastionami (bańkami) A2/AD można zauważyć, że ich lokalizacja jest bardzo podobna. Przyp. aut.
[202] Por. S. Permal, *China's Military Capability and Anti-access Area-denial Operations*, [w:] „Maritime Affairs: Journal of the National Maritime Foundation of India", vol. 10, 2014, issue 2, London 2014.
[203] R. Dalsjö, C. Berglund, M. Jonsson, *Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, Swedish Defence Research Agency FOI, March 2019, s. 10-18.

terenach Ukrainy, gdyż np. wykorzystywane są systemy obrony powietrznej głównie te z poziomu taktycznego i operacyjnego i służą one przede wszystkim do osłony wojsk, stanowisk dowodzenia czy urządzeń logistycznych. W tym przypadku nie można mówić o działaniach antydostępowych. Są to zwykłe rutynowe działania zapewniające osłonę przed uderzeniami z powietrza. Niewątpliwie zarówno Rosja, jak i Chiny (a także np. Iran, Izrael) opracowują i wdrażają do użytku nowe systemy broni dalekiego zasięgu. Faktem jest również, że stanowią one wyzwanie dla sił NATO oraz USA w przypadku konfliktu zbrojnego. Z drugiej strony nie jest to nic nowego. Każde państwo podejmuje (a przynajmniej powinno podejmować) przedsięwzięcia mające na celu zapewnienie bezpieczeństwa sobie i swoim obywatelom. Wydaje się, że trwająca cały czas dyskusja na temat A2/AD jest w równym stopniu odzwierciedleniem dwóch dekad zaniedbania rozwoju realnego i wysokiej klasy potencjału wojskowego w ramach NATO (jak również Unii Europejskiej czy też USA) przeciwko zaawansowanym przeciwnikom państwowym. Przez ostatnie lata członkowie NATO prowadzili przede wszystkim ekspedycyjne działania antyterrorystyczne, przeciwrebelianckie czy operacje reagowania kryzysowego. Obecne działania Rosji oraz Chin powodują, że konieczne stało się wypracowanie nowego spojrzenia odnoszącego się do czasowych, przestrzennych, funkcjonalnych i strukturalnych aspektów podejścia Sojuszu do rozwoju sztuki wojennej i prowadzenia działań zbrojnych[204].

Powszechnie uważa się, że dopatrywanie się zagrożenia ze strony systemów A2/AD dla swobody działania NATO, jest przesadzone. Zarówno analizy techniczne („krzywizna" Ziemi, „horyzont" radarowy, realny zasięg efektorów itp.), jak i doświadczenia bojowe z działań w Syrii oraz Ukrainy wskazują, że ich efektywność jest stosunkowo niewielka w walce z celami ruchomymi, natomiast są one skuteczne w zwalczaniu celów stałych[205]. Z drugiej strony należy być świadomym, że istnieje (lub może zostać opracowany) szereg środków skutecznie przeciwdziałających systemom antydostępowym[206].

---

[204] W ramach Sojuszu opracowywanych jest aktualnie kilka koncepcji z tego obszaru m.in. *Concept for the Deterrence and Defence of the Euro-Atlantic Area* (DDA) czy też *NATO Warfighting Capstone Concept* (NWCC). Por. *NATO Warfighting Capstone Concept (NWCC)*, ACT, Norfolk 2023, s. 2-12; *NATO's Concept for the Deterrence and Defence in the Euro-Atlantic Area Reaffirmed*, OPS, 21.10.2021, pobrano z lokalizacji: https://operationnels.com/ 2021/10/21/natos-concept-for-deterrence-and-defence-in-the-euro-atlantic-area-reaffirmed/ [dostęp: 04.01.2022].

[205] R. Dalsjö, C. Berglund, M. Jonsson, *Bursting*…, dz,. cyt., s. 80-93; K. Giles, M. Boulegue, *Russia's A2/AD Capabilities: Real and Imagined*, The US Army War College Quarterly, vol. 49, nr 1-2 Spring-Summer 2019, s. 21-36 oraz S. G. Jones, *Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare*, CSIS Briefs, 1 June, 2022, pobrano z lokalizacji: https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare) [dostęp: 20.09.2022].

[206] Potwierdzeniem tej tezy mogą być wnioski z ćwiczeń czy też gier wojennych. Por. E. Schmitt, *US Lending Support to Baltic States Fearing Russia*, The New York Times, 01.01.2017, pobrano z lokalizacji:

Z punktu widzenia interesów narodowych Polski zasadne wydaje się rozważenie rozwinięcia zintegrowanego systemu antydostępowego z uwagi na fakt, że konieczność pokonania takiego systemu stwarza możliwości opóźnienia działań przeciwnika i zyskania czasu na przybycie sił sojuszniczych. Z drugiej strony, biorąc pod uwagę środki wykorzystywane obecnie zarówno przez Rosję, jak i Chiny, należy mieć świadomość, że budowa takiego systemu jest czasochłonna oraz wiąże się ze sporymi kosztami.

https://www.nytimes.com/2017/01/01/us/politics/us-baltic-russia.html) [dostęp: 25.04.2022] oraz *337. No Option is Excluded – Using Wargaming to Envision a Chinese Assault on Taiwan*, TRADOC, 1.07.2021, pobrano z lokalizacji: https://madsciblog.tradoc.army.mil/337-no-option-is-excluded-using-wargaming-to-envision-a-chinese-assault-on-taiwan/ [dostęp: 30.12.2021].

ROZDZIAŁ V

KONCEPCJA NARODOWEGO SYSTEMU ANTYDOSTĘPOWEGO

Rozważając zasadność budowy narodowego systemu antydostępowego, należy zwrócić uwagę na jego umiejscowienie jako elementu wzmacniającego odporność państwa. Biorąc pod uwagę wskazane w rozdziale III czynniki określające i diagnozujące odporność państwa, można stwierdzić, że w Polsce istnieje szereg wyzwań w obszarze zwiększenia odporności. Konieczność jej budowy i w dalszej kolejności wzmacniania w siedmiu obszarach wyspecyfikowanych w czasie szczytu NATO w 2016 r. prowadzi do konkluzji, że rozbudowany system antydostępowy może być czynnikiem wpływającym na wzmacnianie odporności państwa. Zapewnienie funkcjonowania infrastruktury krytycznej czy też swobody przemieszczania się ludności i wojsk ma w konsekwencji istotny wpływ na ciągłość sprawowania władzy państwowej, ale też sprawne dowodzenie siłami zbrojnymi. Tworząc zatem zręby systemu antydostępowego, należy zwrócić uwagę na jego oddziaływanie na wzmacnianie systemu odpornościowego państwa. Najlepszym sposobem na zapewnienie ciągłości funkcjonowania w wyżej wymienionych obszarach jest uniemożliwienie lub utrudnienie przeciwnikowi ich degradacji. Biorąc z kolei pod uwagę zaproponowane cechy odpornego państwa, należy wskazać przynajmniej dwa, do których należą: zagwarantowanie bezpieczeństwa przepływów strategicznych oraz sprawny, systematycznie rozwijany i testowany narodowy system obrony, w tym zapewniony dostęp do infrastruktury krytycznej. Te właściwości mogą być zapewnione poprzez właściwie rozwinięty system antydostępowy. W niniejszym rozdziale zostanie podjęta próba określenia specyfikacji takiego systemu oraz przedstawiona koncepcja[207] jego rozwinięcia w naszym kraju.

5.1. Potrzeba budowy systemu antydostępowego w Polsce

Konfrontacyjna polityka Rosji zmierzająca do ustanowienia nowego porządku światowego, a w tym prowadzenie działań wojennych w Ukrainie, sprawia, że istotnym problemem staje się rozbudowa zdolności pozwalających Polsce na utrzymanie oraz

[207] Koncepcja – pomysł lub idea, zwykle określone w dokumencie zapewniającym wytyczne, wskazówki zorientowane na propozycje rozwiązania w odniesieniu do zidentyfikowanego braku lub luki w posiadanych zdolnościach. Koncepcja identyfikuje potrzebę oraz wskazuje kto, gdzie, kiedy i w jaki sposób może zaimplementować proponowane rozwiązanie. Opracowano na podst. *NATO CD&E Handbook*, Edition 2, ACT, February 2021.

podnoszenie poziomu odporności. Należy stwierdzić, że pierwszymi obiektami uderzeń w czasie działań wojennych będą m.in. centra decyzyjne oraz niektóre obiekty infrastruktury krytycznej. Zakłada się, że w pierwszej kolejności użyte zostaną środki rakietowe wystrzeliwane zarówno z platform powietrznych, jak i lądowych, morskich, ale również z przestrzeni kosmicznej. Należy się również spodziewać silnego oddziaływania w cyberprzestrzeni[208]. Celem tych działań będzie m.in. uzyskanie panowania w powietrzu, umożliwienie swobody manewru własnym wojskom oraz złamanie woli obrońców. Cechą współczesnych konfliktów jest także dążenie do jak najszybszego ich zakończenia. Im dłuższy czas ich trwania, tym większym wyzwaniom muszą stawić czoła obie strony (presja środowiska międzynarodowego, potencjalne sankcje gospodarcze, straty ludzkie, możliwość włączenia się w konflikt kolejnego gracza). Dlatego też należy spodziewać się zmasowanego kinetycznego uderzenia na wybrane cele, zniszczenie lub wyeliminowanie polskich sił zbrojnych, infrastruktury wojskowej (w tym infrastruktury krajowego przemysłu obronnego czy też stworzenie warunków uniemożliwiających uzyskania wsparcia ze strony NATO.

Zdaniem wielu analityków należy przypuszczać, że Rosja będzie w dalszym ciągu dążyła do ustanowienia nowego porządku światowego. W tym kontekście niezwykle istotny jest dalszy rozwój sytuacji w Ukrainie i stopień osiągnięcia przez Rosję swoich celów polityczno-wojskowych. Pozwoli to na dalsze kwestionowanie dotychczasowego porządku, wysuwanie kolejnych żądań, a w konsekwencji doprowadzenie do konfrontacji z NATO. Należy zwrócić uwagę na fakt, że jednym z kolejnych (po Ukrainie) celów FR może być Polska.

Trzeba również zaznaczyć, że podejmowane są działania mające na celu zwiększenie poziomu bezpieczeństwa Polski oraz jej potencjału militarnego[209]. Wszelka aktywność na tym polu, o ile będzie realizowana we właściwy sposób, z całą pewnością posłuży także do zwiększenia odporności Polski.

Po przeanalizowaniu ostatnich konfliktów, prowadzonych ćwiczeń przez wojska FR, a przede wszystkim obecnych działań wojennych w Ukrainie, należy jasno stwierdzić, że uzyskanie powodzenia przez przeciwnika będzie zależało od kilku czynników, zarówno

[208] Warto także zwrócić uwagę na fakt, że szereg działań oddziałujących na sferę kognitywną będzie realizowanych na długo przed pełnoskalowym konfliktem. Przyp. aut.
[209] Przykładem może być ustawa o obronie Ojczyzny, ale także działania mające na celu uniezależnienie się od dostaw paliw kopalnych z Rosji. Przyp. aut.

materialnych, jak i niematerialnych. Do czynników materialnych warunkujących powodzenie Rosji można zaliczyć:

- zadanie strat SZ RP do poziomu uniemożliwiającego im prowadzenie skutecznej obrony, szybkie rozbicie tych sił, ich okrążanie i izolowanie;
- przerwanie łańcucha dostaw z pomocą humanitarną i zaopatrzenia logistycznego do podtrzymywania działań oraz uniemożliwienie przybycia na teatr działań wojskom Sojuszu;
- zniszczenie elementów infrastruktury krytycznej;
- prowadzenie ataków na ludność cywilną.

Z kolei wśród czynników niematerialnych można wskazać:

- złamanie ducha (woli) obrońców;
- ustanowienie alternatywnych władz popierających najeźdźców;
- rozbicie jedności członków Sojuszu;
- utratę poparcia światowej opinii publicznej oraz wsparcia ich rządów;
- nieskuteczność sankcji ekonomicznych.

Określając poszczególne elementy, należy rozpocząć od możliwości rozbicia Sił Zbrojnych RP w pierwszych dniach konfliktu. Wykonując zmasowane uderzenie na elementy ugrupowania bojowego wojsk polskich i wprowadzając swoje siły, przeciwnik może uzyskać powodzenie na wybranych kierunkach, otoczyć i izolować nasze wojska. Należy przy tym zwrócić uwagę, że w obecnej sytuacji geopolitycznej przeciwnik może wykonać uderzenia z terytorium Białorusi (Brama Brzeska) oraz Obwodu Królewieckiego (dawniej Kaliningradzkiego). Co więcej, niepewna (jak na razie) sytuacja w Ukrainie może stworzyć dylemat strategiczny związany z możliwością wykorzystania jej terytorium do wprowadzenia wojsk rosyjskich (Brama Przemyska). W sytuacji, gdyby Ukraina stała się w pełni zależna od Moskwy, należałoby zapewnić rozpoznanie, obronę oraz rozśrodkowanie sił na granicy o długości niemal 1 170 km[210].

Z kolei groźba przerwania łańcucha dostaw zarówno z pomocą humanitarną, jak i zaopatrzenia logistycznego do podtrzymywania działań wymaga zapewnienia bezpieczeństwa przede wszystkim w domenie lądowej, powietrznej oraz morskiej.

[210] Zewnętrzna granica Unii Europejskiej na terenie Polski liczy 1 163 km, co stanowi 33% długości granicy państwowej RP. Najdłuższy odcinek przypada na granicę z Ukrainą – 535 km (tj. 46%), nieco mniejszy z Białorusią – 418 km (tj. 35,9%) i najmniejszy z Rosją (obwodem kaliningradzkim) – 210 km (tj. 18,1%). Por. *Charakterystyka obszarów przygranicznych przy zewnętrznej granicy Unii Europejskiej na terenie Polski, Podmioty Gospodarki Narodowej w 2015 r.*, opracowanie sygnalne, Główny Urząd Statystyczny, Warszawa 2016, s. 1.

Z dotychczasowych doświadczeń z działań w Ukrainie wynika, że przerwanie ciągłości dostaw zaopatrzenia na każdym z poziomów (strategicznym, operacyjnym czy taktycznym) może doprowadzić do przegranej. Zatem jednym z najistotniejszych obiektów do osłony stają się lotniska oraz porty przeładunkowe. Nie można też zapominać o ważnych węzłach drogowych i kolejowych.

Funkcjonowanie elementów infrastruktury krytycznej jest jednym z najistotniejszych wyzwań stojących przed powołanymi do tego organami ze względu na kluczową ich rolę w funkcjonowaniu państwa i życiu jego obywateli. Poprzez jej zniszczenie, uszkodzenie lub zakłócenie wpływa się na życie, morale i mienie obywateli oraz na rozwój gospodarczy państwa. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów dla państwa polskiego. Istota zadań związanych z infrastrukturą krytyczną sprowadza się nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki[211]. Biorąc pod uwagę wnioski płynące z dotychczasowych działań w Ukrainie, można z dużą dozą pewności stwierdzić, że niszczenie elementów infrastruktury krytycznej będzie jednym z głównych celów przeciwnika. Będzie on w ten sposób dążył przede wszystkim do złamania woli dalszej walki wśród obrońców i reszty społeczeństwa, aby wywołać pożądaną przez przeciwnika presję na władze państwowe.

Prowadzenie ataków na ludność cywilną, chociaż traktowane jako zbrodnia wojenna, jest niestety ciągle jednym ze sposobów prowadzenia działań wojennych przez Federację Rosyjską, który nie zmienił się przez lata. Należy zdawać sobie sprawę, że w dalszym ciągu ludność cywilna będzie jednym z najbardziej podatnych na uderzenia elementów państwa. Warto uświadomić sobie, że mimo wszystkich ewentualnych przedsięwzięć związanych z rozbudową systemów obronnych nie będzie możliwości bezpośredniej ochrony ludności w każdym miejscu i w każdym czasie. Odpowiednio skonstruowany system antydostępowy może jednak w sposób pośredni wpłynąć na zwiększenie jej szans przetrwania.

Z kolei oddziaływanie na sferę kognitywną będzie z całą pewnością realizowane na długo przed wybuchem konfliktu zbrojnego, jak również w jego trakcie[212]. Celem tych

[211] Por. *Systemy infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, pobrano z lokalizacji: https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej [dostęp: 12.12.2022].
[212] Zob. R. Reczkowski, A. Lis, *Cognitive Warfare: what is our actual knowledge and how to build state resilience?* [w:] *The Total Defence 21st Century.com – Building a Resilient Society: Theory and Practice Journal*, red. M. Lasoń, M. Klisz, L. Elak, nr 3/2022, Wyd. Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2022, s. 51-61.

działań będzie przede wszystkim wywieranie wpływu na postawę ludności kraju (wpływ nie tylko na to jak ludzie myślą, ale i działają), a także zmiana nastawienia wśród władz i opinii społecznej innych państw. Dlatego też jednym z głównych obszarów, w którym będą prowadzone działania mające na celu kształtowanie odpowiednich (z punktu widzenia przeciwnika) postaw obywateli i władz, będzie cyberprzestrzeń.

5.2. Ogólne założenia systemu

Utrzymanie pożądanego poziomu bezpieczeństwa, a w tym odporności, nie jest stanem samym w sobie, ale ciągłym procesem realizowanym przez szereg podmiotów, zarówno państwowych, jak i pozapaństwowych we wszystkich domenach. Oznacza to, że aktywność na tym polu musi być wielowymiarowa i powinna być realizowana w przestrzeni kosmicznej, powietrznej, lądowej, morskiej (nawodnej i podwodnej), a także w cyberprzestrzeni oraz w przestrzeni kognitywnej.

Współczesne konflikty zbrojne, w których uczestniczyły wojska Sojuszu (np. w Iraku, Afganistanie czy też Syrii), były odmienne od historycznie ukształtowanego przeznaczenia sił zbrojnych. Obecnie wojska są przeznaczone głównie do prowadzenia działań zbrojnych będących przedłużeniem polityki państw – konfliktów między państwami/sojuszami[213]. Ostatnie lata to przede wszystkim działania nieregularne i walka z terroryzmem i przeciwnikiem niepaństwowym. Działania te prowadzone były przede wszystkim w domenie lądowej i powietrznej.

W tym miejscu warto wspomnieć o rozwijanej przez Sojusz koncepcji prowadzenia operacji wielodomenowych (ang. *Multi-domain operations* – MDO)[214]. Potrzeba ich prowadzenia wynika ze zmieniającego się środowiska bezpieczeństwa, co zostało odzwierciedlone m.in. w nowej *Koncepcji strategicznej NATO*[215]. Środowisko to wymaga redefinicji sposobu prowadzenia działań zbrojnych perspektywie krótko-, średnio-

[213] Takie podejście wydawało się aktualne do czasu aneksji Krymu, czego wyrazem była deklaracja szczytu walijskiego złożona przez szefów państw i rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Walii 5 września 2014 r. Por. *Deklaracja Szczytu NATO w Walii*, 05.09.2014, pobrano z lokalizacji: https://www.bbn.gov.pl/ftp/dok/Deklaracja%20szczytu%20walijskiego.pdf [dostęp: 25.02.2020]. Potwierdzeni em konieczności dalszych zmian był 24 lutego 2022 r., czyli rozpoczęcie pełnoskalowego konfliktu zbrojnego w Ukrainie.

[214] Operacje wielodomenowe: ukierunkowanie działań militarnych we wszystkich domenach i środowiskach, zsynchronizowanych z działaniami pozamilitarnymi w celu umożliwienia Sojuszowi osiągnięcia zbieżnych efektów we właściwym czasie (tłum. autora). Definicja oryginalna: *...orchestration of military activities, across all domains and environments, synchronised with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance*. Por. *Allied Joint Doctrine*, AJP-01(F), 19.12.2022 r., s. 3.

[215] Por. *NATO 2022 Strategic Concept*, dz. cyt.

i długookresowej oraz opracowania nowych koncepcji rozwoju. W konsekwencji zostanie utrzymana wiarygodność militarna NATO. Niezaprzeczalnym faktem jest, że zarówno Rosja, jak i Chiny oddziałują na członków NATO we wszystkich pięciu domenach operacyjnych. Dla zneutralizowania tych niekorzystnych wpływów konieczne jest wypracowanie rozwiązań, które pozwolą NATO na skoordynowane i zsynchronizowane działanie we wszystkich domenach i środowiskach. W tym miejscu warto wspomnieć, że obecnie pojedynczy komponent, prowadząc działania tylko w „swojej" domenie, poza nielicznymi wyjątkami, jest zależny od efektów uzyskanych przez pozostałe komponenty. Natomiast osiągnięcie zamierzonych rezultatów zależy od umiejętnego „łączenia" działań w pojedynczych domenach z jednoczesną koordynacją aktywności w pozostałych. Dotyczy to tak wielu współczesnych operacji, że nie sposób wyobrazić sobie ich prowadzenie tylko w jednej domenie bez oddziaływania ze strony pozostałych. Istnieje zatem potrzeba spojrzenia w kategoriach szerszych niż tylko zwykła synchronizacja i koordynacja działań. Ponadto warunkiem koniecznym jest zmiana mentalności i sposobów postrzegania środowiska przyszłych operacji. Aby zrozumieć tę nową rzeczywistość, należy upewnić się, że wszyscy jednakowo rozumieją kwestie prowadzenia operacji wielodomenowych oraz posiadają umiejętność i chęć wykorzystania dostępnych rozwiązań technologicznych, które pozwolą na ich planowanie i realizację. Warto także podkreślić, że zasadniczym założeniem prowadzenia takich operacji jest zintegrowanie posiadanych zdolności we wszystkich domenach w ramach jednego zespołu zadaniowego wykorzystującego zaawansowane technologie w celu prowadzenia zsynchronizowanych działań z uwzględnieniem słabych stron przeciwnika. Dlatego też uważa się, że w planowaniu wojskowym należy w pełni uwzględnić możliwości i zagrożenia związane z przestrzenią kosmiczną i cyberprzestrzenią oraz rozwinąć zdolność nie tylko do łączenia informacji ze wszystkich domen i środowisk, ale także do optymalizacji działań wielodomenowych pomiędzy podmiotami wojskowymi a niewojskowymi w celu uzyskania komplementarnego wyniku. Wyniki tego skoordynowanego podejścia w pięciu domenach operacyjnych jeszcze bardziej uwypuklą wymiar efektów fizycznych, wirtualnych i poznawczych. Fundamentalne znaczenie dla sukcesu operacji wielodomenowych będzie miała transformacja cyfrowa ze względu na fakt, że NATO przekształca się w organizację skoncentrowaną na danych, która docenia, dzieli, wymienia i wykorzystuje je do osiągnięcia swoich celów. Wskazuje się także na fakt, że efektywne prowadzenie operacji wielodomenowych może być osiągnięte jedynie poprzez zmianę kulturową dokonaną przez poszczególnych członków Sojuszu z tradycyjnego

podejścia do operacji połączonych na takie, które jest szerzej skoncentrowane we wszystkich pięciu domenach operacyjnych[216]. To nowe spojrzenie na sposób prowadzenia działań uwzględnia złożoność nowoczesnego pola walki, tempo zmian w dostępie do informacji i w procesie podejmowania decyzji, a także rolę aktorów państwowych i niepaństwowych w kształtowaniu środowiska operacyjnego.

Biorąc pod uwagę założenia związane z prowadzeniem działań w środowisku wielodomenowym oraz te określone w nowych koncepcjach strategicznych rozwijanych w NATO, tj. *Concept for the Deterrence and Defence of the Euro-Atlantic Area* (DDA) oraz *NATO Warfighting Capstone Concept* (NWCC)[217], zasadne staje się podjęcie działań zmierzających do rozwoju systemu obronnego Polski, który nie będzie tylko odpowiedzią na rozwój zdolności przez Rosję. Właściwym sposobem postępowania jest swoista ucieczka do przodu, czyli zbudowanie zdolności, które pozwolą na niedopuszczenie do inwazji ze strony przeciwnika. Jednym z takich sposobów może być opracowanie i wprowadzenie narodowego systemu antydostępowego, który z jednej strony posiadałby zdolności do odstraszania przeciwnika, z drugiej zaś umożliwiał powstrzymanie agresji, przybycie sił Sojuszu oraz zapewniał w sposób możliwie najlepszy niezakłócone funkcjonowanie elementów infrastruktury krytycznej. Ważne jest także, aby taki system umożliwiał działania w każdych warunkach z wysokim prawdopodobieństwem osiągnięcia zakładanego celu, był w jak największym stopniu autonomiczny, ale pozwalał na sprzęgnięcie go z ewentualnym systemem antydostępowym NATO, UE lub koalicyjnym. Taki system powinien umożliwić skuteczne odstraszanie, w konsekwencji zmniejszenie prawdopodobieństwa rozpoczęcia pełnoskalowego konfliktu z udziałem sił zbrojnych, a w przypadku jego rozpoczęcia – skuteczną obronę i stworzenie warunków do przeprowadzenia działań ofensywnych. Biorąc pod uwagę wnioski płynące z dotychczasowych działań w Ukrainie, konieczna wręcz staje się budowa takich zdolności, które uniemożliwią lub przynajmniej znacznie utrudnią

[216] Por. *Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries*, ACT, 29.07.2022, pobrano z lokalizacji: https://www.act.nato.int/articles/multi-domain-operations-out-pacing-and-out-thinking-nato-adversaries [dostęp: 20.12.2022].

[217] Celem tych dwóch koncepcji jest zapewnienie, że Sojusz będzie lepiej przygotowany do odstraszania, a jeśli to konieczne, do obrony przed potencjalnymi zagrożeniami i wyzwaniami obecnie i w przyszłości. Poprzez wprowadzanie innowacyjnych rozwiązań, nowych koncepcji i planów oraz ich implementację Sojusz zachowa zdolność do dalszego rozwoju. DDA łączy aktualną myśl wojskową NATO w obliczu nieprzewidywalnego świata i radzenia sobie z konsekwencjami zmienionego i ewoluującego środowiska bezpieczeństwa i skupia się przede wszystkim na sposobach radzenia sobie z aktualnymi zagrożeniami. NWCC z kolei wskazuje, jakie wysiłki należy przedsięwziąć w NATO w perspektywie 20 lat. Koncepcja ta skupia się na rozwoju sojuszniczych sił zbrojnych, identyfikuje potencjalne luki w zdolnościach i dostarcza niezbędnych rekomendacji, aby zapewnić, że NATO jest gotowe i zdolne do spełnienia wymagań przyszłości. Por. *Allied Joint Doctrine*, AJP-01(F), dz. cyt., s. 35.

przekroczenie granic (zarówno tych fizycznych, realnych, jak i tych w wymiarze niefizycznym) Polski przez siły rosyjskie. W tym celu niezbędne jest posiadanie potencjału militarnego, który zniechęci przeciwnika do realizacji tego celu. Pozbawienie go przekonania, że osiągnie swoje cele poprzez wykorzystanie posiadanych środków bojowych jest głównym odstraszającym czynnikiem systemu antydostępowego[218]. Z drugiej strony istotną kwestią jest opracowanie założeń, którym ten system miałby odpowiadać. Jedną z możliwości mogłaby być idea podobna to tej rozwijanej w Republice Federalnej Niemiec w czasach „zimnej wojny". W latach 1960–1963 zbudowano ciągłą strefę ognia wzdłuż jej wschodniej granicy z wykorzystaniem systemów Nike Hercules i Hawk. W centrum każdego sektora rozmieszczono systemy przeciwlotnicze Nike Hercules o zasięgu 160 km, które były przeznaczone do zwalczania środków napadu powietrznego na dużej wysokości. Nike Hercules otoczone były systemami Hawk o zasięgu 35 km (później w wyniku modernizacji zasięg zwiększono do 42 km). Te ostatnie systemy były przeznaczone do zwalczania celów powietrznych na mniejszych wysokościach. Kolejne sektory ciągnęły się od granicy z Danią do granicy ze Szwajcarią. Przeciwlotniczych systemów rakietowych, które tworzyły ciągłą strefę ognia z wielowarstwowym polem, nie można było ominąć. Łańcuch systemów obrony powietrznej osłaniał najważniejsze obiekty na terenie Niemiec, a także główne zgrupowania wojsk lądowych[219]. Pytanie, które można sobie postawić, to czy podobna idea nie jest nieco archaiczna oraz czy Polska na tak rozbudowany system może sobie pozwolić pod względem finansowym? Trzeba stwierdzić, że zastosowanie ciągłej, wielowarstwowej strefy na długości ponad 1 000 km. jest w dzisiejszych warunkach niezwykle trudne do osiągnięcia, choćby biorąc pod uwagę tylko koszt finansowy. Rozważając taką możliwość, należałoby zakupić co najmniej 10 baterii zestawu Patriot z systemem ICBS, których przybliżony koszt to 48 mld dolarów[220]. Do tego należałoby nabyć kilkadziesiąt systemów o krótszym zasięgu w celu zapewnienia wielowarstwowego systemu ognia oraz zachowania pełnej komplementarności systemu. Należy także

[218] Na podstawie dyskusji, jaka toczyła się w ostatnich latach nad zagrożeniem ze strony rosyjskiego A2/AD, można stwierdzić, że element odstraszający spełnił swoje zadanie. Na ten temat powstało szereg publikacji, przeprowadzono dużą ilość gier wojennych, symulacji i rozważań, w jaki sposób pokonać rosyjski system. Zaprojektowano środki bojowe oraz rozpoczęto prace nad opracowaniem koncepcji stwarzających warunki do pokonania tego systemu. Wydano znaczne kwoty, podjęto spory wysiłek intelektualny w związku z rozbudową wielowarstwowego systemu, którego skuteczności na dobrą sprawę nikt nie sprawdził. Przyp. aut.

[219] R. Ciastoń, R. Czulda, J. Gruszczyński, M. Kowalski, T. Smura, *Obrona przeciwrakietowa na świecie – wnioski dla Polski*, Fundacja im. Kazimierza Pułaskiego, Warszawa 2016, s. 28.

[220] Por. R. Lesiecki, *Wisła i Patrioty za 4,75 mld dolarów. Kontrakt podpisany*, Defence 24, 28.03.2018, pobrano z lokalizacji: ttps://defence24.pl/polityka-obronna/wisla-i-patrioty-za-475-mld-dolarow-kontrakt-podpisany [dostęp: 27.12.2022].

zauważyć, że w tym przypadku jest mowa tylko o kosztach przeznaczonych na zakup systemów przeciwlotniczych i przeciwrakietowych rozmieszczonych wzdłuż granicy, które byłyby tylko jednym z wielu elementów niezbędnych do budowy narodowego systemu antydostępowego. Co więcej, taki system nie zapewniłby niezawodnej osłony elementów infrastruktury krytycznej rozmieszczonej w głębi kraju. W dalszej części dysertacji autor zaproponuje sposób budowy efektywnego systemu.

Podstawowym zagadnieniem, które powinno się określić w kontekście budowy narodowego systemu antydostępowego, jest znalezienie odpowiedzi na pytanie, do czego system antydostępowy jest potrzebny? Odpowiedź wydaje się prosta – do odstraszania, zapewniania osłony przed uderzeniami (w każdej domenie), stworzenia warunków do rozwinięcia sił własnych i Sojuszu do wykonania uderzenia oraz osłony elementów infrastruktury krytycznej, a w konsekwencji – do zapewnienia ciągłości funkcjonowania państwa.

Stworzenie systemu antydostępowego będącego elementem odstraszania może nastąpić poprzez rozbudowę i demonstrowanie własnych zdolności do wykonywania głębokich uderzeń czy też posiadanie umiejętności i możliwości prowadzenia operacji zarówno defensywnych i ofensywnych w cyberprzestrzeni. Z drugiej strony konieczne jest posiadanie wyszkolonych sił i efektywnych środków do zapewnienia obrony i zmniejszenia efektywności środków przeciwnika. Dzięki temu będzie możliwe stosunkowo niezakłócone funkcjonowanie elementów infrastruktury krytycznej oraz innych obiektów wpływających na potencjał gospodarczy, co z kolei wpłynie na zachowanie zdolności państwa do zabezpieczenia krytycznych potrzeb dla obywateli. Z kolei niezależność od zewnętrznych dostawców oraz producentów poprzez posiadanie własnego, silnego przemysłu obronnego wpływa na postrzeganie państwa jako samodzielnego gracza zdolnego do produkcji nowoczesnych środków bojowych. Oczywiście należy być w tym miejscu realistą i skupić się na rozwoju i wytwarzanu sprzętu, w którego produkcji polskie zakłady posiadają doświadczenie, np. środki obrony przeciwlotniczej czy niektóre rodzaje dronów. Niemniej istotne jest oddziaływanie na przeciwnika w warstwie niematerialnej i wytworzenie w nim przekonania, co do skuteczności i efektywności sił zbrojnych, gotowości do państwa do prowadzenia obrony oraz zwartości społeczeństwa.

Operacjonalizując dotychczasowe rozważania na temat ogólnych założeń narodowego systemu antydostępowego, można pokusić się o określenie zdolności, które powinien posiadać:

- zdolność do odstraszania;
- zdolność do stworzenia warunków umożliwiających ciągłe funkcjonowanie obiektów infrastruktury krytycznej i innych obiektów wpływających na potencjał obronny państwa;
- zdolność do zapewnienia ciągłej i wiarygodnej świadomości sytuacyjnej dla wszystkich decydentów (zarówno cywilnych, jak i wojskowych);
- zdolność do wykonywania uderzeń już na terenie przeciwnika w wymiarze fizycznym i w cyberprzestrzeni oraz rozbicia jego zgrupowań uderzeniowych jeszcze przed granicą państwa;
- zdolność do zapewniania warunków do niezakłóconego rozwinięcia sił własnych, jak również przybywających sił wzmocnienia Sojuszu.

5.3. Charakterystyka elementów funkcjonalnych systemu antydostępowego oraz ich wykorzystanie

Po rozpatrzeniu przedstawionych w poprzednim rozdziale systemów antydostępowych rozbudowanych przez Chiny i Rosję można dostrzec pewne różnice wynikające zarówno z odmiennej oceny środowiska bezpieczeństwa, jak i środowiska operacyjnego. Obydwa państwa również w odmienny sposób traktują zagadnienia związane z zapewnieniem bezpieczeństwa, wzbronieniem dostępu czy oceną sposobu działania przeciwnika.

W przypadku budowy przez Polskę własnego systemu antydostępowego zasadne jest zatem wzięcie pod uwagę wniosków będących konkluzją oceny środowiska bezpieczeństwa dokonanej w rozdziale drugim. Na podstawie dotychczasowych rozważań można przyjąć, że celem utworzenia narodowego systemu antydostępowego powinno być zbudowanie zdolności do zapobiegania lub ograniczania przeciwnikowi możliwości rozmieszczania swoich sił oraz swobody ich manewru na określonym obszarze, a także zapobiegania lub pogarszania możliwości atakujących sił w zakresie wejścia w broniony obszar. Ze względu na obszar Polski, w tym przede wszystkim brak głębi operacyjnej (w porównaniu do chociażby Chin czy Rosji), uznaje się, że zasadne jest nierozdzielanie działań w zakresie **A2** (przeciwdziałanie dostępowi) od tych realizowanych w ramach **AD** (pozbawienie swobody

działania), a traktowanie ich jako spójny, jednolity system. Należy uzmysłowić sobie fakt, że prowadzenie działań w ramach AD miałoby miejsce na polskich ziemiach pomiędzy Bugiem a Wisłą. Spowodowałyby to potężne straty zarówno wśród ludności cywilnej, jak i w obiektach infrastruktury krytycznej oraz gospodarczej państwa. Z drugiej strony wymuszałoby to konieczność późniejszych walk zmierzających do odzyskania tego terenu. Ponadto budowanie zdolności w dwóch odrębnych obszarach podniosłoby koszty budowy takiego systemu[221].

W dalszej części autor skupił się na określeniu poszczególnych elementów systemu antydostępowego w oparciu o niezbędne zdolności, a nie wskazywaniu, jaki konkretnie sprzęt (i w jakiej liczbie) powinien zostać włączony w jego strukturę. Takie podejście pozwoli na uwypuklenie roli, jaką tak zbudowany system mógłby odegrać w realizacji wspomnianych wyżej celów. Z drugiej strony taka idea pozwoliłaby na wykonanie swoistego kroku do przodu, a jednocześnie wpisywać by się mogła w podstawy koncepcji prowadzania operacji wielodomenowych. Zdaniem wielu ekspertów[222] wojna w Ukrainie może zostać określona jako pierwsze starcie w ramach prowadzenia operacji wielodomenowych, w czasie którego na poziomie operacyjnym posiadane są zdolności do organizowania i wykorzystania możliwości dostępnych w innych domenach do osiągnięcia wspólnego celu i generowania efektów w wymiarze fizycznym, kognitywnym oraz w sferze wirtualnej. Patrząc z tej perspektywy, można stwierdzić, że nawet pojedynczy komponent na poziomie taktycznym przyczynia się do zwiększenia zdolności do prowadzenia operacji wielodomenowych. Z drugiej strony biorąc pod uwagę, że domeny są zintegrowane i przenikają się wzajemnie, prawdopodobne jest, że pojedyncze działanie zapoczątkowane w jednej domenie zakończy się generowaniem efektów w sąsiedniej domenie. W związku z tym warto pokusić się o nowe spojrzenie na problematykę budowy systemu antydostępowego w Polsce. Jest to nowatorskie podejście, gdyż dotychczas większość rozważań, ćwiczeń, gier wojennych itp. prowadzonych w Sojuszu koncentrowała się na działaniach związanych z pokonaniem systemów antydostępowych przeciwnika, a nie na budowie własnego. Zdaniem autora należy pomyśleć o utworzeniu swoistych stref (baniek) antydostępowych, wykorzystując założenia koncepcji MDO. Naczelną ideą takiej koncepcji budowy narodowego systemu byłoby wyposażenie związków operacyjnych oraz

[221] Taki wniosek wynika z dotychczasowych badań, w tym przeprowadzonych wywiadów z ekspertami.
[222] Materiały własne pozyskane przez autora w ramach rozmów z ekspertami odpowiedzialnymi za opracowanie koncepcji prowadzenia operacji wielodomenowych z Allied Command Transformation oraz Allied Command Operations.

taktycznych w narzędzia i zdolności umożliwiające im wykorzystanie środków dostępnych w innych domenach do utworzenia tych stref nad swoim obszarem odpowiedzialności. Poprzez stworzenie warunków do przeciwdziałania dostępowi w swoim obszarze odpowiedzialności pojawia się możliwość utworzenia obszaru antydostępowego w rejonie kontaktu z przeciwnikiem dzięki wzajemnemu połączeniu tych stref. Tak zbudowany system, który może zostać nazwany systemem antydostępowym pierwszej linii, pozwala nie tylko na uniemożliwienie, a przynajmniej znaczne utrudnienie ataków wykonywanych za pomocą środków napadu powietrznego czy rakiet, lecz także stwarza warunki do użycia własnych środków uderzenia dalekiego zasięgu wykorzystanych do uderzeń na ważne elementy w ugrupowaniu przeciwnika (stanowiska dowodzenia i kierowania, urządzenia logistyczne, infrastrukturę lotniskową itp.). System powinien charakteryzować się wysoką manewrowością sił własnych oraz prowadzeniem działań (ofensywnych, defensywnych czy stabilizacyjnych) mających na celu zagwarantowanie odporności zarówno w wymiarze wojskowym, jak i cywilnym. Wykorzystanie zdolności do budowania przewagi w czasie prowadzenia działań wielodomenowych pozwala na generowanie wielowymiarowych efektów w celu wpływania na postawę i zachowanie przeciwnika oraz wspierania innych podmiotów cywilnych i wojskowych. Ze względu na wielodomenowy charakter tych działań eksperci zwracają uwagę na fakt, że obszary, w których są one prowadzone, niekoniecznie muszą mieć ściśle określone geograficznie granice. Te obszary, gdzie jest realizowany manewr, należy rozumieć jako strefy wielodomenowe, które w pewnych fazach prowadzenia działań mogą częściowo na siebie zachodzić lub się przenikać. Wszelkie działania w poszczególnych strefach muszą być prowadzone jednocześnie w sposób zharmonizowany, zintegrowany i komplementarny. Należy stwierdzić, że ich integracja musi przyczynić się przede wszystkim do degradacji siły bojowej przeciwnika poprzez oddziaływanie na jego krytyczne zdolności zlokalizowane w różnych domenach. Ponadto pozwala na stworzenie warunków do ochrony i konsolidacji swojej siły bojowej oraz elementów wpływających na zachowanie odporności. Realizacja takiej koncepcji budowy stref antydostępowych jest możliwa dzięki ewolucji technologicznej, gdzie każda wykorzystywana platforma (np. samolot, dron, okręt, czołg i szereg innych) staje się czujnikiem, który zbiera i udostępnia dane oraz wzmacnia świadomość sytuacyjną, tworząc sieć opartą na relacjach łączących sensory, decydentów i poszczególne środki rażenia rozmieszczone w przestrzeni oraz działające na całym obszarze prowadzonych działań. Jednocześnie wykorzystanie nowoczesnych (np. sztuczna inteligencja czy też

nanotechnologia) i niezawodnych środków przekazywania danych przyczyni się do szybszego i bezpieczniejszego obiegu, udostępniania oraz przetwarzania dużej ilości danych w sieci. To z kolei wpłynie na poprawę jakości i szybkości procesu decyzyjnego, a w konsekwencji zwiększy poziom synchronizacji i efektywność wykorzystania sensorów i środków rażenia działających w różnych domenach i zapewni harmonizację oraz integrację uzyskanych efektów w różnych wymiarach.

Dlatego też już na poziomie grupy bojowej czy batalionu należy posiadać zdolności i umiejętności planowania, realizacji i oceny działań w pojedynczych strefach (bańkach) antydostępowych. W tym kontekście istotne jest wykorzystanie cyfrowych systemów pozyskiwania, analizy, przetwarzania i przekazywania danych, wykorzystanie możliwości oferowanych przez różne domeny, wymiary (m.in. kosmicznej, cyberprzestrzeni czy też w spektrum elektromagnetycznym) lub wykorzystanie systemów bezzałogowych. Ponadto nie wyklucza się, że niektóre jednostki mogą być również wyposażone w zrobotyzowane systemy autonomiczne do realizacji wybranych zadań w ramach poszczególnych działań prowadzonych w złożonych środowiskach. Z kolei druga linia miałaby na celu ochronę własnego potencjału, który musi być przygotowany do wejścia do walki oraz wojskowych i cywilnych węzłów krytycznych, aby wygenerowanć przewagę komparatywną oraz utrzymać elementy wpływające na zachowanie odporności. Takie zestawienie sił i środków tworzących system antydostępowy z wykorzystaniem zasad koncepcji prowadzenia operacji wielodomenowych stanowi swoiste *novum* i pozwala w maksymalny sposób wykorzystać walory nowoczesnej technologii.

W dalszej części zostanie przedstawiona propozycja wykorzystania sił i środków, które zdaniem autora umożliwiłyby zbudowanie efektywnego systemu utrudniającego przeprowadzenie działań ofensywnych przez Rosję w sposób podobny do tych prowadzonych w Ukrainie.

Dla pełnego zrozumienia zaproponowanej koncepcji celowe jest wskazanie zdolności w poszczególnych domenach operacyjnych, jak również w domenie kognitywnej, które będą wpływały na efektywność narodowego systemu antydostępowego. Podkreślenia wymaga fakt, że efekty uzyskiwane w poszczególnych domenach nie powinny być rozpatrywane jako odrębne, ale powinny być ich swoistym połączeniem. Autor zwraca uwagę, że trudno jest jednoznacznie przypisać poszczególną zdolność do konkretnej domeny. Przykładem może być sytuacja związana z wykorzystaniem środków rażenia (rakiety NMS – *Naval Strike Missile*) Morskiej Jednostki Rakietowej. Siły i środki tej jednostki prowadzą działania na

lądzie, a efekty jej działalności będą obserwowane przede wszystkim w domenie morskiej, ale rakiety mogą być również wykorzystane w domenie lądowej, a nawet powietrznej.

W domenie lądowej celowe jest rozwinięcie zdolności do precyzyjnego rażenia stanowisk dowodzenia, zgrupowań wojsk, jak również systemów logistycznych na poziomie operacyjno-taktycznym czy też elementów infrastruktury krytycznej przeciwnika. Biorąc pod uwagę doświadczenia płynące z Ukrainy, systemy te powinny cechować się wysoką manewrowością i posiadać efektory o zasięgu pozwalającym na oddziaływanie na odległość co najmniej 300–500 km. Umożliwi to zniwelowanie potencjału bojowego przeciwnika[223]. Problemem może być utrzymanie zdolności do ciągłego zaopatrzenia w tej klasy rakiety. Celowe zatem jest podjęcie działań zmierzających do rozpoczęcia ich produkcji w Polsce. Biorąc pod uwagę określone w rozdziale czwartym kluczowe zdolności antydostępowe, należy dążyć także do zabezpieczenia odpowiedniej ilości środków artyleryjskich, rakiet i pocisków do niszczenia celów powierzchniowych na mniejszej głębokości[224]. Doświadczenia płynące z wojny w Ukrainie potwierdzają zasadność stosowania zapór minowych oraz systemów rozbudowy inżynieryjnej. Budowa systemu, w swoich założeniach podobnego do tego zastosowanego przez Rosjan na południu Ukrainy, nasyconego obiektami fortyfikacyjnymi i polami minowymi (przeciwczołgowymi, ale również przeciwpiechotnymi[225]), wpłynie na tempo działań przeciwnika, a w sprzyjających warunkach zmusi go do zmiany kierunku działania. Kolejnym elementem wpływającym na zbudowanie zdolności antydostępowych w domenie lądowej może być szerokie wykorzystanie tzw. bezzałogowych pojazdów lądowych przeznaczonych między innymi do prowadzenia rozpoznania, ochrony elementów infrastruktury krytycznej, jak również prowadzenia uderzeń na wybrane obiekty. Istotnym komponentem wpływającym na efektywość systemu antydostępowego jest posiadanie zdolności do pozyskiwania, analizy, przetwarzania, rozprzestrzeniania, a przede wszystkim właściwego wykorzystania informacji rozpoznawczych. Jednym z elementów niezbędnych do funkcjonowania systemu antydostępowego jest posiadanie i wykorzystanie jednostek sił specjalnych na terenie

[223] Należy zwrócić uwagę na fakt, że posiadanie nowoczesnych środków przeznaczonych do obrony podnosi koszt potencjalnego ataku ze względu na konieczność zwiększenia liczby pocisków, rakiet, które mogłyby pokonać rozbudowany system antydostępowy. Z drugiej strony zwiększa to zużycie tych środków, które i tak z wysokim prawdopodobieństwem zostaną zniszczone. Przyp. aut.
[224] Dzienne zużycie środków artyleryjskich przez wojska ukraińskie to ok. 6 tys. pocisków. Z kolei wojska rosyjskie zużywają jej ok. 30 tys. sztuk dziennie. Przyp. autora.
[225] Nie narusza to jednak postanowienia *Konwencji o zakazie użycia, składowania, produkcji i przekazywania min przeciwpiechotnych oraz o ich zniszczeniu* z 1997 r. Przyp. autora.

przeciwnika zapewniających między innymi pozyskiwanie danych rozpoznawczych czy też prowadzenie działań specjalnych. Przy budowie systemu antydostępowego należy wziąć także pod uwagę siły i środki będące na wyposażeniu wojsk operacyjnych oraz Wojsk Obrony Terytorialnej, które utworzą tzw. pierwszą linię antydostępową i będą zdolne do oddziaływania w więcej niż jednej domenie. Posiadane przez nie środki obrony powietrznej są ich integralną częścią, a ich zasadniczą rolą jest zapewnienie osłony siłom własnym przed rozpoznaniem i uderzeniami z powietrza. Będą one jednak powodowały obniżenie potencjału przeciwnika, co w konsekwencji wpłynie na osiągnięcie celu przeciwdziałania dostępowi. Jest to jeden z elementów zaproponowanej wizji nowego systemu antydostępowego w oparciu o koncepcję MDO.

W domenie powietrznej konieczne jest zapewnienie zdolności do zapobieżenia atakowi lub pogorszenia możliwości atakujących sił w zakresie wejścia w broniony obszar. Istotnym elementem jest zapewnianie osłony przed zagrożeniami z powietrza (środki rakietowe, samoloty, śmigłowce, drony itp.). Doświadczenia płynące z działań wojennych w Ukrainie wskazują jednoznacznie, że uderzenia z powietrza występują najczęściej, a zarazem stanowią ogromne zagrożenie także dla obiektów rozmieszczonych w głębi kraju, w tym elementów infrastruktury krytycznej wpływających na utrzymanie odporności. W celu zniwelowania niszczących skutków takich uderzeń istotne znaczenie ma pozyskanie zestawów zdolnych do oddziaływania na szerokie spektrum środków, które mogą zostać użyte przez przeciwnika. Utworzenie wielowarstwowego systemu oddziaływania na elementy wykorzystywane do prowadzenia ataków umożliwi reagowanie na różnorodne zagrożenia z powietrza. Należy przy tym zwrócić uwagę na właściwe rozmieszczenie zestawów, aby zminimalizować ryzyko uderzeń na obiekty ważne dla ciągłości kierowania państwem oraz istotne obiekty infrastruktury krytycznej. Przede wszystkim koniecznością staje się zapewnienie osłony portów, infrastruktury naftowej i gazowej oraz stacji przeładunkowych. Ważne jest także posiadanie zdolności do zwalczania celów powietrznych na jak największych odległościach (nawet nad terenem przeciwnika). Z całą pewnością należy zdać sobie sprawę z kosztów takich zakupów. Zdaniem gen. broni Waldemara Skrzypczaka Polska potrzebuje przynajmniej 16 baterii Patriot do zapewnienia osłony[226]. Biorąc pod uwagę cenę wynegocjowaną w 2018 r. za dwie baterie, koszt 16 takich

[226] Por. wywiad M. Zaborskiego z RMF FM z 28.03.2018 r. *Gen. Skrzypczak o bateriach Patriot: Kupiliśmy bezpieczeństwo polityczne i „parasol" na pół Warszawy*, pobrano z lokalizacji: https://www.rmf24.pl/tylko-w-rmf24/popoludniowa-rozmowa/news-gen-skrzypczak-o-bateriach-patriot-kupilismy-bezpieczenstwo-,nId,2562969#crp_state=1 [dostęp: 12.01.2023].

systemów to przynajmniej 32 mld dolarów[227]. Przy projektowaniu takiego systemu należy uwzględnić ich zasięgi (zarówno efektorów, jak i systemów rozpoznania, kierowania ogniem czy identyfikacji). Duże spektrum pozyskanych środków powinno wpłynąć na zapewnienie rażenia różnych środków napadu powietrznego. Niecelowe jest np. niszczenie relatywnie taniego drona jednorazowego użycia rakietą zestawu Patriot lub SKY SABRE[228]. Koszty mogą być niewspółmierne do korzyści. Zatem koniecznością jest posiadanie różnego rodzaju środków do reagowania na rozmaite zagrożenia. Poszczególne zestawy powinny być tak rozmieszczone, aby umożliwiały wzajemną osłonę i oddziaływanie na różnych zakresach odległości i wysokości. W dalszej kolejności należy także dążyć do pozyskania środków zapewniających oddziaływanie na pociski hipersoniczne. Coraz większego znaczenia w domenie powietrznej nabiera wykorzystanie dronów, w tym m.in. rozpoznawczych i uderzeniowych. Ich użycie jest znakomitym przykładem przenikania się poszczególnych domen. Działające w przestrzeni powietrznej systemy bezzałogowe będą wykorzystywane do prowadzenia np. rozpoznania, kierowania ogniem artylerii, jak również do wykonywania uderzeń na obiekty przeciwnika. Kolejnym elementem systemu antydostępowego w domenie powietrznej są załogowe środki powietrzne. Dlatego też należy uznać za celowe pozyskanie przez Polskę samolotów F-35, z których każdy jest tak naprawdę uzbrojonym zestawem różnorodnych sensorów, łączącym w sobie wielozadaniowość z sieciocentrycznością. Samoloty tego typu integrują szerokie spektrum informacji płynących z całej gamy sensorów, w które są one wyposażone, ze wszystkich domen operacyjnych i przetwarzają je, tworząc obraz dający świadomość sytuacyjną. Wskazania tych sensorów można wykorzystać do rażenia celów przez np. wyrzutnie HIMARS i inne środki walki[229]. Co więcej, po analizie danych możliwe jest naprowadzanie pocisków i rakiet wystrzelonych z innej platformy (np. zestaw Patriot, fregata) czy też przekazanie kontroli

[227] K. Janoś, *Umowa na Patrioty wreszcie podpisana. Zobacz, ile kosztuje bezpieczeństwo i co dają nam te rakiety*, Money.pl, 28.03.2018, pobrano z lokalizacji: https://www.money.pl/gospodarka/wiadomosci/artykul/mon-blaszczak-modernizacja-patriot-offset,151,0,2401943.html [dostęp: 21.10.2022].

[228] Koszt jednej rakiety PAC-2 zestawu Patriot to kwota 3–4 mln dolarów. Z kolei koszt jednego irańskiego drona Shahed-136 używanego przez Rosję w Ukrainie to około 20000 dolarów. Por. C. Mein, *How US Patriot missile systems could impact the Russia-Ukraine war*, The Hill, 21.12.2022 r., pobrano z lokalizacji: https://thehill.com/policy/defense/3777058-how-us-patriot-missile-systems-could-impact-the-russia-ukraine-war/ [dostęp: 10.01.2023] oraz M. Jankowicz, *Iranian-made drones cost as little as $20,000 to make but up to $500,000 to shoot down, a growing concern in Ukraine, report says*, Business Insider, 04.01.2023, pobrano z lokalizacji: https://www.businessinsider .com/suicide-drones-much-cheaper-launch-than-shoot-down-ukraine-nyt-2023-1 [dostęp: 16.05.2023].

[229] M. Szopa, *Defence24 Day: Operacje wielodomenowe w Siłach Zbrojnych RP*, Defence24, 27.05.2022, pobrano z lokalizacji: https://defence24.pl/polityka-obronna/defence24-day-operacje-wielodomenowe-w-silach-zbrojnych-rp [dostęp: 28.12.2022].

innemu samolotowi znajdującemu się często w sporej odległości. Możliwa jest także integracja danych o zagrożeniach z różnych segmentów widma elektromagnetycznego (częstotliwości radarowe, zakres widzialny, podczerwień, ultrafiolet). Środki rażenia dalekiego zasięgu, np. rakiety AGM-158B JASSM-ER przeznaczone do uderzeń na wysokoopłacalne cele naziemne (np. centra dowodzenia i łączności, lotniska, mosty czy też węzły logistyczne), pozwolą na niszczenie elementów istotnych dla prowadzenia operacji przez przeciwnika. Istotne jest, że realizacja tego zadania będzie możliwa już w trakcie przekraczania granicy państwa, co pozwoli na zlikwidowanie zaplecza logistycznego i odwodów.

Przy tworzeniu zrębów narodowego systemu antydostępowego nie można zapominać o uwzględnieniu domeny morskiej. Polska, posiadająca 770-kilometrowy dostęp do Morza Bałtyckiego, jest wpięta w światowy system szlaków morskich, a zarazem ma szereg elementów infrastruktury krytycznej rozmieszczonej na wybrzeżu i w pasie przybrzeżnym, w tym infrastruktury energetycznej, terminali gazowych czy portów. Zatem ochrona i uniemożliwienie lub chociażby utrudnienie przeciwnikowi ataku na te elementy powinna być jednym z głównych zadań realizowanych w domenie morskiej. Celowe zatem staje się pozyskanie zdolności do zamknięcia wyjść z rosyjskich portów bałtyckich, zapewnienia możliwości stworzenia wysuniętej strefy antydostępowej na morzu (również w głębinie wodnej) oraz wykonania uderzeń rakietowych na obiekty lądowe. Posiadanie takich zdolności mogłoby uniemożliwić przeciwnikowi przeprowadzenie niespodziewanego ataku na infrastrukturę. Do realizacji takich zadań konieczne jest pozyskanie okrętów z odpowiednimi systemami rozpoznania, naprowadzania, wymiany danych i uzbrojenia. W ten sposób umożliwiono by Morskiej Jednostce Rakietowej prowadzenie ognia poza linię horyzontu i wykorzystanie pełnego zasięgu rakiet. Byłoby to możliwe dzięki wskazywaniu celów dla tej jednostki przez okręty Marynarki Wojennej. Podobna sytuacja mogłaby być stworzona dla wydłużenia zasięgu systemów obrony powietrznej wynikającego z ograniczeń własnych stacji radiolokacyjnych. Ponadto stworzenie wielowarstwowej strefy antydostępowej na morzu umożliwiłoby własnemu lotnictwu działanie w ramach wsparcia komponentu morskiego. Celowe jest zatem pozyskanie: platform pływających wyposażonych w sensory radarowe zdolne do rozpoznania, namierzenia, śledzenia i prowadzenia wielu celów o różnej powierzchni skutecznego odbicia; systemu rozpoznania, analizy, przetwarzania i przesyłania danych zdolnego do współpracy z siłami realizującymi działania w domenie lądowej, powietrznej i kosmicznej; środków rażenia zdolnych do

zapewnienia wielowarstwowej strefy obrony powietrznej oraz umożliwiających rażenie okrętów nawodnych i podwodnych; środków do stawiania zapór minowych na morzu oraz pozwalających na transport sił specjalnych. Siły działające w domenie morskiej powinny także dysponować arsenałem środków bezzałogowych zdolnych do realizacji zadań zarówno w wodzie, jak i w powietrzu. Rozbudowa floty dronów pozwoli na zmniejszenie kosztów pozyskania drogich, wyspecjalizowanych platform morskich. Z przeprowadzonych przez autora wywiadów z ekspertami związanymi z działalnością Marynarki Wojennej (z Polski i krajów NATO) wynika, że właściwe byłoby pozyskanie okrętów podwodnych oraz nawodnych (fregaty i korwety) z zintegrowanym systemem wykrywania, naprowadzania i kierowania ogniem, a ponadto wyposażonych w rakiety manewrujące[230].

Jedną z dwóch nowych domen operacyjnych jest przestrzeń kosmiczna. Dla uzyskania wysokiej efektywności narodowego systemu antydostępowego wykorzystanie możliwości, jakie daje kosmos, staje się wręcz koniecznością. Szczególną rolę można przypisać umożliwieniu komunikacji i przepływu danych poprzez wykorzystanie satelitów do wsparcia procesu dowodzenia, kierowania oraz rozpoznania (np. zdjęcia satelitarne) czy nawet prognozy pogody. Wykorzystanie satelitów pozwala na lokalizowanie celów, pozycjonowanie wojsk własnych i przeciwnika, a także wypracowanie danych do przeprowadzenia precyzyjnego uderzenia[231]. Oznacza to, że dostęp do możliwości, które oferuje przestrzeń kosmiczna, zapewni uzyskanie świadomości sytuacyjnej zarówno na Ziemi, jak i w stosunku do innych podmiotów w kosmosie. Co więcej, satelity pozwalają na wczesne wykrycie wystrzelonych rakiet i pocisków (kluczowe dla wczesnego ostrzegania i podejmowania decyzji). Z drugiej strony posiadanie dostępu do broni antysatelitarnej pozwalającej na niszczenie satelitów przeciwnika pozwoliłoby na przerwanie komunikacji oraz utratę przez niego możliwości prowadzenia rozpoznania. Zasadne zatem jest podjęcie działań zmierzających do pozyskania zdolności do wykorzystania przestrzeni kosmicznej, przede wszystkim do zapewnienia stabilnych form komunikacji, przepływu danych i rozpoznania ze względu na fakt, że zdaniem ekspertów, użycie kinetycznej broni antysatelitarnej jest obecnie mało prawdopodobne. Zdaniem autora posiadanie wskazanych

[230] Autor zgodnie z przyjętymi wcześniej założeniami nie podaje liczby poszczególnych egzemplarzy sprzętu, jakie Polska mogłaby lub powinna pozyskać. Wynika to przede wszystkim z ograniczeń wskazanych na początku pracy. Przyp. autora.

[231] Należy zwrócić uwagę, że większość nowoczesnych środków rażenia zdolnych wykonać uderzenie na dużej odległości wykorzystuje systemy GPS/GLONASS. Zablokowanie dostępu do nich utrudnia, a czasami wręcz uniemożliwia przeprowadzenie precyzyjnego ataku. Przyp. autora.

wyżej możliwości będzie miało niebagatelny wpływ na efektywność narodowego systemu antydostępowego[232].

Kolejną nową domeną jest cyberprzestrzeń, w której – w odróżnieniu od klasycznych domen operacyjnych – jasne zdefiniowanie granic jest praktycznie niemożliwe. Wynika to z wielu czynników, ale przede wszystkim rozproszenia usług i infrastruktury oraz braku jawnych granic w znaczeniu prawa międzynarodowego. Jedną z metod określenia cyberprzestrzeni danego państwa jest reguła suwerenności[233], niestety ma ona ograniczone zastosowanie w przypadku działań zbrojnych i próbie technicznej ochrony cyberprzestrzeni. Próby określenia i zamknięcia tych wirtualnych granic poprzez wykorzystanie metod zarówno fizycznych, jak i logicznych mogą okazać się niemożliwe lub zbyt kosztowne w realizacji. Blokowanie logiczne, poprzez dopuszczenie tylko połączeń z terenu Polski (ang. *geoblocking*), pozostaje mało skuteczne ze względu na możliwość wykorzystania technologii zmieniających dane o lokalizacji użytkownika (ang. *geospoofing*) poprzez tworzenie tuneli (VPN – *Virtual Private Network*) bezpośrednio do kraju. Możliwa jest próba filtrowania lub blokowania takiego ruchu, ale koszt takiej operacji byłby olbrzymi i nie gwarantowałby sukcesu ze względu na możliwość budowania tuneli w innych protokołach i olbrzymią ilość danych, jakie musiałyby zostać przetworzone. Dodatkowo próby monitorowania zaszyfrowanego ruchu spotkałyby się z oporem społecznym i mogłyby naruszać konstytucyjne i unijne prawa do prywatności. Podobnie wygląda sytuacja z próbą fizycznego ograniczenia dostępu poprzez odcięcie połączeń bezpośrednio z danym przeciwnikiem. Niemożliwe jest zamknięcie ruchu tylko z jednego kierunku – protokoły budowania tras (*routing*) po prostu przekierują ruch poprzez inne państwo. Dodatkowo istnieje olbrzymia infrastruktura bezprzewodowa i satelitarna, nad która kontrola jest ograniczona. Przykładem tego może być chociażby *Starlink*. Odcięcie wszelkiej łączności miałoby katastrofalny wpływ na ludność i usługi świadczone przez lokalnych dostawców. Istnieje jednak kilka metod, które mogą ograniczyć działanie przeciwnika. Pierwszym krokiem jest określenie obszaru, który ma być chroniony i doprowadzenie do autonomizacji jego działania. Poza systemami służącymi siłom

[232] Podstawą do opracowania części dotyczącej wykorzystania przestrzeni kosmicznej są materiały własne autora, pozyskane w trakcie prac nad sojuszniczą doktryną prowadzenia operacji w przestrzeni kosmicznej. Przyp. autora.

[233] M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017, s. 11-29.

zbrojnym taka inwentaryzacja powinna objąć także sektory infrastruktury krytycznej[234]. Tak zdefiniowany obszar pozwoli na zachowanie ciągłości operacyjnej i umożliwi zaimplementowania pewnych dodatkowych form ochrony. Dodatkowo dzięki uniezależnieniu od usług zewnętrznych (np. umieszczonych w publicznych chmurach) możliwe będzie czasowe odcięcie tych systemów od zewnętrznej ingerencji, oczywiście kosztem degradacji usług dla użytkowników.

System obrony dla tak zdefiniowanego obszaru może przewidywać niżej wymienione metody:

1) Środowiska *Sandbox* (piaskownica), które umożliwiają bezpieczne uruchamianie załączników i skryptów w izolacji od sieci użytkowej. Dopiero po „detonacji", dane docierają do użytkownika wewnątrz chronionej sieci.
2) *Honey-pots* – fałszywe strony, serwisy, które mają odwrócić uwagę atakujących od właściwych zasobów. Pozwalają one na rozpoznanie metod pracy atakujących, ich identyfikację i pozwalają na spowolnienie ataku poprzez dostarczenie fałszywych danych.
3) *Canary tokens* – umieszczone we właściwej sieci pliki lub dane, które nie mają wartości same w sobie, ale pozwalają na wykrycie ataku. Przykładem może być chociażby plik z listą fałszywych użytkowników/haseł, jeśli ktoś spróbuje wykorzystać te dane, to oczywistym jest, że nie jest prawdziwym użytkownikiem sieci.
4) Operacje odwetowe, tzw. *hack-back*. W przypadku wykrycia ataku z wykorzystaniem ww. metod możliwe jest przeprowadzenie ataku zwrotnego, mającego na celu wyeliminowanie źródła zagrożenia. Takie działania niosą jednak za sobą olbrzymie ryzyko, jako że hackerzy często wykorzystują zainfekowane komputery osób prywatnych do przeprowadzania swoich ataków.

Wszystkie wymienione powyżej metody, jakkolwiek skuteczne, mogą zostać zaimplementowane wyłącznie w ograniczonej skali. Przeniesienie ich na skalę kraju może okazać się niemożliwe ze względu zarówno na koszt, jak i ograniczenia prawne.

Inną metodą, która obecnie zyskuje na popularności, jest zmiana modelu obrony na tzw. *Zero Trust* (zerowe zaufanie). Jest to odejście od koncepcji budowy obrony przed przeciwnikiem na poziomie zabezpieczania sieci i przeniesienie jej bliżej zasobów. To także

[234] R. Mattioli, C. Levy-Bencheton, *Methodologies for the identification of Critical Information Infrastructure assets and services*, ENISA, Heraklion 2014, s. 4-10.

odejście od budowy zapór i murów na rzecz ścisłej kontroli i ochrony pojedynczych zasobów. W pełni zaimplementowany model *Zero Trust* pozwala na funkcjonowanie nawet w środowisku, w którym przeciwnik zyskał znaczącą kontrolę nad naszą infrastrukturą poprzez silną i ciągłą weryfikację użytkowników i zasobów. Obecnie taka architektura jest wdrażana w wielu krajach, w tym USA[235].

Coraz powszechniejsze korzystanie z mediów społecznościowych, sieci i komunikatorów społecznościowych oraz urządzeń przenośnych umożliwia obecnie prowadzenie działań w domenie kognitywnej. Przewagę w niej osiągnie ta strona, która rozpocznie te działania – wybierze czas, miejsce i środki. Dostęp do mediów społecznościowych umożliwia wpływanie na odbiorców, udostępnianie wybranych dokumentów, produkcji filmów wideo, śledzenie wybranych osób itp. Działania antydostępowe w tej domenie powinny przede wszystkim koncentrować się na zwiększaniu świadomości społeczeństwa, aby wzmocnić jego odporność na manipulację, dezinformację, wybiórczą informację. Pozwoli to w konsekwencji na zmniejszenie prawdopodobieństwa narzucenia narracji kształtującej postawy społeczeństwa zgodnie z wolą przeciwnika. Jednym z proponowanych rozwiązań jest system monitorowania działań w domenie kognitywnej, który byłby użyteczny w rozpoznaniu i śledzeniu tych działań. Mógłby on obejmować tablicę sterującą, która integrowałaby dane z szerokiego zakresu mediów społecznościowych, mediów nadawczych, komunikatorów społecznych i portali społecznościowych. Wyświetlałaby ona mapy geograficzne i mapy sieci społecznościowych, które pokazywałyby rozwój podejrzanych kampanii w określonym czasie. Dzięki rozpoznaniu miejsc, zarówno geograficznych, jak i wirtualnych, z których pochodzą posty, wiadomości i artykuły informacyjne w mediach społecznościowych, a także tematów dyskusji, nastroju, językowych znaków rozpoznawczych, tempa publikacji i innych czynników, taka tablica może ujawnić powiązania i powtarzające się wzorce. Można zaobserwować powiązania między kontami w mediach społecznościowych (np. przesyłanie treści, komentarze, interakcje) i ich czas[236]. Wykorzystanie algorytmów uczenia maszynowego (w przyszłości sztucznej inteligencji) oraz rozpoznawania wzorców mogłoby

[235] S. Rose, O. Borchert, S. Mitchell, S. Connelly, *Zero Trust Architecture*, NIST, Waszyngton 2020, s. 32-41.
[236] Opracowano na podstawie: *Wojny kognitywne: niszczenie odporności społeczeństwa*, Centrum Badań Polityki Europejskiej, 05.05.2023, pobrano z lokalizacji: https://cbpe.pl/2023/05/05/wojny-kognitywne-niszczenie-odpornosci-spoleczenstwa/ [dostęp: 24.07.2023].

pomóc w szybkiej identyfikacji i klasyfikacji pojawiających się kampanii bez konieczności interwencji człowieka[237].

Konkludując, należy stwierdzić, że dla uzyskania wysokiej efektywności w taki sposób zbudowanego systemu antydostępowego niezbędne jest wykorzystanie wszelkich możliwości, jakie dają poszczególne domeny. Konieczna jest także ich pełna integracja, która jest możliwa przy zastosowaniu nowoczesnych, przełomowych technologii. Wykorzystanie środków rozpoznawczych działających w różnych domenach pozwoli na uzyskanie pełnej świadomości sytuacyjnej, w każdym miejscu i czasie. Umożliwi to skoordynowanie użycia wszelkich środków rażenia będących dostępnych w danej chwili. Decyzja o użyciu poszczególnych sensorów i efektorów mogłaby być podejmowana z wykorzystaniem sztucznej inteligencji.

5.4. System antydostępowy Polski jako część nadsystemu Sojuszu

Rozpatrując zaproponowany wyżej sposób budowy narodowego systemu antydostępowego w oparciu o koncepcję prowadzenia operacji wielodomenowych, zasadne wydaje się tworzenie wspólnej, spójnej i wzajemnie uzupełniającej się tarczy antydostępowej Sojuszu. Takie rozwiązanie wymagałoby z pewnością zaplanowania i budowy poszczególnych podsystemów w sposób skoordynowany przez poszczególne państwa, które przystąpiłyby do jego tworzenia. Z całą pewnością należy się liczyć w tym przypadku, że nie wszystkie kraje Sojuszu byłyby zainteresowane budową takiego systemu. W związku z tym celowe wydaje się utworzenie swoistej koalicji państwchętnych, szczególnie tych leżących na wschodniej granicy NATO.

Patrząc na zasady, jakie określono dla operacji wielodomenowych, można z dużą dozą prawdopodobieństwa założyć, że poszczególne kraje rozbudowując swoje zdolności w tym zakresie, mogłyby przystąpić do utworzenia szczelnej, mobilnej, elastycznej tarczy antydostępowej nad obszarem przynajmniej części Sojuszu. Położenie poszczególnych państw, posiadane zdolności, skoordynowane cele rozbudowy poszczególnych elementów systemu mogą zapewnić wykorzystanie możliwości jednych sygnatariuszy przez drugich. Wspólna polityka zakupów, szkolenie oraz dowodzenie i kierowanie takim systemem

[237] L. Aronhime, A. Cocron (red.), *Countering cognitive warfare: awareness and resilience*, [w:] *NATO Review*, 20.05.2021, pobrano z lokalizacji: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [dostęp: 18.02.2022].

przyczyniłoby się do podziału kosztów, a w konsekwencji do chętniejszego przystąpienia poszczególnych państw do takiej inicjatywy.

Z drugiej strony podejmowane są inicjatywy polegające na budowie europejskiej tarczy rakietowej. Można je traktować jako początek tworzenia wspólnego systemu antydostępowego. Istotna jest inicjatywa, która ma na celu m.in. wzmocnienie zintegrowanej obrony powietrznej i przeciwrakietowej (ang. *Integrated Air and Missile Defence* – IAMD) NATO poprzez ułatwienie wielonarodowego nabycia i integracji szerokiego zakresu zdolności obrony powietrznej przez kraje europejskie. Jedną z takich prób jest projekt europejskiej tarczy antyrakietowej. Do tej pory w projekcie tym uczestniczy 17 państw[238]. Jest to nic innego jak próba budowy jednego z elementów systemu antydostępowego, jakim jest zapewnienie osłony przed uderzeniami rakiet balistycznych oraz innych środków napadu powietrznego (zarówno załogowych, jak i bezzałogowych). Idea utworzenia wspólnej tarczy jest wynikiem przeświadczenia, że Europa nie jest w stanie zapewnić sobie efektywnej ochrony przed zagrożeniami z powietrza. System ten polegałby na wspólnym nabywaniu sprzętu obrony powietrznej i rakiet przez sygnatariuszy tego porozumienia. Zgodnie z komunikatem udostępnionym na stronach NATO inicjatywa ta ma umożliwić wszystkim uczestniczącym w niej państwom wspólne opracowanie systemu obrony przeciwlotniczej i przeciwrakietowej z wykorzystaniem interoperacyjnych rozwiązań dostępnych na rynku. Takie wielonarodowe i wielopłaszczyznowe podejście oferuje uczestnikom elastyczny i skalowalny sposób wzmocnienia ich zdolności odstraszania i obrony w sposób skuteczny oraz opłacalny[239]. Jak do tej pory z różnych względów do tej inicjatywy nie przyłączyła się Polska ani Francja. Do głównych przyczyn nieprzystąpienia Francji do tego programu jest chęć stawiania na własne rozwiązania w obszarze technologii militarnych oraz koncentracja na europejskich programach zbrojeniowych. Francuzi nie są zainteresowani zakupem ani amerykańskich, ani niemieckich systemów. Z kolei Polska jest w trakcie wdrażania zaawansowanych programów obrony powietrznej krótkiego oraz

[238] Do tej inicjatywy należą następujące państwa: Belgia, Bułgaria, Czechy, Dania, Estonia, Finlandia, Holandia, Litwa, Łotwa, Niemcy, Norwegia, Rumunia, Słowacja, Słowenia, Szwecja, Węgry oraz Wielka Brytania. Por. *European Sky Shield Initiative gains two more participants*, 15.02.2023, pobrano z lokalizacji: https://www.nato.int/cps/en /natohq/news_211687.htm [dostęp: 18.03.2023].

[239] Por.: *14 NATO Allies and Finland agree to boost European air defence capabilities*, 13.10.2022, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/news_208103.htm?selectedLocale=en [dostęp: 27.03.2023].

średniego zasięgu i skupia się na rozwijaniu współpracy wojskowo-przemysłowej z USA i z Wielką Brytanią[240].

Pomijając sprawy związane z polityką, wspomniana wyżej inicjatywa jest tylko jednym z elementów budowy wspólnego systemu antydostępowego. Dotychczasowe pomysły w tym obszarze koncentrowały się przede wszystkim na poszukiwaniu możliwości zapewnienia swoistego parasola ochronnego przed uderzeniami z powietrza. Nie skupiano się na innych zagrożeniach (np. ataki z morzą czy z lądu). Zdaniem autora jest to swego rodzaju spłycenie zagadnienia. Budowę wspólnego systemu antydostępowego warto byłoby projektować, wykorzystując analizę wszelkich możliwych zagrożeń, których właściwa identyfikacja pozwoliłaby na określenie potrzeb w tym zakresie. Biorąc pod uwagę potencjalne zagrożenia i wyzwania dla bezpieczeństwa naszego państwa, zdaniem autora właściwe byłoby zaplanowanie systemu w oparciu o koncepcję prowadzenia operacji wielodomenowych w sposób zaproponowany w podrozdziale 5.3.

W przypadku budowy takiego systemu należałoby wykorzystać doświadczenia oraz możliwości poszczególnych krajów. Kolejnym ważnym zagadnieniem jest określenie, czy konieczna jest budowa takiego systemu przy współudziale większości państw NATO, czy też może raczej należało by się skupić na zawiązaniu swojego rodzaju koalicji chętnych. Zdaniem autora za celowe należy uznać podjęcie prób przekonania do tego pomysłu państw leżących na wschodniej granicy Sojuszu (Finlandia, Litwa, Łotwa, Estonia, Polska oraz Rumunia), Szwecji będącej w trakcie akcesji do NATO, a także Ukrainy (jako potencjalnego członka NATO w przyszłości). Pozwoliłoby to na wykorzystanie sumy doświadczeń poszczególnych członków i partnerów NATO w rozwoju poszczególnych środków uzbrojenia (mogących stanowić istotne elementy przyszłego systemu antydostępowego) czy też ich położenia geograficznego (np. Gotlandia).

Przyłączenie się Szwecji do tego projektu pozwoliłoby na istotną zmianę sytuacji w rejonie Morza Bałtyckiego. Dzięki wykorzystaniu położenia Gotlandii możliwe byłoby ograniczenie swobody ruchu sił morskich Federacji Rosyjskiej na Bałtyku. Warto zwrócić uwagę, że wiele podmorskich kabli służących komunikacji jest połączonych za pośrednictwem Gotlandii. Uwzględniając zagrożenia dla infrastruktury krytycznej wskazane w poprzednim rozdziale, wykorzystanie możliwości, które oferuje Szwecja, miałoby

[240] J. Gotkowska, *Germany's European Sky Shield Initiative*, Ośrodek Studiów Wschodnich, 14.10.2022, pobrano z lokalizacji: https://www.osw.waw.pl/en/publikacje/analyses/2022-10-14/germanys-european-sky-shield-initiative [dostęp: 24.02.2023].

niebagatelne znaczenia dla wzmocnienia odporności. Wielu ekspertów uważa, że wyspa Gotlandia jest dogodnym miejscem do rozwinięcia niektórych elementów systemu antydostępowego, np. zintegrowanego systemu obrony powietrznej i przeciwrakietowej oraz przeciwokrętowej. Z drugiej strony może stać się zapleczem logistycznym dla operujących okrętów będących również kolejnymi elementami opisywanego systemu. Uważa się, że dołączenie Szwecji do takiej koalicji pozwoli na wzmocnienie systemu bezpieczeństwa w rejonie Bałtyku[241].

Fińska akcesja do NATO, a w perspektywie możliwość przyłączenia się do inicjatywy utworzenia regionalnego systemu antydostępowego, stworzyła nowe istotne szanse na zapobieżenie ewentualnej inwazji Rosji. Finlandia ma rozbudowaną infrastrukturę obrony cywilnej, zbudowaną na podstawie narodowej strategii bezpieczeństwa, która może być aktywowana w przypadku kryzysu i wojny. Obejmuje ona m.in. zapasy żywności i paliwa w strategicznych magazynach na co najmniej sześć miesięcy oraz schrony dla ludności miejskiej. Cywilny aparat obrony totalnej Finlandii powstał jako bezpośrednia konsekwencja odparcia pełnowymiarowej inwazji Związku Radzieckiego w latach 40. Te strategiczne zapasy zostały wykorzystane podczas pandemii Covid-19, co pokazało ich przydatność. Odporność jest połączeniem zdolności i stanu umysłu – etos gotowości Finlandii stanowi wzór do naśladowania dla państw członkowskich NATO, które chcą sprostać wyzwaniom XXI wieku[242]. Z drugiej strony zaawansowanie technologiczne tego kraju, szczególne w dziedzinie bezpieczeństwa cybernetycznego, może być postrzegane jako niebagatelny wpływ na rozwój systemu antydostępowego w domenie cyberprzestrzeni[243]. Kolejnym elementem wniesionym przez Finlandię mogą być jej zdolności do prowadzenia uderzeń artyleryjskich na elementy ugrupowania przeciwnika[244].

---

[241] Por.: F. K. Chang, *Sweden's Importance to NATO's Defense of the Baltics*, Foreign Policy Research Institute, 28.09.2017, pobrano z lokalizacji: https://www.fpri.org/2017/09/swedens-importance-natos-defense-baltics/ [dostęp: 23.06.2022].

[242] R. Forsberg, A-M. Kähkönen, J. C. Moyer, *Finland's Contributions to NATO: Strengthening the Alliance's Nordic and Arctic Fronts*, Wilson Center, 08.11.2022, pobrano z lokalizacji: https://www.wilsoncenter.org/article/finlands-contributions-nato-strengthening-alliances-nordic-and-arctic-fronts [dostęp: 14.01.2023].

[243] Z przeprowadzonych w 2022 r. przez Reboot Digital PR Services badań wynika, że Finlandia jest krajem o najniższym poziomie zagrożenia cybernetycznego w skali globalnej. Eksperci stworzyli indeks, z którego wynika, że Finlandia jest krajem o najwyższym współczynniku cyberbezpieczeństwa. Por. *Finland scores highly for cybersecurity: Digital Nomads*, Helsinki Times, 24.08.2022, pobrano z lokalizacji: https://www.helsinkitimes.fi/world-int/22088-finland-scores-highly-for-cybersecurity-digital-nomads.html [dostęp: 22.02.2023].

[244] E. Braw, *What Finland Can Offer NATO, Foreign Policy*, 14.04.2022, pobrano z lokalizacji: https://foreignpolicy.com/2022/ 04/14/ what-finland-can-offer-nato/ [dostęp: 21.01.2023] oraz spotkania i rozmowy autora z przedstawicielami SZ Finlandii.

Rozpatrując z kolei rolę państw bałtyckich w budowie regionalnego systemu antydostępowego, warto zwrócić uwagę na ich potencjał[245], a z drugiej strony na postulaty opracowane przez ekspertów amerykańskiego *think-tanku* Jamestown Foundation, którzy jasno wskazują na konieczność wzmocnienia zdolności obronnych przez te państwa do poziomu umożliwiającego odparcie, z ograniczonym wsparciem sojuszników, pierwszego uderzenia Federacji Rosyjskiej, a także przygotowania teatru działań oraz przyjęcia sił wzmocnienia NATO[246]. W celu zaangażowania tych państw do stworzenia takiego systemu należałoby skupić się na zdolnościach, które te kraje mogłyby wnieść jako wartość dodaną. Można by rozważyć rozwinięcie zdolności tych krajów do uniemożliwienia lub znacznego utrudnienia swobody ruchu sił i środków rosyjskiej Floty Bałtyckiej, wykorzystując do tego flotę licznych niewielkich aparatów bezzałogowych. Umożliwiłoby to stały monitoring oraz prowadzenie działań ofensywnych i defensywnych na powierzchni i pod powierzchnią wody[247]. Efekty takich działań wpisywałyby się z całą pewnością w zwiększenie poziomu odporności poprzez osłonę elementów morskiej infrastruktury krytycznej (w tym także polskiej). Istotnym wkładem w budowę systemu antydostępowego mogłyby być także elementy systemu obrony powietrznej i przeciwrakietowej tych państw.

Celowe wydaje się także podjęcie dyskusji z pozostałymi partnerami w ramach bukaresztańskiej dziewiątki, czyli z: Bułgarią, Czechami, Rumunią, Słowacją i Węgrami. Ich położenie geograficzne oraz posiadane siły i środki pozwoliłyby na stworzenie systemu antydostępowego od północnych krańców Europy aż po wybrzeże Morza Czarnego.

Zaangażowanie wyżej wymienionych partnerów, w tym także Ukrainy (jej doświadczenie z prowadzenia wojny z Rosją są bezcenne), umożliwiłoby stworzenie efektywnego systemu antydostępowego mogącego stanowić realny sposób na odstraszanie przeciwnika, ochronę własnych elementów infrastruktury krytycznej, a w przypadku agresji – znaczne utrudnienie, a wręcz uniemożliwienie jej prowadzenia. Takie rozwiązania mogłyby doprowadzić do maksymalnego wykorzystania posiadanego potencjału przez poszczególnych partnerów, a także w znaczny sposób ograniczyć koszty realizacji tego przedsięwzięcia. Należy dodać, że istotna jest także ścisła współpraca ze Stanami

[245] Zgodnie z ostatnim (za 2023 r.) zestawieniem Global Firepower określającym siłę militarną poszczególnych krajów (oceną objęto 145 krajów) Litwa zajmuje 93., Łotwa 95., Estonia 104. miejsce. Dla porównania Polska uplasowała się na 20. miejscu. Por. *2023 Military Strength Ranking*, pobrano z lokalizacji: https://www.globalfirepower.com/ countries-listing.php [dostęp: 31.03.2023].
[246] Por.: R. D. Hooker, *How to Defend the Baltic States*, The Jamestown Foundation, Waszyngton, October 2019 r.
[247] Por. C. Herdt, M. Zublic, *Baltic Conflict: Russia's Goal to Distract NATO?,* CSIS, Waszyngton, November 2022 r.

Zjednoczonymi w budowaniu takiego systemu. Ich doświadczenie i posiadane zdolności mogłyby zostać udostępnione państwom leżącym na wschodniej granicy Sojuszu. Wspomniane wyżej niektóre zdolności, którymi dysponują (lub mogą dysponować) poszczególni potencjalni uczestnicy takiej inicjatywy, wzmocnione zdolnościami USA, mogłyby posłużyć jako baza do rozbudowy wspólnego, zintegrowanego, realizowanego zgodnie z założeniami koncepcji prowadzenia operacji wielodomenowych systemu antydostępowego będącego elementem systemu obronnego Sojuszu Północnoatlantyckiego[248].

5.5. Konkluzje

Doświadczenia płynące z wojny w Ukrainie oraz zbrodnicza działalność Rosji stawiają pod znakiem zapytania zasadność czasowego oddania terenu przeciwnikowi. Po wydarzeniach w Buczy czy innych rejonach będących pod okupacją rosyjską staje się oczywiste, że do podobnych sytuacji z dużą dozą prawdopodobieństwa mogłoby dojść także w Polsce w przypadku agresji Federacji Rosyjskiej. Nie można także zapominać, że im więcej terenu zajmie przeciwnik, tym większych strat w majątku narodowym należy oczekiwać. Z drugiej strony zniszczenie elementów infrastruktury krytycznej (np. sieci przesyłu energii, nafto- i gazoportów, kabli energetycznych) może doprowadzić do uzależnienia gospodarczego od agresora. Z tego też chociażby powodu warto rozważyć możliwość budowy narodowego systemu antydostępowego z opcją włączenia go w nadsystem regionalny lub Sojuszu.

Ze względu na warunki terenowe, brak głębi operacyjnej, konieczność niedopuszczenia wojsk rosyjskich do przekroczenia granicy Polski za zasadne uważa się odejście od typowego podziału na strefę A2 i AD. Termin A2/AD zaproponowany przez Amerykanów na potrzeby ewentualnej wojny z Chinami nie ma zastosowania w przypadku Polski czy innych krajów leżących na wschodniej granicy Sojuszu. W polskich realiach celowe jest dążenie do ustanowienia strefy, która znacząco utrudniłaby lub wręcz uniemożliwiła przekroczenie granicy państwa przez przeciwnika.

[248] Podobne rozwiązania, mające na celu budowę własnego system antydostępowego (tzw. Blue A2/AD), postulowane są między innymi przez ekspertów z korporacji RAND. Por. T. K. Kelly, D. C. Gompert, D. Long, *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression*, RAND Corporation, Santa Monica 2016, a także T. M. Bonds, J. B. Predd, T. R. Heath, M. S. Chase, M. Johnson, M. J. Lostumbo, J. Bonomo, M. Mane, P. S. Steinberg, *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?*, RAND Corporation, Santa Monica 2017.

Stworzenie systemu, który byłby tylko swego rodzaju murem przed agresorem, spowoduje, że nie byłby on w pełni funkcjonalny. Konieczne jest jego uzupełnienie w środki ofensywne, które umożliwiłyby rażenie centrów dowodzenia, elementów logistycznych, zgrupowań wojsk czy także elementów infrastruktury krytycznej przeciwnika w celu pozbawienia go zdolności do kontynuowania działań. Mogłyby one zostać także wykorzystane do zniwelowania efektywności systemów uzbrojenia przeciwnika. Zasadne jest budowanie systemu antydostępowego na zasadzie *tarczy i włóczni*, tzn. zdolności do obrony i uderzenia na dużych odległościach. Dlatego istotne jest dalsze inwestowanie w nowoczesne, efektywne systemy umożliwiające oddziaływanie we wszystkich domenach. Posiadanie takich środków zwiększa koszty, które przeciwnik będzie musiał ponieść podczas agresji.

W przypadku napaści system umożliwiałby zmniejszenie skutków uderzeń rakietami, środkami napadu powietrznego czy artylerią, a w konsekwencji mógłby zapewnić utrzymanie zakładanego poziomu odporności, a w tym w możliwie największym stopniu niezakłócone funkcjonowanie obiektów infrastruktury krytycznej. Jak istotne jest utrzymanie ciągłości wytwarzania i przesyłu energii czy zapewnienie transportu pokazuje przykład Ukrainy.

Budowa systemu antydostępowego stanowi bardzo złożone podejście do obrony kraju lub określonej części jego terytorium. Obejmuje zarówno elementy odstraszania, jak i odporności, aby zapobiec wszelkim atakom poprzez wykazanie zdolności do zwalczania sił przeciwnika w przypadku ich wejścia na nasze terytorium lub na wspólny obszar operacji sojuszniczej. System antydostępowy koncentruje się na działaniach i zdolnościach przede wszystkim dalekiego zasięgu, które mają na celu uniemożliwienie siłom przeciwnika wejścia na obszar operacyjny. Taki system powinien być redundantny oraz umożliwiać wzajemną osłonę (strefy wykrywania i ognia powinny się zazębiać), aby w konsekwencji zapewnić jego odporność. Powinien także posiadać zdolności pozwalające na oddziaływanie na przeciwnika we wszystkich domenach pola walki, ze szczególną rolą poszczególnych rodzajów sił zbrojnych: powietrznych, lądowych, marynarki wojennej, sił specjalnych, wojsk obrony terytorialnej, wspieranych przez zdolności cybernetyczne i walki elektronicznej. Takie wykorzystanie posiadanych zasobów pozwoli na zadanie przeciwnikowi znacznych strat i opóźnianie jego działań, co może spowodować rewizję planów, ograniczyć postępy i powstrzymać agresję; równolegle stworzy to warunki dla sił własnych do konsolidacji obrony i rozpoczęcia działań ofensywnych.

Rozwijana koncepcja operacji wielodomenowych w NATO, ale również w poszczególnych krajach, może w znaczny sposób przyczynić się do rzeczywistego budowania systemu antydostępowego opartego na prowadzeniu działań we wszystkich pięciu domenach. Narodowy system antydostępowy, wykorzystujący najnowocześniejsze technologie, działający zgodnie z zasadami koncepcji MDO we wszystkich domenach, może umożliwić wzbronienie dostępu, a także zadanie dużych strat wojskom przeciwnika, a w konsekwencji pozbawć ich możliwości dalszego oddziaływania. Wykorzystanie nowoczesnych technologii, zmiana mentalności, analiza przepisów prawnych, efektywny proces szkolenia może umożliwić wprowadzenie istotnych zmian w procesie planowania i organizowania działań. Niezmiernie ważne jest również zapewnienie wszystkim użytkownikom jednakowej świadomości sytuacyjnej, co w połączeniu ze wszystkimi innymi elementami pozwoli na efektywne wykorzystanie dostępnych w danej chwili odpowiednich środków. Niezwykle istotne jest zrozumienie, że proces decyzyjny w zakresie użycia odpowiednich środków będzie musiał być realizowany na stosunkowo niskich szczeblach dowodzenia. Należy sobie uzmysłowić, że każdy element proponowanego systemu może i powinien multiplikować potencjał pozostałych składników systemu. Aby cały proces był realizowany sprawnie, z wysokim prawdopodobieństwem realizacji zakładanych celów, niezbędne jest także wykorzystanie możliwości, które daje sztuczna inteligencja.

Z kolei przekonanie partnerów do budowy wspólnej, regionalnej inicjatywy dotyczącej systemu antydostępowego z całą pewnością będzie ogromnym wyzwaniem dyplomatycznym. Na przeszkodzie mogą stanąć poszczególne partykularne interesy polityczne, ale także szczegółowy podział kosztów. Zdaniem ekspertów korporacji RAND perspektywy dla takiego regionalnego systemu w Europie są dobre ze względu na zapewnienie przez NATO odpowiednich mechanizmów planowania, a w razie potrzeby także użycia siły oraz posiadania stosownych do tego kompetencji.

Rozszerzenie NATO o Szwecję i Finlandię z natury rzeczy stworzy Sojuszowi większą przestrzeń do obrony, ale z drugiej strony (np. posiadane zdolności militarne, wysoka odporność cywilna, zaawansowana technologia telekomunikacyjna) oferuje zwiększenie poziomu bezpieczeństwa w regionie poprzez posiadanie zdolności do obrony na północno-wschodniej flance, zwłaszcza w pobliżu Sankt Petersburga, Morza Bałtyckiego i Arktyki czy rosyjskiego Półwyspu Kola. Można nawet stwierdzić, że Morze Bałtyckie stanie się morzem wewnętrznym NATO, co w konsekwencji może oznaczać zamknięcie Floty Bałtyckiej w portach i uniemożliwienie jej realizacji zaplanowanych zadań.

Kluczowym problemem staje się określenie możliwości zbudowania zarówno narodowego, jak i sojuszniczego (regionalnego) systemu antydostępowego. Trwająca wojna w Ukrainie, mobilizacja Sojuszu, zwiększanie wydatków na Siły Zbrojne RP, zmiana mentalności w Europie, uświadomienie sobie zagrożenia ze strony Rosji, nowe koncepcje i rozwój technologiczny – wszystkie te czynniki sprawiają, że szansa na zbudowanie takiego systemu rośnie. Z całą pewnością należałoby rozpocząć budowę takiego systemu w Polsce, co mogłoby stać się swego rodzaju inkubatorem rozwoju przedmiotowej inicjatywy w regionie. Należy stwierdzić, że wspólnie zbudowany system antydostępowy na wschodniej granicy Sojuszu przyczyniłby się do znacznego rozwoju poziomu bezpieczeństwa zarówno w regionie, jak i dla całego Sojuszu.

ZAKOŃCZENIE

Przedmiotowa dysertacja jest zwieńczeniem kilkuletnich badań i rozważań autora nad zapewnieniem bezpieczeństwa państwa poprzez rozwijanie jego odporności oraz stworzenia warunków do budowy narodowego systemu antydostępowego.

Zastosowane metody empiryczne oraz teoretyczne były właściwe w stosunku do przyjętych problemów badawczych. Także zweryfikowanie hipotez było możliwe dzięki wykorzystaniu spektrum metod badawczych. Istotny wpływ na całokształt niniejszej publikacji miało zaangażowanie wielu ekspertów z kraju i z zagranicy, co w konsekwencji przyczyniło się do uwiarygodnienia przeprowadzonych badań. Należy uznać, że uzyskane wyniki badań w pełni potwierdziły słuszność przyjętych hipotez.

Współczesne środowisko bezpieczne podlega ciągłej zmianie, co stwarza niepewność co do kierunku tych zmian. Kształtujący się nowy porządek światowy powoduje wiele zagrożeń i wyzwań. Problematyczne staje się nawet określenie źródła zagrożeń – czy będzie nim podmiot państwowy czy niepaństwowy? Z wysokim prawdopodobieństwem można określić jednak, że aktywność tego podmiotu będzie prowadzona w każdej zidentyfikowanej dotychczas domenie operacyjnej (ląd, wody, kosmos, przestrzeń powietrzna oraz cyberprzestrzeń), a także w tych, które nie są jeszcze określane jako operacyjne, a mają ogromny wpływ na kształtowanie postaw – np. w domenie kognitywnej.

Z dużym prawdopodobieństwem można założyć, że cechą charakterystyczną nowo ukształtowanego ładu światowego, z kilkoma dominującymi graczami, będzie ciągła rywalizacja w wielu wymiarach, np. gospodarczym, naukowym, ale także w militarnym. Wykorzystanie zdobyczy technologicznych przyczyni się do zwiększenia możliwości wywierania określonego wpływu i kształtowania pożądanych postaw. Takie zmiany mogą doprowadzić do ciągłego testowania systemu odpornościowego państwa i jego zdolności do radzenia sobie ze skutkami zagrożeń. Jednak z drugiej strony tworzą się pewne szanse dla rozwoju własnych zdolności wykorzystywanych do budowy narodowego systemu bezpieczeństwa.

Istotnym elementem budowy systemu bezpieczeństwa państwowego jest rozwijanie i budowanie nowych zdolności odpornościowych. Konieczność budowy i utrzymania odporności została dostrzeżona zarówno na szczeblu Sojuszu, jak i w poszczególnych państwach wchodzących w jego skład. Problematyka ta jest także dostrzegana w Polsce, która jest jednym z głównych podmiotów zaangażowanych w jej budowę na poziomie

NATO. Wzmocnienie odporności w poszczególnych państwach jest jednym z kluczowych wyzwań stojących przed Sojuszem. Suma pojedynczych zdolności powinna przełożyć się na zbiorowy system odporności NATO, które będzie odpowiednio przygotowane i zdolne do reagowania, odzyskiwania sił i adaptacji do nowych warunków. Pożądany stopień odporności wpływa na wytworzenie u przeciwnika przekonania o zwiększonych kosztach, a nawet bezcelowości działań zmierzających do realizacji założonych przez niego celów.

Budowa odpornego państwa to ciągła praca prowadzona przez wszystkie podmioty odpowiedzialne za jego bezpieczeństwo. Niezmiennym warunkiem jest ścisła koordynacja i synchronizacja wysiłków na rzecz tworzenia odporności, zarówno władz cywilnych, jak i wojskowych. Budowa odpornego państwa wymaga holistycznego podejścia, które umożliwi osiągnięcie zakładanych efektów. Istotnym problemem jest także odpowiednie zarządzanie wszelkimi komponentami mającymi wpływ na odporność i zdolność do współpracy w poszczególnych sektorach. Potencjał naukowo-badawczy oraz zdolność do adaptacji rozwiązań opracowanych poza granicami kraju pozwalają na implementację technologii umożliwiających budowę nowoczesnych systemów zwiększających odporność w poszczególnych obszarach funkcjonowania państwa.

Zdiagnozowany poziom odporności Polski wymaga zintensyfikowania działań zmierzających do jego wzrostu. Istnieją obszary, w których należy podjąć zdecydowane działania naprawcze. Zabezpieczenie dostaw energii, zarządzanie przemieszczaniem się ludności czy zapewnienie wydolności służby zdrowia to te sektory, w których należy podjąć zdecydowane kroki w celu wyeliminowania istniejących słabości.

System odporności państwa powinien być systematycznie sprawdzany i testowany. Przygotowanie odpowiedniego programu szkoleń, ćwiczeń weryfikujących aktualny stan przygotowania państwa powinien być obiektem szczególnego zainteresowania decydentów. Ciągła weryfikacja, zgrywanie poszczególnych elementów, zarówno w układzie narodowym, jak i koalicyjnym pozwoli na uzyskanie spójnego i rzeczywistego obrazu aktualnej sytuacji. Należy zaznaczyć, że problem ten jest dostrzegany w Sojuszu oraz w Polsce. Dotychczasowe działania pozwalają mieć nadzieję na podtrzymanie tego trendu w przyszłości.

Jednym z determinantów pozwalających na wzmocnienie i utrzymanie na wysokim poziomie komponentów wpływających na odporność Polski może być wykreowanie systemu uniemożliwiającego lub przynajmniej mocno utrudniającego dostęp do naszego państwa we wszystkich wymiarach – zarówno fizycznym, jak i niefizycznym.

Dotychczasowe próby podejmowane przez niektóre kraje wskazują na potencjalne możliwości w nich się kryjące. Systemy antydostępowe pozwalają na wytworzenie poczucia nieopłacalności prowadzenia działań ofensywnych oraz drastycznego wzrostu kosztu ich realizacji. Szczególnego wymiaru nabiera system zbudowany przez Chiny, którego pokonanie lub przełamanie wiąże się z wysokimi kosztami zarówno osobowymi, jak i materialnymi dla Stanów Zjednoczonych. Dotychczas przeprowadzone symulacje i ćwiczenia dowodzą tego niezbicie.

Warto zatem rozważyć ideę budowy takiego systemu w Polsce. Z dotychczasowych wniosków płynących z wojny w Ukrainie, jak również z działań Hamasu w październiku 2023 r., należy uznać za konieczne podjęcie wszelkich działań uniemożliwiających przeciwnikowi zajęcie chociażby części terytorium naszego kraju. Z drugiej strony warto również zwrócić uwagę, że zniszczenie lub znaczne uszkodzenie elementów infrastruktury krytycznej może doprowadzić do znacznego osłabienia możliwości państwa, w tym jego zdolności do zabezpieczenia podstawowych potrzeb. Ponadto pod znakiem zapytania stoi kwestia czasu niezbędnego do odbudowy i powrotu do stanu pierwotnego. Dlatego też istotną kwestią jest zbudowanie zdolności do w miarę niezakłóconego funkcjonowania wszystkich elementów państwa wpływających na jego odporność.

Jednym z kluczowych elementów budowy tych zdolności jest umiejętność obserwacji i wyciągania właściwych wniosków z dotychczasowych działań i zdarzeń. Dlatego też zasadne jest podjęcie działań związanych z budową pełnowymiarowego systemu uniemożliwiającego lub przynajmniej znacząco utrudniającego przeciwnikowi dokonanie agresji na obszar Polski. Taki system mógłby odgrywać również rolę swoistego elementu odstraszającego oraz tworzącego warunki do powstania dylematu związanego z oszacowaniem kosztów w stosunku do zakładanych zysków. Powinien on wytworzyć przekonanie, że naruszenie chronionego obszaru jest niezwykle utrudnione, wiąże się z wysokimi kosztami, a jednocześnie umożliwia obrońcy podjęcie działań odwetowych już na terytorium przeciwnika.

System antydostępowy powinien posiadać zdolności do oddziaływania we wszystkich zidentyfikowanych pięciu domenach, jak również w domenie kognitywnej. Tylko taki spójny i skoordynowany system ma szansę stać się rzeczywistą przeszkodą dla przeciwnika. Umiejętność wykorzystania atutów takiego systemu będzie z pewnością jedną z istotnych kwestii rozważanych podczas jego budowy. Ponadto należy się liczyć z koniecznością wprowadzenia zasadniczych zmian w procesie planowania, organizowania i prowadzenia

działań. Będzie to zapewne powiązane także z potrzebą przeprowadzenia zmian mentalnych w społeczeństwie, a także przeglądu i dostosowania szeregu aktów prawnych. Taki system będzie wymagał także wykorzystania nowoczesnych technologii oraz sztucznej inteligencji.

Główne pytania, które można sobie zadać, dotyczą kosztów oraz możliwości realizacji takiego projektu przez Polskę. Zdaniem autora wiele dotychczas realizowanych programów może być wykorzystanych do budowy narodowego systemu antydostępowego. Oczywiście należałoby rozważyć pozyskanie także innych zdolności, które pozwoliłyby na zwiększenie obecnych możliwości. Do kosztów należałoby także doliczyć te związane z koniecznością przeszkolenia osób zaangażowanych w funkcjonowanie takiego systemu. Z całą pewnością sumaryczne koszty byłyby znaczne. Dlatego też warto rozważyć przekonanie innych partnerów do budowy w regionie wspólnego systemu uniemożliwiającego przeciwnikowi dostęp do ich przestrzeni. Wydaje się, że szanse na taką inicjatywę są spore, biorąc pod uwagę chociażby wzrost zagrożenia ze strony Rosji, ale również podmiotów niepaństwowych. Sytuacja ta spowodowała zmianę mentalności w krajach europejskich, co może wpłynąć na podjęcie decyzji o rozpoczęciu prac związanych z budową regionalnego systemu antydostępowego.

Zdaniem autora rozwiązanie problemów badawczych oraz pozytywna weryfikacja hipotez dają argumenty do stwierdzenia, że cele badań zostały w pełni osiągnięte. Autor zbadał i dokonał oceny systemu odpornościowego Polski. Przeprowadził także diagnozę, która pozwoliła zidentyfikować obszary o stosunkowo dobrym jego poziomie, jak również te, które wymagają podjęcia zdecydowanych środków zaradczych. Na podstawie oceny odporności Polski oraz po przeanalizowaniu założeń będących podstawą funkcjonowania dotychczas istniejących systemów antydostępowych zaproponował koncepcję utworzenia spójnego, narodowego systemu. Z tych względów dysertacja ma charakter nie tylko poznawczy, ale także utylitarny. Zawarte w rozprawie wnioski i propozycje mogą przyczynić się do podjęcia działań zwiększających poziom odporności państwa oraz budowy systemu, który zapewniałby możliwość niezakłóconego funkcjonowania państwa. Dysertacja wnosi zatem wkład w zwiększenie bezpieczeństwa naszego państwa oraz poczucia bezpieczeństwa jego obywateli.

Obok poczucia spełnienia naukowego autor widzi potrzebę prowadzenia dalszych badań nad systemem odporności Polski. W przedmiotowej dysertacji skupiono się tylko na siedmiu obszarach wpływających na tę odporność. Autor zdaje sobie sprawę, że nie wyczerpuje to w pełni problematyki. Wynika to przede wszystkim ze świadomości własnej

niedoskonałości, a co za tym idzie potrzeby weryfikacji zaproponowanych rozwiązań w toku dalszych, pogłębionych badań naukowych. Powinny one obejmować przede wszystkim kompleksową ocenę odporności państwa we wszystkich aspektach jego funkcjonowania. Badaniami należy objąć również systemy militarne wpływające na utrzymywanie gotowości cywilnej. Będą one z całą pewnością wymagały dostępu do dokumentów niejawnych i niedostępnych dla ogółu społeczeństwa. Istnieje także potrzeba powołania zespołu ekspertów, z szerokimi uprawnieniami, do przygotowania kompleksowej oceny stanu odporności Polski. Kolejnym obszarem badań mogą być możliwości zintegrowania obecnie rozwijanych programów zwiększających poziom nasycenia środkami walki we wspólny system uniemożliwiający przeciwnikowi penetrację obszaru państwa w każdej z domen.

Autor wyraża także nadzieję, że przeprowadzone w niniejszej dysertacji rozważania, zarówno teoretyczne, jak i empiryczne, posłużą nie tylko do studiowania i zgłębiania podjętej problematyki, ale zostaną również uwzględnione w pracach koncepcyjnych nad budową odpornego państwa.

SPIS TABEL I RYSUNKÓW

Spis tabel

Spis rysunków

BIBLIOGRAFIA

Książki i artykuły

1. Acosta J., Chandra A., Madrigano J., *An Agenda to Advance Integrative Resilience Research and Practice. Key Themes From a Resilience Roundtable*, RAND Corporation, Santa Monica 2017.
2. *Allied Joint Doctrine*, AJP-01(F), NSO 2022.
3. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2016.
4. Bartosiak J., *Koncepcja operacyjna wojny powietrzno-morskiej na zachodnim Pacyfiku*, Fundacji Republikańskiej, Warszawa 2012.
5. Błażewicz Z., *Strategiczne środowisko bezpieczeństwa – istota i ewolucja*, [w:] M. Kubiński (red.), *Siły Zbrojne RP w procesie budowy narodowego potencjału odstraszania*, Akademia Obrony Narodowej, Warszawa 2015.
6. Bonds T. M., Predd J. B., Heath T. R., Chase M. S., Johnson M., Lostumbo M. J., Bonomo J., Mane M., Steinberg P. S., *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?*, RAND Corporation, Santa Monica 2017.
7. *Charakterystyka obszarów przygranicznych przy zewnętrznej granicy Unii Europejskiej na terenie Polski, Podmioty Gospodarki Narodowej w 2015 r.*, opracowanie sygnalne, Główny Urząd Statystyczny, Warszawa 2016.
8. Ciastoń R., Czulda R., Gruszczyński J., Kowalski M., Smura T., *Obrona przeciwrakietowa na świecie – wnioski dla Polski*, Fundacja im. Kazimierza Pułaskiego, Warszawa 2016.
9. Ciekanowski Z., Nowicka J., Wyrębek H., *Bezpieczeństwo państwa w obliczu współczesnych zagrożeń*, Wyd. Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2016.
10. Cieśla S., *State Resilience*, [w:] *Strategic and Operational Challenges in the (Post) Pandemic World*, Globstate Vol. 4, Issue 1, Wyd. CDiS SZ, Bydgoszcz 2022.
11. Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i obronności państwa,* Wyd. Akademii Podlaskiej, Siedlce 2009.
12. Cieślewicz S., Skiba A., Reczkowski R., *Współczesne bezpieczeństwo transatlantyckie – implikacje dla Sił Zbrojnych RP*, Wyd. CDiS SZ, Bydgoszcz 2018.
13. *Concepts and Dilemmas of State Building in Fragile Situations From Fragility to Resilience*, OECD, Paryż 2008.
14. Czaja J., *Teoretyczne i praktyczne podstawy budowy kultury strategicznej w Polsce*, [w:] *Strategia bezpieczeństwa narodowego Polski*, red. J. Gryz, Wyd. PWN, Warszawa 2013.
15. Czupryński A., *Obszar oraz obiekt i przedmiot badań w naukach o bezpieczeństwie*, [w:] *Nauki o bezpieczeństwie. Wybrane problemy badań,* Wyd. CNBOP-PIB, Józefów 2017.
16. Czupryński, A., Wiśniewski, B., Zboina, J, *Nauki o bezpieczeństwie. Wybrane problemy badań*, Wyd. CNBOP-PIB, Józefów 2017.

17. Dalsjö R., Berglund C., Jonsson M., *Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, Swedish Defence Research Agency FOI, Sztokholm 2019.

18. Dawidczyk, A., Swoboda, P., *Projektowanie celów polityki bezpieczeństwa na użytek strategii bezpieczeństwa narodowego,* [w:] „Bezpieczeństwo narodowe" – kwartalnik BBN, nr 42/2023, Wyd. BBN, Warszawa 2023.

19. Domagała, A., Kautsch, M., Kulbat, A., Parzonka, K., *Exploration of estimated emigration trends of polish health professionals*, [w:] „International Journal of Environmental Research and Public Health", nr 19(2)/2022, Oxford Academic, Oxford 2022.

20. *Encyklopedia Gospodarki Materiałowej*, Państwowe Wydawnictwo Ekonomiczne, Warszawa 1989.

21. Focus 2023, *The Norwegian Intelligence Service's assessment of current security challenges*, Norwegian Intelligence Service, Oslo 2023.

22. *Gaining and Maintaining Access: An Army–Marine Corps Concept*, version 1.0, U.S. Army and U.S. Marine Corps, Fort Eustis 2012.

23. Gajewski Z. (opr.), *Migranci ekonomiczni w Polsce. Fakty i mity*, [w:] „Magazyn THINKTANK", nr 36, Warszawa 2020.

24. Gasztold A., *Zagrożenia hybrydowe dla infrastruktury krytycznej*, [w:] „Biuletyn Kwartalny", Rządowe Centrum Bezpieczeństwa, lipiec 2021.

25. Giles K., Boulegue M., *Russia's A2/AD Capabilities: Real and Imagined*, [w:] „The US Army War College Quarterly", vol. 49, nr 1-2, Carlisle 2019.

26. *Global Risk Report 2023 – 18th Edition*, World Economic Forum, Geneva 2023.

27. *Global Trends 2040. A more contested World*, The National Intelligence Council, Waszyngton 2021.

28. Głowiak K., *Stosunek Polaków do przyjmowania uchodźców przed i w warunkach europejskiego kryzysu migracyjnego*, [w:] „Historia i Polityka", nr 35(42)/2021, Wyd. UMK, Toruń 2021.

29. Gotkowska J., *NATO 2030: na drodze do nowej strategii*, Ośrodek Studiów Wschodnich, Warszawa 2021.

30. Gryz J., *Bezpieczeństwo państwa. Władza – polityka – strategia,* Wyd. Akademii Obrony Narodowej, Warszawa 2013.

31. Grzeszak J., Leśniewicz F., Śliwowski P., Święcicki I., *Pandenomics: Zestaw narzędzi fiskalnych i monetarnych w dobie kryzysów,* Polski Instytut Ekonomiczny, Warszawa 2020.

32. Herdt C., Zublic M., *Baltic Conflict: Russia's Goal to Distract NATO?,* CSIS, Waszyngton 2022.

33. Hooker R. D., *How to Defend the Baltic States*, The Jamestown Foundation, Waszyngton, 2019.

34. *Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*, U.S. Department of Defense , Waszyngton 2019.

35. Joint Doctrine Note 1-18, *Strategy*, Joint Chiefs of Staff, Waszyngton 2018.

36. *Joint Operational Access Concept (JOAC)*, U.S. Department of Defense, Waszyngton, 2012.

37. Juchniewicz M., *Innowacje w logistyce łańcucha dostaw żywności*, [w:] „Zeszyty naukowe Uniwersytetu Szczecińskiego", nr 875. Problemy Zarządzania, Finansów i Marketingu, nr 41, t. 2, Szczecin 2015.

38. Jureńczyk Ł., *Polityczno-wojskowy wymiar rywalizacji między Chińską Republiką Ludową a Stanami Zjednoczonymi Ameryki w XX i XXI wieku*, „Annales, Sectio K. Politologia" 2017, vol. 24, nr 2.

39. Kacperska E., Kacprzak M., Kmieć D., Król A., Łukasiewicz K., *Migracje międzynarodowe w Europie. Trendy, problemy, wyzwania*, Wydawnictwo SGGW, Warszawa 2019.

40. Kalinowski R., *Od gotowości cywilnej do zarządzania kryzysowego,* [w:] „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa", nr 4, Poznań 2013.

41. Kelly T. K., Gompert D. C., Long D., *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression*, RAND Corporation, Santa Monica 2016.

42. Kitler W., *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*, Wyd. AON, Warszawa 2011.

43. *Komunikat z badań: Opinie o integracji i działaniach UE nr 90/22,* CBOS, Warszawa 2022.

44. *Komunikat z badań: Polacy wobec wojny na Ukrainie i ukraińskich uchodźców*, CBOS, nr 101/22, Warszawa 2022.

45. *Komunikat z badań: Stosunek do NATO i obecności wojsk sojuszniczych w Polsce* nr *40/22*, CBOS, Warszawa 2022.

46. Kotarbiński T., *O pojęciu metody*, PWN, Warszawa 1975.

47. Koziej S., Wołkowicz F., *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, Wyd. AON, Warszawa 1998.

48. Kozłowska-Burdziak M., *Warunki bezpieczeństwa żywnościowego Polski (ze szczególnym uwzględnieniem województwa podlaskiego)*, „Optimum. Economic Studies", nr 3(97), Białystok 2019.

49. Koźmiński A. K., Piotrowski W., W *Zarządzanie. Teoria i praktyka,* PWN, Warszawa 2002.

50. Kozub M., *Konflikty społeczno-militarne XXI wieku. Strategiczne środowisko bezpieczeństwa do roku 2030*, Wyd. Akademii Obrony Narodowej, Warszawa 2010.

51. Kozub M., *Myśleć strategicznie o bezpieczeństwie przyszłości*, Wyd. Akademii Obrony Narodowej, Warszawa 2013.

52. Krajewski M., *O metodologii nauk i zasadach pisarstwa naukowego. Uwagi podstawowe*, Wyd. Uniwersytetu Śląskiego, Gliwice 2010.

53. Krepinevich, A. F., Watts, B. D., *The last warrior: Andrew Marshall and the shaping of modern American defense strategy*, Nowy Jork 2015.

54. Lutyński J., *Metody badań społecznych*, Łódzkie Towarzystwo Naukowe, Łódź 2000.

55. Lorenz W., *NATO wobec zmian klimatu – oczekiwania i możliwości*, [w:] „Biuletyn PISM", nr 215 (2147), 28 października 2020, Warszawa 2020.

56. Łobocki M., *Metody i techniki badań pedagogicznych,* Kraków 2003.

57. *Mały słownik języka polskiego,* PWN, Warszawa 1968.

58. *Mały rocznik statystyczny Polski 2021*, GUS, Warszawa 2021.

59. Maslow, A., *Motywacja i osobowość*, Warszawa 2010.

60. Masten, A. S., *Ordinary magic: Resilience in development*. Guilford Publications, Nowy Jork 2015.

61. Mastro O. S., *China Anti-access/Area Denial (A2AD) Capabilities: Is the U.S. Rebalancing Enough?*, [w] Natter W. H., Brooks J., *American Strategy and Purpose: Reflections on Foreign Policy and National Security in an Era of Change*, Createspace Independent Publishing Platform, 2014.

62. Mattioli R., Levy-Bencheton C., *Methodologies for the identification of Critical Information Infrastructure assets and services*, ENISA, Heraklion 2014.

63. Meyer-Minnemann L., *Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience*, [w:] Hamilton D. (red), *Forward Resilience Protecting Society in an Interconnected World*, Johns Hopkins University, Waszyngton 2016.

64. Mokrzycki J., Reczkowski R., Cieśla S., *Analiza środowiska bezpieczeństwa w perspektywie 2035 roku*, Wyd. CDiS SZ, Bydgoszcz 2020.

65. Nalaskowski S., *Metody badań i diagnozowania edukacji*, UMK-MEN, Toruń 2000.

66. *NATO CD&E Handbook*, Edition 2, ACT, luty 2021.

67. *NATO Warfighting Capstone Concept* (NWCC), ACT, Norfolk 2023.

68. *Ocena stanu rozwoju badań i użytkowania przestrzeni kosmicznej – raport za 2021 rok*, Polska Agencja Kosmiczna, Gdańsk 2022.

69. *Office of Technology Assessment: Ballistic Missile Defense Technologies*. University Press of Pacific, Honolulu 2002.

70. *Operacje reagowania kryzysowego spoza artykułu 5* – DD/3.4(A), CDiS SZ**,** Bydgoszcz 2013.

71. Perkins W. A., *Component Integration Challenges presented by Advanced Layered Defence Systems (A2/AD)*, [w:] „The Three Swords Magazine", nr 33/2018, Stavanger 2018.

72. Permal S., *China's Military Capability and Anti-access Area-denial Operations*, [w:] „Maritime Affairs: Journal of the National Maritime Foundation of India", vol. 10, 2014, Issue 2, London 2014.

73. Pieter J., *Zarys metodologii pracy naukowej*, PWN, Warszawa 1975.

74. Pilch T., Bauman T., *Zasady badań pedagogicznych*, Wyd. Akademickie Żak, Warszawa 2001.

75. *PLA Aerospace Power: A primer on trends in China's Military Air, Space, and Missile Forces*, US Air University, Montgomery 2017.

76. Popisil J., Kuehn F.P., *The Resilient State: New Regulatory Modes in International Approaches to Statebuilding?*, University of Edinburgh „Research Paper Series", nr 2016/03, Edinburgh 2016.

77. Reach C., Geist E., Doll A., Cheravitch J., *Competing with Russia Militarily Implications of Conventional and Nuclear Conflicts*, RAND Corporation, Santa Monica 2021.

78. Reczkowski R., *Implikacje geopolityczne i wojskowe dla Polski i SZ RP z zaangażowania Federacji Rosyjskiej (FR) w konflikt domowy w Syrii*, Wyd. CDiS SZ, Bydgoszcz 2016.

79. Reczkowski R., Lis A., *Cognitive Warfare: what is our actual knowledge and how to build state resilience?* [w:] „The Total Defence 21st Century.com – Building a Resilient Society: Theory and Practice Journal", red. M. Lasoń, M. Klisz, L. Elak, nr 3/2022, Wyd. Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2022.

80. Reczkowski R., Raubo J.M., Jureńczyk Ł., Podraza A., Turowski P., *Świat po pandemii Covid-19 z wojną na Ukrainie w tle. Perspektywa rozwoju ładu światowego i środowiska bezpieczeństwa do 2040 roku. Wyzwania dla bezpieczeństwa Polski. Tom 1 – wymiar polityczny i geopolityczny*, Wyd. CDiS SZ, Bydgoszcz 2023.

81. Redo M., Siemiątkowski P., *Zewnętrzne bezpieczeństwo finansowe państwa*, Uniwersytet Mikołaja Kopernika, Toruń 2017.

82. Roepke W. D., Thankey H., *Odporność – pierwsza linia obrony*, NATO Reviev, 2019.

83. Rose S., Borchert O., Mitchell S., Connelly S., *Zero Trust Architecture*, NIST, Waszyngton 2020.

84. Ruszel M., *Świat po pandemii COVID-19 w wymiarze ekonomicznym i zasobów naturalnych.* Raport z webinarium przeprowadzonego w dniu 18 marca 2021 roku przez Centrum Doktryn i Szkolenia Sił Zbrojnych w ramach kampanii analiz środowiska bezpieczeństwa pk. „Nowe Urządzenie Polskie – NUP 2X35", Bydgoszcz 2021.

85. Sawyer R., *Chinese Strategic Power: Myths, Intent, and Projections*, [w:] „Journal of Military and Strategic Studies", vol. 9, nr 2, 1 styczeń 2007.

86. Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge 2017.

87. Shaughnessy J., Zechmeister J., Zechmeister E., Rucińska M., *Metody badawcze w psychologii*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2002.

88. *Słownik Języka Polskiego*, t.1, Wyd. PWN, Warszawa 1978.

89. *Słownik terminów i definicji NATO*, NSO, Bruksela 2017.

90. Smura T., *Modernizacja Chińskiej Armii Ludowo-Wyzwoleńczej*, [w:] „Pułaski Policy Paper", nr 3, Warszawa 2021.

91. Sondel J., *Słownik łacińsko-polski dla prawników i historyków*, TAiWPN Universitas, Kraków 2006.

92. Stańczyk J., *Środowisko bezpieczeństwa państwa w ujęciu strategicznym*, [w:] „Studia Bezpieczeństwa Narodowego", nr 1/2015, vol. 7, Wyd. WAT, Warszawa 2015.

93. Stańczyk J., *Środowisko bezpieczeństwa w ujęciu międzynarodowym*, [w:] „Rocznik Bezpieczeństwa Narodowego", nr 2/2018, vol. 12, Wrocław 2018.

94. *Strategia 5G dla Polski*, Ministerstwo Cyfryzacji, Warszawa 2018.

95. *Strategia Zrównoważonego Rozwoju Transportu do 2030 roku*, Ministerstwo Infrastruktury, Warszawa 2019.

96. *Strategic Foresight Report 2023*, European Commission, Bruksela 2023.

97. Świderska I., Lebiecki P., *Stan bezpieczeństwa budowli piętrzących wodę w Polsce na koniec 2009 roku*, Materiał z XXV Konferencji Naukowo-Technicznej, Międzyzdroje 24-27 maj 2011.

98. Szczudlik J., *„Nowa era" w polityce obronnej Chin*, [w:] „Biuletyn PISM", nr 122 (1870), Warszawa 2019.

99. *The NATO Alternative Analysis Handbook*, Edition 2, ACT 2017.

100. *The Strategic Foresight Analysis Report 2017*, Allied Command Transformation, Norfolk 2017.

101. Tomaszewski T., *Wstęp do psychologii*, PWN, Warszawa 1963.

102. Turbiville G. H., Kipp J. W., Mendel W. M., *The Changing Security Environment,* [w:] „Military Review", Fort Leavenworth 1997.

103. Vego M., *Joint Operational Warfare: Theory and practice*, Naval War College, 2007.

104. Vego M., *Soviet Naval Tactics*, Naval Institute Press, Annapolis, 1992.

105. Wiejski P., *Zielony ład dla Europy. Uwarunkowania, narzędzia, perspektywy*, Instytut Spraw Publicznych, Warszawa 2019.

106. Wiśniewski B. (red.), *Bezpieczeństwo w teorii i badaniach naukowych*, Wyd. Wyższa Szkoła Policji, Szczytno 2011.

107. *Wsparcie przez państwo-gospodarza* – DD-4.5(B), wer. 2, wyd. elektroniczne, CDiS SZ, Bydgoszcz 2019 r.

108. Zaczyński W., *Praca badawcza nauczyciela*, PWN, Warszawa 1995.

109. *Zdrowie i ochrona zdrowia w 2020 r*., Główny Urząd Statystyczny, Warszawa−Kraków 2021.

110. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego: koncepcje – struktury – funkcjonowanie*, Wyd. Naukowe Scholar, Warszawa 1999.

111. Zięba R., Zając J., *Budowa zintegrowanego systemu bezpieczeństwa narodowego Polski – Ekspertyza,* Warszawa 2010.

112. *Zmiany klimatu a bezpieczeństwo międzynarodowe* (PL Version), European Commission, Bruksela 2015.

113. Zybertowicz, A., *Cyber kontra real. Cywilizacja w techno-pułapce*, Wyd. Nowej Konfederacji, Warszawa 2022.

Akty normatywne i prawne

1. *Karta Narodów Zjednoczonych oraz Statut Międzynarodowego Trybunału Sprawiedliwości*, Departament Informacji ONZ, 1956.
2. *Polityka energetyczna Polski do 2040 roku*, Ministerstwo Klimatu i Środowiska, Załącznik do uchwały nr 22/2021 Rady Ministrów z dnia 2 lutego 2021 r.
3. *Procedura postępowania na wypadek wystąpienia zdarzenia z dużą liczbą poszkodowanych*, Ministerstwo Zdrowia, Warszawa, 2020.
4. *Traktat Północnoatlantycki*, Waszyngton 1949.
5. Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny, Dz.U. 2022 poz. 655.
6. Ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, Dz.U. 2022 poz. 583.
7. Ustawa z dnia 20 lipca 2017 r. – Prawo wodne, Dz.U. 2017 poz 1566.

Raporty instytucji państwowych

1. *Raport o stanie rynku telekomunikacyjnego w Polsce w 2021 r.*, Urząd Komunikacji Elektronicznej, Warszawa 2022 r.
2. *Raport. Nadzór nad stanem technicznym i stanem bezpieczeństwa wodnych budowli piętrzących*, Najwyższa Izba Kontroli, Warszawa 2016.
3. *Raport: System ochrony zdrowia w Polsce – stan obecny i pożądane kierunki zmian,* Najwyższa Izba Kontroli, Warszawa 2019 r.
4. *Raport: Utrzymanie i eksploatacja sieci wodociągowych w miastach,* Najwyższa Izba Kontroli, Warszawa 2018.
5. *Raport: Zapewnienie bezpieczeństwa zaopatrzenia w wodę dużych aglomeracji miejskich na wypadek wystąpienia sytuacji kryzysowych,* Najwyższa Izba Kontroli, Warszawa 2017.

Źródła internetowe

1. *14 NATO Allies and Finland agree to boost European air defence capabilities*, NATO 2022, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/news_208103.htm?SelectedLocale=en [dostęp: 27.03.2023].
2. *2023 Military Strenght Ranking*, Global Firepower 2023, pobrano z lokalizacji: https://www.globalfirepower.com/countries-listing.php [dostęp: 31.03.2023].
3. *5G: sieci telekomunikacyjne nowej generacji*, gov.pl, 17.04.2017, pobrano z lokalizacji: https://www.gov.pl/web/5g/korzysci [dostęp: 06.12.2022].
4. L. Aronhime, A. Cocron (red.), *Countering cognitive warfare: awareness and resilience*, [w:] NATO Review, 20.05.2021, pobrano z lokalizacji: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html [dostęp: 18.02.2022].

5. Bartman K., *Polsce nie grozi głód, ale potrzebne są rezerwy żywności. Takie, które nie "wyparują" z magazynów*, Money.pl, 28.03.2022, pobrano z lokalizacji: https://www.money.pl/gospodarka/polsce-nie-grozi-glod-ale-potrzebne-sa-rezerwy-zywnosci-takie-ktore-nie-wyparuja-z-magazynow-6750665549720480a.html [dostęp: 05.12.2022].

6. Bednarz P., *Czy Polska może odciąć się dziś od ropy? Możliwości są, ale skutki nagłego odcięcia byłyby trudne do zniesienia*, Business Insider, 28.05.2022, pobrano z lokalizacji: https://businessinsider.com.pl/finanse/odciecie-sie-od-dostaw-rosyjskiej-ropy-jakie-beda-skutki-dla-polski/kc0sdn0 [dostęp: 26.11.2022].

7. Behrendt P., *Chińska flota zielonych wód*, Nowa Konfederacja, 06.06.2017, pobrano z lokalizacji: http://www.nowakonfederacja.pl/chinska-flota-zielonych-wod [dostęp: 21.10.2021].

8. Bełdowicz, A., *Eksport rosyjskiej ropy spada, Polska wciąż w pierwszej 10. Importerów,* Rzeczpospolita, 16.11.2022, pobrano z lokalizacji: https://klimat. rp.pl/energia/art37426311-eksport-rosyjskiej-ropy-spada-polska-wciaz-w-pierwszej-10-importerow [dostęp: 27.11.2022].

9. Boulègue M., *Russia's Military Posture in the Arctic Managing Hard Power in a 'Low Tension' Environment*, Chatham House, 2806.2019, pobrano z lokalizacji: https://www.chathamhouse.org/sites/default/files/2019-06-28-Russia-Military-Arctic_0.pdf [dostęp: 04.05.2022].

10. Braw E., *What Finland Can Offer NATO,* Foreign Policy, 14.042022, pobrano z lokalizacji: https://foreignpolicy.com/2022/ 04/14/ what-finland-can-offer-nato/ [dostęp: 21.01.2023].

11. Chang F. K., *Sweden's Importance to NATO's Defense of the Baltics*, Foreign Policy Research Institute, 28.09.2017, pobrano z lokalizacji: https://www.fpri.org/2017/09/swedens-importance-natos-defense-baltics/ [dostęp: 23.06.2022].

12. *China's Massive Belt and Road Initiative*, Council on Foreign Relations, 2.02.2023, pobrano z lokalizacji: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative [dostęp: 24.11.2021].

13. Cieślik E., *Walka o metale ziem rzadkich*, Forsal.pl, 15 kwiecień 2022, Pobrano z lokalizacji: https://forsal.pl/gospodarka/artykuly/8400146,walka-o-metale-ziem-rzadkich.html [dostęp: 21.11.2022].

14. *CIO Survey 2020 Report: Everything changed. Or did it?*, KPMG, 18.11.2020, pobrano z lokalizacji: https://assets.kpmg/content/dam/kpmg/pl/pdf/2020/11/pl-Harvey-Nash-KPMG-CIO-survey-2020.pdf [dostęp: 25.01.2021].

15. Ciślak J., *Armia rosyjska – armia agresora: Wojsko w Obwodzie Kaliningradzkim [RAPORT]*, Defence24, 30.04.2022, pobrano z lokalizacji: https://defence24.pl/sily-zbrojne/armia-rosyjska-armia-agresora-wojsko-w-obwodzie-kaliningradzkim-raport [dostęp: 04.05.2022].

16. Ciszak P., *Trwa wyścig o gaz. Gigant straszy Europę. „Zagrożenia nie można zlekceważyć"*, money.pl, 23.04.2023, pobrano z lokalizacji: https://www.money.pl/gielda/trwa-wyscig-o-gaz-gigant-straszy-europe-zagrozenia-nie-mozna-zlekcewazyc-6889460731505216a.html [dostęp: 27.05.2023].

17. *Civil preparedness*, NATO 2021, pobrano z lokalizacji: https://www.nato.int/cps/en/ natohq/topics_49158.htm [dostęp 26.07.2021].

18. *Commitment to enhance resilience*, NATO 2016, pobrano z lokalizacji: https://www.nato.int/cps/en/natohq/official_texts_ 133180.htm?selected Locale=en [dostęp: 27.07.2021].

19. *Deklaracja Szczytu NATO w Madrycie*, 29.06.2022, pobrano z lokalizacji: https://www.prezydent.pl/aktualnosci/wypowiedzi-prezydenta-rp/wystapienia/deklaracja-szczytu-nato-w-madrycie, 56384 [dostęp:19.08.2022].

20. *Deklaracja Szczytu NATO w Walii*, 5.09.2014, pobrano z lokalizacji: https://www.bbn.gov.pl/ftp/dok/Deklaracja%20szczytu%20walijskiego.pdf [dostęp: 25.02.2020].

21. Dura M., *Rosyjskie rakietowe baterie nadbrzeżne: do obrony i szantażu politycznego [KOMENTARZ]*, Defence24, 20.01.2022, pobrano z lokalizacji: https://defence24.pl/ sily-zbrojne/rosyjskie-rakietowe-baterie-nadbrzezne-do-obrony-i-szantazu-politycznego-komentarz [dostęp: 04.05.2022].

22. *Encyklopedia PWN*, pobrano z lokalizacji: https://encyklopedia.pwn.pl/haslo/odpornosc; 3949963.html [dostęp: 23.07.2021].

23. *European Sky Shield Initiative gains two more participants*, NATO, 15.02.2023, pobrano z lokalizacji: https://www.nato.int/cps/en /natohq/news_211687.htm [dostęp: 18.03.2023].

24. *Europol-INTERPOL Report on Migrant Smuggling Networks.* Europol.eu, 17.05.2016, pobrano z lokalizacji: https://www.europol.europa.eu/publications-events/publications/ europol-interpol-report-migrant-smuggling-networks#downloads [dostęp: 14.12.2021].

25. Fidziński M., *Ilu mamy lekarzy w Polsce (oprócz tego, że za mało)? Odpowiedź nie jest prosta*, Gazeta,pl, 27.08.2021, pobrano z lokalizacji: https://next.gazeta.pl/next/7,151003, 27500831,ilu-mamy-lekarzy-w-polsce-oprocz-tego-ze-za-malo-odpowiedz.html [dostęp: 23.11.2022].

26. *Finland scores highly for cybersecurity: Digital Nomads*, Helsinki Times, 24.08.2022, pobrano z lokalizacji: https://www.helsinkitimes.fi/world-int/22088-finland-scores-highly-for-cybersecurity-digital-nomads.html [dostęp: 22.02.2023].

27. Forsberg R., Kähkönen A-M., Moyer J. C., *Finland's Contributions to NATO: Strengthening the Alliance's Nordic and Arctic Fronts*, Wilson Center, 8.11.2022, pobrano z lokalizacji: https://www.wilsoncenter.org/article/finlands-contributions-nato-strengthening-alliances-nordic-and-arctic-fronts [dostęp: 14.01.2023].

28. Friediger J., *HCC 2021: brakuje lekarzy specjalistów? A może mamy za dużo specjalizacji?, rynekzdrowia.pl*, 12.06.2021, pobrano z lokalizacji: https://www.rynekzdrowia.pl/ Nauka/HCC-2021-brakuje-lekarzy-specjalistow-A-moze-mamy-za-duzo-specjalizacji, 222357,9.html [dostęp: 29.09.2021].

29. Gawęda M., *Rosyjskie bastiony A2/AD (ANALIZA)*, Defence 24, 29.07.2018, pobrano z lokalizacji: https://defence24.pl/sily-zbrojne/rosyjskie-bastiony-a2ad-analiza [dostęp: 20.05.2023].

30. Georgieva K., *No lost generation: can poor countries avoid the Covid trap?* The Guardian, 29.09.2020, pobrano z lokalizacji: https://www.theguardian.com/business/2020/sep/29/ covid-pandemic-imf-kristalina-georgieva [dostęp: 25.01.2022].

31. Gotkowska J., *Germany's European Sky Shield Initiative*, Ośrodek Studiów Wschodnich, 14.10.2022, pobrano z lokalizacji: https://www.osw.waw.pl/en/publikacje/analyses/ 2022-10-14/germanys-european-sky-shield-initiative [dostęp: 24.02.2023].

32. http://www.budowle.pl/budowla,liniamaginota [dostęp: 16.03.2017].

33. http://www.budowle.pl/budowla,wielki-mur-chinski [dostęp: 16.03.2017].

34. https://www.bbn.gov.pl/ftp/dok/01/DoktrynaFederacjiRosyjskiej.pdf [dostęp: 04.10.2021].

35. https://www.oecd.org/coronavirus/en/data-insights/number-of-medical-doctors-and-nurses?utm_term=PAC& utm_medium=social&utm_source=twitter&utm_content= [dostęp: 20.09.2021].

36. https://www.populationof.net/pl/poland/ [dostęp: 30.05.2023].

37. Jakóbik W., *Ile jeszcze ropy Polska sprowadza z Rosji? (ANALIZA)*, Biznes Alert, 07.02.2023, pobrano z lokalizacji: https://biznesalert.pl/polska-ile-sprowadza-ropa-rosja-import-sankcje-pkn-orlen/ [dostęp: 30.05.2023].

38. Jankowicz M., *Iranian-made drones cost as little as $20,000 to make but up to $500,000 to shoot down, a growing concern in Ukraine, report says*, Business Insider, 04.01.2023, pobrano z lokalizacji: https://www.businessinsider.com/suicide-drones-much-cheaper-launch-than-shoot-down-ukraine-nyt-2023-1 [dostęp: 16.05.2023].

39. Janoś K., *Umowa na Patrioty wreszcie podpisana. Zobacz, ile kosztuje bezpieczeństwo i co dają nam te rakiety*, Money.pl, 28.03.2018, pobrano z lokalizacji: https://www.money.pl/gospodarka/wiadomosci/artykul/mon-blaszczak-modernizacja-patriot-offset,151,0, 2401943.html [dostęp: 21.10.2022].

40. Jones S. G., *Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare*, CSIS Briefs, 1.06.2022, pobrano z lokalizacji: https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare [dostęp: 20.09.2022].

41. Kacprzak I., *Sondaż: Polacy chcą, by uchodźcy wojenni partycypowali w kosztach życia*, Rzeczpospolita, 25.11.2022, pobrano z lokalizacji: https://www.rp.pl/ spoleczenstwo/art37484871-sondaz-polacy-chca-by-uchodzcy-wojenni-partycypowali-w-kosztach-zycia [dostęp: 29.11.2022].

42. Knuth K., *The term "Resilience" is everywhere – but what does it really mean?*, ENSIA, 07.05.2019, pobrano z lokalizacji: https://ensia.com/articles/what-is-resilience/ [dostęp: 26.07.2021].

43. Kozieł H., *Metale ziem rzadkich. Wąskie gardło cywilizacji cyfrowej*, Rzeczpospolita, 18.02.2022, pobrano z lokalizacji: https://www.rp.pl/plus-minus/art35711091-metale-ziem-rzadkich-waskie-gardlo-cywilizacji-cyfrowej [dostęp: 27.11.2022].

44. Köylüoğlu B., *Modern Dunyanin Jeopolitik Faylari*, Strateji & Finans, 18.04.2021, pobrano z lokalizacji: https://www.stratejivefinans.com/modern-dunyanin-jeopolitik-faylari/ [dostęp: 30.12.2021].

45. Lade S., *What is resilience*, Stockholm Resilience Centre, 19.02.2015, pobrano z lokalizacji: https://www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html [dostęp: 21.07.2021].

46. LaGrone S., *CNO Richardson: Navy Shelving A2/AD Acronym*, USNI News, 3.10.2016, pobrano z lokalizacji: https://news.usni.org/2016/10/03/cno-richardson-navy-shelving-a2ad-acronym [dostęp: 25.07.2021].

47. LaGrone S., *Pacific Commander Davidson Asks Congress to Fund 'Regain the Advantage' Plan Aimed at China*, USNI News, 18.04.2019, pobrano z lokalizacji: https://news.usni.org/2019/04/18/pacific-commander-davidson-asks-congress-to-fund-regain-the-advantage-plan-aimed-at-china [dostęp: 14.11.2021].

48. Lesiecki R., *Wisła i Patrioty za 4,75 mld dolarów. Kontrakt podpisany*, Defence 24, 28.03.2018, pobrano z lokalizacji: https://defence24.pl/polityka-obronna/wisla-i-patrioty-za-475-mld-dolarow-kontrakt-podpisany [dostęp: 27.12. 2022].

49. Lisowska K., *MON o wojskowej służbie zdrowia: tworzymy plan także na wypadek wojny*, Puls Medycyny, 27.10.2022, pobrano z lokalizacji: https://pulsmedycyny.pl/mon-o-wojskowej-sluzbie-zdrowia-tworzymy-plan-takze-na-wypadek-wojny-1167938 [dostęp: 24.11.2022].

50. Lurka K., *Czy medycy uciekają z kraju?*, Menedżer Zdrowia, 2.06.2022, pobrano z lokalizacji: https://www.termedia.pl/mz/Czy-medycy-uciekaja-z-kraju-,47293.html [dostęp: 03.12.2022].

51. *Madrid Summit Declaration*, NATO, 29.06.2022, pobrano z lokalizacji: https:// www.nato.int/cps/en/natohq/ official_texts_ 196951.htm [dostęp: 20.09.2022].

52. Matyasik G., *Jak wygląda polska odporność?,* Infosecurity24, 4.04.2023, pobrano z lokalizacji: https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [dostęp: 10.09.2023].

53. Mein C., *How US Patriot missile systems could impact the Russia-Ukraine war*, The Hill, 21.12.2022, pobrano z lokalizacji: https://thehill.com/policy /defense/ 3777058-how-us-patriot-missile-systems-could-impact-the-russia-ukraine-war/ [dostęp: 10.01.2023].

54. Mróz, A., *Polska nadal importuje tani gaz LPG z Rosji*. Rzeczpospolita, 24.02.2023, pobrano z lokalizacji: https://moto.rp.pl/tu-i-teraz/art38017441-polska-nadal-importuje-tani-gaz-lpg-z-rosji [dostęp: 28.05.2023].

55. *Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries*, ACT, 29.07.2022, pobrano z lokalizacji: https://www.act.nato.int/articles/multi-domain-operations-out-pacing-and-out-thinking-nato-adversaries [dostęp: 20.12.2022].

56. *NATO 2022 Strategic Concept*, NATO, 29.06.2022, pobrano z lokalizacji: https://www.nato.int/ nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf [dostęp: 27.07.2022].

57. *NATO's Concept for the Deterrence and Defence in the Euro-Atlantic Area* Reaffirmed, OPS, 21.10.2021, pobrano z lokalizacji: https://operationnels.com/2021/10/21/natos-concept-for-deterrence-and-defence-in-the-euro-atlantic-area- reaffirmed/ [dostęp: 04.01. 2022].

58. *No Option is Excluded – Using Wargaming to Envision a Chinese Assault on Taiwan*, TRADOC, 1.07.2021, pobrano z lokalizacji: https://madsciblog.tradoc.army.mil/337-no-option-is-excluded-using-wargaming-to-envision-a-chinese-assault-on-taiwan/ [dostęp: 30.12.2021].

59. *Odpowiedź UE na wyzwanie migracji,* Parlament Europejski, 17.07.2017, pobrano z lokalizacji: https://www.europarl.europa.eu/news/pl/headlines/society/20170629STO786 29 /odpowiedz-ue-na-wyzwanie-migracji [dostęp: 27.11.2022].

60. Paulewicz-Bazała P., *Las w obliczu zagrożenia suszą*, Wodne Sprawy, 13.07.2023, pobrano z lokalizacji: https://wodnesprawy.pl/las-w-obliczu-zagrozenia-susza-kryzys-klimatyczny-p/ [dostęp: 16.08.2023].

61. Perry B., *Entering the Bear's Lair: Russia's A2/AD Bubble in the Baltic Sea*, The National Interest, 20.09.2016, pobrano z lokalizacji: https://nationalinterest.org/blog/the-buzz/entering-the-bears-lair-russias-a2-ad-bubble-the-baltic-sea-17766 [dostęp: 09.10.2021].

62. *Polityka migracyjna Polski – diagnoza stanu wyjściowego*, Departament Analiz i Polityki Migracyjnej MSWiA, 15.12.2020, pobrano z lokalizacji: https://www.gov.pl/ attachment/2a65e5d4-52c5-40ac-ada9-3b3f988f86b9 [dostęp: 27.11.2022].

63. Przybytek-Pawlik J., *Średnia wieku pielęgniarek to 53 lata. Szefowa NIPiP alarmuje: "Pielęgniarka idzie na emeryturę i umiera"*, rynekzdrowia.pl, 25.10.2021, pobrano z lokalizacji: https://www.rynekzdrowia.pl/Polityka-zdrowotna/Srednia-wieku-pielegniarek-to-53-lata-Szefowa-NIPiP-alarmuje-quot-Pielegniarka-idzie-na-emeryture-i-umiera-quot-Polityka-zdrowot,226026,14.html [dostęp: 17.08.2022].

64. *Resilience and Article 3*, NATO, 2.08.2020, pobrano z lokalizacji: https://www.nato.int/ cps/en/natohq/topics_132722.htm, 2021 [dostęp: 26.07.2021].

65. Schmitt E., *US Lending Support to Baltic States Fearing Russia*, The New York Times, 1.01.2017, pobrano z lokalizacji: https://www.nytimes.com/2017/ 01/01/us/politics/us-baltic-russia.html) [dostęp: 25.04.2022].

66. Sierak A., *Polska może mieć zaskakujące źródła metali ziem rzadkich*, wnp.pl, 21.04.2023, pobrano z lokalizacji: wnp.pl. https://www.wnp.pl/gornictwo/polska-moze-miec-zaskakujace-zrodla-metali-ziem-rzadkich,701550.html [dostęp: 22.05.2023].

67. Simon L., *Demysttifying the A2/AD Buzz,* War on the Rocks, 4.01.2017, pobrano z lokalizacji: https://warontherocks.com/ 2017/ 01/demystifying-the-a2ad-buzz/ [dostęp: 24.07.2021].

68. *Służba zdrowia potrzebuje zastrzyku finansowego. Dorzucimy się wszyscy*, Money.pl, 22.04.2021, pobrano z lokalizacji: https://www.money.pl/gospodarka/sluzba-zdrowia-potrzebuje-zastrzyku-finansowego-dorzucimy-sie-wszyscy-6631700437547968a.html [dostęp: 02.10.2022].

69. *Surowce na okupowanych przez Rosję terenach Ukrainy warte 12 bln dolarów [Raport],* Bankier.pl., 11.08.2022, pobrano z lokalizacji: https://www.bankier.pl/wiadomosc/ Surowce-na-okupowanych-przez-Rosje-terenach-Ukrainy-warte-12-bln-dolarow-Raport-8388889.html [dostęp: 21.11.2022].

70. *Systemy infrastruktury krytycznej*, Rządowe Centrum Bezpieczeństwa, pobrano z lokalizacji: https://www.gov.pl/web/rcb/systemy-infrastruktury-krytycznej [dostęp: 12.12.2022].

71. Szałaj K., *Czy Polska jest rzeczywiście samowystarczalna żywnościowo? Sprawdzamy!*, Tygodnik Poradnik Rolniczy, 17.03.2022, pobrano z lokalizacji: https://www.tygodnik-rolniczy.pl/articles/wojna-w-ukrainie-rolnictwo/czy-polska-jest-samowystarczalna-zywnosciowo-sprawdzamy-czego-nam-brakuje/ [dostęp: 19.11.2022].

72. Szopa M., *Defence24 Day: Operacje wielodomenowe w Siłach Zbrojnych RP*, Defence24, 27.05.2022, pobrano z lokalizacji: https://defence24.pl/polityka-obronna/defence24-day-operacje-wielodomenowe-w-silach-zbrojnych-rp [dostęp: 28.12.2022].

73. *The National Resilience Strategy. A Call for Evidence*, Cabinet Office, 13.07.2021, pobrano z lokalizacji: https://assets.publishing.service.gov.uk/ government/uploads/ system/uploads/ attachment_data/file/1001404/Resilience_Strategy_-_Call_for_Evidence.pdf [dostęp: 22.07.2023].

74. Turecki K., *Atlantic Council: NATO musi się przygotować na rosyjską inwazję*, Onet.pl, 25.07.2016, pobrano z lokalizacji: https://wiadomosci. onet.pl/tylko-w-onecie/atlantic-council-nato-musi-sie-przygotowac-na-rosyjska-inwazje /44ceqr [dostęp: 10.03.2020].

75. Wall C., Wegge N., *The Russian Arctic Threat. Consequences of the Ukrainian War*, CSIS 2023, pobrano z lokalizacji: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-01/230125_Wall_RussianArcticThreat_0.pdf?VersionId=e8h73TdoOUjdJO3Y4nOTc4 [dostęp: 21.02.2023].

76. Wills S., *Kaliningrad: Impregnable Fortress or „Russian Alamo"?*, CNA, 15.05.2023, pobrano z lokalizacji: https://www.cna.org/our-media/indepth/2023/05/ kaliningrad-impregnable-fortress-or-russian-alamo [dostęp: 25.06.2023].

77. *Wstępny szacunek produktu krajowego brutto w 1 kwartale 2023 r.*, Główny Urząd Statystyczny, 31.05.2023, Pobrano z lokalizacji: https://stat.gov.pl/obszary-tematyczne/ rachunki-narodowe/kwartalne-rachunki-narodowe/wstepny-szacunek-produktu-krajowego-brutto-w-1-kwartale-2023-roku,3,83.html [dostęp: 31.05. 2023].

78. *Wojny kognitywne: niszczenie odporności społeczeństwa*, Centrum Badań Polityki Europejskiej, 05.05.2023, pobrano z lokalizacji: https://cbpe.pl/2023/05/05/wojny-kognitywne-niszczenie-odpornosci-spoleczenstwa/ [dostęp: 24.07.2023].

79. Zaborski M., *Gen. Skrzypczak o bateriach Patriot: Kupiliśmy bezpieczeństwo polityczne i „parasol" na pół Warszawy*, RMF FM, 28.03.2018, pobrano z lokalizacji: https://www.rmf24.pl/tylko-w-rmf24/popoludniowa-rozmowa/news-gen-skrzypczak-o-bateriach-patriot-kupilismy-bezpieczenstwo-,nId,2562969#crp_state=1 [dostęp: 12.01.2023].

80. Zaniewicz M., *Perspektywy uniezależnienia się UE od rosyjskiego gazu*, PISM, 28.04.2022, pobrano z lokalizacji: https://www.pism.pl/publikacje/perspektywy-uniezaleznienia-sie-ue-od-rosyjskiego-gazu [dostęp: 27.11.2022].

ZAŁĄCZNIKI

Załącznik 1.

WYNIKI BADAŃ OPINII EKSPERTÓW – BUDOWA I UTRZYMANIE ODPORNOŚCI

Kwestionariusz wywiadu

I. Cel wywiadu

Celem wywiadu jest zbadanie opinii oraz poglądów dotyczących problematyki związanej z budowaniem i utrzymaniem odporności.

II. Tematyka i problemy

1. Pana zdaniem, na czym polega istota odporności państwa? Jak można ją zdefiniować?
2. Jakimi cechami, Pana zdaniem, powinno charakteryzować się odporne państwo?
3. Jakie potencjalne zagrożenia dla odporności państwa mógłby Pan zidentyfikować?
4. W jaki sposób, Pana zdaniem, należy budować odporność państwa?
5. Jak oceniłby Pan obecny stopień odporności Polski na zidentyfikowane wcześniej zagrożenia?

III. Odpowiedzi na problemy – protokoły z przeprowadzonych wywiadów

Protokół wywiadu nr 1

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Sztabie Generalnym WP

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

Istota odporności przejawia się w zdolności państwa do przeciwdziałania zagrożeniom a także szybkiego powrotu do normalnego funkcjonowania po powstałej sytuacji kryzysowej.

Odpowiedź 2.

Do zasadniczych cech wpływających na fakt, że dane państwo jest odporne należą przede wszystkim sprawność podejmowania decyzji, jasne i sprawdzane procedury działania. Istotnym problem jest wprowadzenie właściwego podziału kompetencji.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń dla odporności państwa należą te związane z działalnością podmiotów zewnętrznych, mające na celu destabilizację sytuacji w kraju.
b. Z drugiej strony, dużą uwagę należy zwrócić na zagrożenia wewnętrzne, do których należy zaliczyć słabą świadomość klasy politycznej oraz społeczeństwa w zakresie rozpoznawania i zrozumienia zagrożeń.

Odpowiedź 4.

a. Budowa odpornego społeczeństwa jest zadaniem, którego realizacja musi przebiegać w długim okresie. Nie jest to zagadnienie, które można podnieść na wyższy poziom w ciągu kilku czy kilkunastu miesięcy. To z pewnością proces wieloletni i wymagający współpracy wielu podmiotów.
b. Budowa odpornego państwa powinna zacząć się od edukacji społeczeństwa, rozpoczętej już w szkole podstawowej. Należy także dążyć do właściwie uporządkowanej i przejrzystej struktury społeczeństwa, w której każdy obywatel ma przypisane swoje zadania w zależności od zajmowanej pozycji i posiadanego zakresu działania.

Odpowiedź 5.

a. Ocena obecnego stopnia odporności Polski obarczona jest brakiem właściwej wiedzy w poszczególnych jej segmentach.
b. W mojej ocenie stopień odporności jest niski z uwagi na brak jasnych i czytelnych procedur oraz powolne tempo podejmowanych decyzji. Na taką ocenę wpływa także brak zrozumienia przez społeczeństwo realnych zagrożeń. Ponadto zbyt powolne jest tempo modernizacji (przebudowy) państwa (w tym wojska i innych służb mundurowych).

Protokół wywiadu nr 2

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Sztabie Generalnym WP

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa to uporządkowany system norm, procedur oraz środków pozwalających na identyfikację, a następnie przeciwdziałanie zagrożeniom dla bezpieczeństwa państwa.
b. System powinien być oparty na określonych i akceptowalnych progach ryzyka, których zniwelowanie wymaga działań w wielodomenowym środowisku ukierunkowanych na przywrócenie lub wzmocnienie stanu pierwotnego.

Odpowiedź 2.

a. Odporne państwo cechuje się zdolnością do osiągnięcia synergii w zakresie bezpieczeństwa państwa poprzez dedykowane służby, w tym siły zbrojne oraz społeczeństwo.
b. Odporne państwo opiera się na świadomości społecznej, zaufaniu do organów władzy przy jednoczesnym sprawnym funkcjonowaniu aparatu państwa.

Odpowiedź 3.

a. Jednym z głównych zagrożeń dla odporności jest niespójne prawo oraz uregulowania dotyczące funkcjonowania poszczególnych elementów państwa.
b. Kolejnym istotnym zagrożeniem jest nieświadome społeczeństwo o dużej podatności na propagandę i dezinformację.
c. Istotnym problemem jest brak ciągłości lub wysoka zmienność w obszarze polityki zagranicznej państwa.
d. Kolejnym zagrożeniem jest nieprzygotowanie lub niewykształcenie szerokich grup społecznych (z elementów aparatu państwa) do realizacji zadań w ramach ogólnokrajowego kryzysu.

Odpowiedź 4.

a. Budowa odpornego społeczeństwa powinna rozpocząć się od właściwej edukacji w celu zwiększenia świadomości szerokiego kręgu społeczeństwa odnośnie faktycznej sytuacji w kraju i regionie.
b. Kolejnym krokiem powinno być przygotowanie instytucji, które nie funkcjonują na co dzień w ramach organizacji aparatu bezpieczeństwa (np. szkoły), do realizacji zadań w ramach kryzysu.
c. Istotnym zagadnieniem jest także skoordynowane działanie w ramach komunikacji strategicznej w państwie.

Odpowiedź 5.

a. Stopień odporności oceniam jako dostateczny. Poprawa poziomu odporności wymaga wprowadzenia szeregu rozwiązań, pozwalających na skuteczne przeciwdziałanie zagrożeniom w długiej perspektywie.

Protokół wywiadu nr 3

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Operacyjnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istotę odporności można określić, jako zdolność do całkowitego przeciwdziałania negatywnym zdarzeniom lub zminimalizowania skutków w przypadku wystąpienia negatywnych zdarzeń.

Odpowiedź 2.

a. Odporne państwo powinno cechować się rozwiniętym, scentralizowanym systemem I&W (ang. *Indicators and Warnings*) ponad układem militarnym i pozamilitarnym.
b. Kolejną istotną cechą jaką powinno charakteryzować się odporne państwo, jest posiadanie zdolności do rozpoznawania prowokacji.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń zaliczyłbym skupienie się na partyjnych interesach w polityce, zamiast realizacji przedsięwzięć zgodnych z interesami państwa. Jednocześnie zauważam brak systemowych rozwiązań na rzecz budowania odporności pomiędzy resortami.
b. Zwróciłbym także uwagę na polaryzację społeczno-kulturową w Polsce i jednoczesny brak wykształconego egalitaryzmu.
c. Do istotnych zagrożeń należy zaliczyć także brak zaufania do władzy i manipulowanie obywatelami. W mojej opinii wszystkie zagrożenia, które zidentyfikowałem, wyrastają z jednego „pnia" związanego z systemem władzy.

Odpowiedź 4.

a. Moim zdaniem należy zwrócić uwagę na przygotowanie świadomego społeczeństwa, które nie byłoby podatne na propagandę, fake newsy oraz manipulacje.

b. Dlatego też zdecydowanie podkreśliłbym znaczenie edukacji dla budowy takiego społeczeństwa.

Odpowiedź 5.

a. Moim zdaniem trudno jest dokonać jednoznacznej oceny odporności państwa bez dostępu do wielu danych, z których znaczna część jest niejawna. Z drugiej strony ciężko jest także ocenić przed wystąpieniem samego zdarzenia. W pewnych jednak obszarach, np. w wypadku wystąpienia zdarzeń (ataków) terrorystycznych, stopień odporności jest bardzo wysoki.

Protokół wywiadu nr 4

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Centrum Doktryn i Szkolenia SZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1, 2 i 4.

a. Uważam, że można kilka elementów pogrupować. W mojej opinii na pytania nr 1, 2 i 4 można udzielić jednej spójnej odpowiedzi.
b. Istnieje konieczność zdefiniowania pojęcia odporności państwa, tj. stworzenie definicji obejmującej odpowiedź na kwestię, czym jest odporność państwa wobec konkretnych zagrożeń. Inna reakcja będzie w celu zminimalizowania zagrożeń militarnych, a inna na działania innego rodzaju, np. prowadzenie dezinformacji i wpływu na świadomość społeczną.
c. Odporność powinna cechować się umiejętnością przewidywania zagrożeń zarówno tych zewnętrznych, jak i wewnętrznych oraz radzenia sobie z nimi przez państwo w sposób najbardziej efektywny. Innymi działaniami będą te w sferze militarnej, a innymi te, poza tym obszarem, a każde z nich będzie odrębnym zdarzeniem. Nie oznacza to jednak, że nie będzie zachodziło zjawisko wzajemnego przenikania się części z nich.
d. Odporność państwa powinna być spójnym systemem współdziałania w płaszczyźnie militarnej, społecznej i politycznej.
e. Stabilny system polityczny i rozwiązania prawne wspierają budowę odpornego państwa poprzez tworzenie wizerunku państwa jako wiarygodnego partnera przestrzegającego umów i norm prawnych. To także ciągłe rozwijanie świadomości społecznej w obszarze budowy silnego państwa.

Odpowiedź 3 i 5.

a. Problematyczne jest dokonywanie oceny stopnia odporności państwa bez zidentyfikowanych zagrożeń.
b. Budowę odporności państwa powinno się realizować adekwatnie do rozpoznanych oraz przewidywanych zagrożeń. Należałoby zwrócić uwagę,

że powinno się podchodzić do tego problemu w sposób holistyczny, uwzględniając zagrożenia militarne jak również pozamilitarne. Ciekawym problem pozostaje np. ocena stopnia odporności państwa czy wręcz jej budowa w warunkach nieprzewidywalności systemu prawnego i sądowniczego.

Protokół wywiadu nr 5

I. Dane ogólne eksperta

Stanowisko: specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istotę odporności państwa charakteryzuje zdolność państwa do niedopuszczenia do negatywnych skutków oddziaływania obcych mocarstw na sytuację w kraju.

Odpowiedź 2.

a. Odporne państwo powinno być suwerenne i charakteryzować się jednością narodową.
b. Odporne państwo powinno być konsekwentne w działaniu a obywatele powinni posiadać dużą świadomość, aby nie ulegać dezinformacji.
c. Powinna być zachowana ciągłość kierowania i dowodzenia państwem oraz siłami zbrojnymi w czasie pokoju, kryzysu i wojny.

Odpowiedź 3.

a. Jednym z głównych zagrożeń dla odporności państwa może być nieracjonalna polityka wewnętrzna prowadząca do wzrostu podziałów w kraju, a także różnorodne cele polityków.
b. Negatywny wpływ na odporność mogą mieć także sytuacje związane z niespójnymi aktami prawnymi, a także powszechna dezinformacja.

Odpowiedź 4.

a. Budowę odporności państwa powinno rozpocząć się od rozwoju sił militarnych przygotowanych do obrony kraju.
b. Kolejnym istotnym elementem wpływających na odporność jest rozwijanie współpracy cywilno-wojskowej na wszystkich szczeblach. Tylko właściwa koordynacja wspólnych działań może pozwolić na właściwe postrzeganie zagadnień związanych z rozbudową odpornością.
c. Istotnym elementem budowy odpornego państwa jest także wprowadzenie ograniczeń dla polityków, w szczególności w sytuacjach kryzysowych. Moim

zdaniem należałoby wprowadzić przepisy pozwalające, w odpowiednich sytuacjach, na pociągnięcie polityków do odpowiedzialności.

Odpowiedź 5.

a. Odnosząc się do zidentyfikowanych wcześniej zagrożeń, w mojej opinii, odporność Polski kształtuje się na poziomie średnim.

Protokół wywiadu nr 6

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Dowództwie Operacyjnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istotą odporności państwa jest właściwe zidentyfikowanie zagrożeń (w różnych obszarach) oraz umiejętnie przygotowany zestaw narzędzi (procedur), którymi państwo może oddziaływać na zagrożenia. Istnieje konieczność bieżącej analizy i umiejętności dostosowania się do sytuacji.

Odpowiedź 2.

a. Odporne państwo powinno charakteryzować się rzetelnością i umiejętnością właściwej oceny zagrożeń.
b. Państwo powinno zachowywać elastyczność w doborze środków do przeciwdziałania zagrożeniom.
c. Istotnym elementem jest posiadanie silnego mandatu przez wybraną w demokratycznych wyborach władzę.

Odpowiedź 3.

a. Brak samowystarczalności pod względem posiadania, wydobycia i produkcji surowców energetycznych, co wpływa na podatność na działalność innych państw.
b. Zaniechanie właściwego przygotowania szeregu obszarów związanych z zachowaniem odporności wynikająca ze „ślepej" wiary w moc sojuszy, takich jak UE czy NATO.
c. Brak dobrze przygotowanej dyplomacji, która może nie być w stanie właściwie reagować na zagrożenia inne niż bezpośrednia konfrontacja zbrojna.

Odpowiedź 4.

a. Rzetelnie określona racja stanu Polski, która pomimo zmian partii rządzących będzie właściwie rozumiana i kontynuowana ponad podziałami.

b. Kolejnym istotnym elementem wpływających na odporność jest dywersyfikacja dostaw źródeł energii.
c. Do istotnych cech zaliczyć można także uczestnictwo w różnego rodzaju sojuszach, które będą się wzajemnie balansować.

Odpowiedź 5.

a. Uważam, że obecnie jesteśmy przygotowani na poziomie dobrym, a zaplanowane na przyszłość działania powinny tę sytuację poprawić.

Protokół wywiadu nr 7

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Dowództwie Operacyjnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności państwa charakteryzuje się niezależnością od innych podmiotów narodowych, a także samowystarczalnością w obszarze surowców i zasobów energetycznych. Istota ta przejawia się także poprzez pełną niezależność gospodarczą i energetyczną. Ważnym elementem odporności jest zachowanie spójności partii politycznych w rządzeniu państwem. To także posiadanie i ciągły rozwój samowystarczalnego (w jak największym stopniu) przemysłu zbrojeniowego.

Odpowiedź 2.

a. Odporne państwo charakteryzować się może nieuleganiem wpływom państw trzecich. Istotnym czynnikiem jest także zbudowanie większości międzynarodowej do przeforsowania własnych koncepcji i idei. Taka sytuacja jest nierozerwalnie związana z posiadaniem silnej pozycji politycznej na arenie międzynarodowej.
b. Kolejną cechą odpornego państwa jest uzyskanie niezależności gospodarczej oraz budowa dobrze rozwiniętej gospodarki i przemysłu (w tym zbrojeniowego).

Odpowiedź 3.

a. Do najistotniejszych zagrożeń zaliczyłbym przede wszystkim:
    - wpływ państw trzecich,
    - zbyt duży szum informacyjny przekazywany w mediach,
    - zbyt duże uzależnienie od pomocy sojuszniczej,
    - brak możliwości samoobrony państwa.

Odpowiedź 4.

a. Dążenie do niezależności gospodarczej, technologicznej i finansowej. Korzystanie z własnych technologii, ich rozwój i inwestycje w te technologie.
b. Dążenie do spójności władz państwowych, jednomyślności w określaniu strategicznych celów. Uniezależnienie się od wpływów i interesów państw trzecich.

Odpowiedź 5.

a. W skali od 1 do 10 odporność Polski oceniam na 5. Ocena taka wynika ze zbyt dużej podatności na wpływy państw trzecich oraz dużej podatności obywateli na szum informacyjny przedstawiany w mediach.

Protokół wywiadu nr 8

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Sztabie Generalnym WP

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności państwa polega na zdolności do przeciwstawiania się wszystkim niekorzystnym działaniom, zjawiskom, sytuacjom, które mogą doprowadzić do jego destabilizacji.

Odpowiedź 2.

a. Odporne państwo charakteryzuje się skutecznym i egzekwowanym systemem prawnym, wysokim zaufaniem społeczeństwa do klasy politycznej oraz wysoką propaństwową świadomością społeczeństwa, a także sprawnym systemem edukacji.
b. Na odporność państwa wpływ mają także wiarygodne sojusze oraz sprawny i nieustannie doskonalony szeroko rozumiany system obronny państwa.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń, moim zdaniem, należą:
    - niezadowolenie społeczne,
    - duże podziały społeczne – polaryzacja,
    - niestabilność finansowa,
    - korupcja,
    - problemy związane z demografią,
    - zmiana klimatu.

Odpowiedź 4.

a. Ciągłość sprawowania władzy, która ma zaufanie społeczne.
b. Czytelny i skuteczny system sprawowania władzy i jego społeczna kontrola.
c. Sprawiedliwy system społeczny i prawny.
d. Nowoczesny system edukacji.

Odpowiedź 5.

a. Stan odporności państwa jest pozorny, wysoce niewystarczający.

Protokół wywiadu nr 9

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa to jego zdolność do przeciwdziałania, niedopuszczenia do wystąpienia zjawisk niekorzystnych, sytuacji kryzysowych. To także zdolność reagowania i działania po ewentualnym wystąpienia sytuacji kryzysowej – likwidacja skutków.

Odpowiedź 2.

a. Odporne państwo jest zdolne do przezwyciężania kryzysów, utrzymuje odporność elementów infrastruktury krytycznej i posiada sprawny system zarządzania kryzysowego.
b. Odporność jest kształtowana także poprzez utrzymywanie sprawnego systemu gotowości obronnej, stabilną, mało wrażliwą na oddziaływanie czynników zewnętrznych gospodarkę. Należy zwrócić uwagę na stabilność rządu i klarowny system prawny.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń należą:
    - działania informacyjne (dezinformacja),
    - terroryzm,
    - wrogie działania w cyberprzestrzeni,
    - zmiana klimatu,
    - polaryzacja społeczeństwa,
    - niż demograficzny,
    - zależność gospodarcza (finansowa),
    - brak bezpieczeństwa energetycznego,
    - niekontrolowane migracje.

Odpowiedź 4.

a. Odpowiednio szybka identyfikacja zagrożeń i właściwe zarządzanie ryzykiem. To także rozwijanie zdolności Sił Zbrojnych RP do realizacji zadań w zdefiniowanym środowisku wielodomenowym.
b. Budowanie odporności powinno być także powiązane z rozwojem gospodarczym, dążeniem do dywersyfikacji dostaw surowców energetycznych (w tym rozwój alternatywnych źródeł energii).
c. Budowanie i rozwój niewrażliwych na oddziaływanie przeciwnika systemów teleinformatycznych oraz systemów łączności (cyberbezpieczeństwo).

Odpowiedź 5.

a. Wydaje się, że prowadzone są działania zmierzające do podniesienia poziomu odporności państwa. Nie jestem w stanie ocenić stopnia odporności – ocena byłaby nieobiektywna.

Protokół wywiadu nr 10

I. Dane ogólne eksperta

Stanowisko: specjalista w Biurze Bezpieczeństwa Narodowego

Data wywiadu: 29.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności państwa to holistyczne podejście do bezpieczeństwa, które obejmuje wszystkie aspekty zagrożenia bezpieczeństwa i kontroluje proces samooceny oraz identyfikuje podatność na naruszenia odporności.

Odpowiedź 2.

a. Państwo powinno posiadać świadomość sytuacyjną oraz zdolności do wykrywania (ang. *capacity to dedect*) oraz odstraszania (ang. *capacity to deter*).

Odpowiedź 3.

a. Do istotnych zagrożeń zaliczyłbym różnego rodzaju grupy paramilitarne, tzw. NGO (ang. *non-governmental organization*) działające często jako agenci wpływu (fundacje, stowarzyszenia, społeczności on-line), a także partie i ugrupowania, których celem jest „rozbrojenie" atakowanego państwa i instytucji. Ma to na celu doprowadzenie do sytuacji, w której aktorzy wewnętrzni będą realizować cele wrogiej polityki zagranicznej.

Odpowiedź 4.

a. Państwo powinno dysponować pogłębioną oceną zagrożeń i posiadać dokładny przegląd aktorów, posiadanych przez nich środków, narzędzi i celów.

b. Państwo winno rozpoznawać i wdrażać katalog dobrych praktyk w zakresie przeciwdziałania zagrożeniom.

Odpowiedź 5.

a. Wcześniej zidentyfikowane zagrożenia i matryce oddziaływania adwersarzy nie są wystarczająco głęboko przeanalizowane. Brak jest jednostki odpowiadającej za STRATCOM, zarówno na szczeblu centralnym jak i na szczeblu resortów i instytucji. Zauważam potrzebę kontynuacji współpracy

wewnątrz administracji – wojska – służb. W dalszej kolejności zauważalny jest brak konfrontacji i skoordynowania własnych działań prowadzonych przez wszystkie instytucje państwa. Konieczne jest także określenie priorytetów w skali kraju i ich uporządkowanie w czasie.

Protokół wywiadu nr 11

I. Dane ogólne eksperta

Stanowisko: główny specjalista w Biurze Bezpieczeństwa Narodowego

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności to zdolność do podtrzymywania kluczowych funkcji państwa we wszystkich wymiarach pozamilitarnych oraz militarnych. To także zdolność podejmowania trafnych decyzji przez ośrodek polityczny, pomimo mitygowania procesu rządzenia przez deficyt odporności.

Odpowiedź 2.

a. Państwo powinno posiadać zdolności do utrzymania oraz odbudowy ciągłości kluczowych usług, aby podtrzymać funkcjonowanie państwa. To także zdolność do zachowania możliwości rządzenia i przeciwdziałania zagrożeniom.

Odpowiedź 3.

a. Potencjalne zagrożenia wynikają z deficytów określonych w wyniku analizy PMESII. Kluczowe zagrożenia hybrydowe dotyczą przestrzeni informacyjnej a realizowane są za pomocą np. social mediów, mediów tradycyjnych, a także działań w cyberprzestrzeni.

Odpowiedź 4.

a. Kluczem do budowy odporności państwa jest zablokowanie dezinformacji i podjęcie działań umożliwiających utrzymywanie świadomości społeczeństwa odpornej na działania strony przeciwnej.

Odpowiedź 5.

a. W obecnej chwili posiadamy znikomą zdolność do radzenia sobie ze skutkami dezinformacji, w szczególności w sektorze pozamilitarnym.

Protokół wywiadu nr 12

I. Dane ogólne eksperta

Stanowisko: specjalista w Dowództwie Operacyjnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa to zdolność do identyfikowania nieuchronnych zagrożeń oraz posiadanie skutecznych narzędzi (mechanizmów) neutralizacji (ograniczania) skutków wystąpienia tych zagrożeń i odtwarzania stanu wyjściowego.

Odpowiedź 2.

a. W tym przypadku należy zwrócić uwagę na posiadanie zdolności do identyfikacji, wykrywania i atrybucji zagrożeń.
b. Istotnym zagadnieniem jest także posiadanie zdolności do terminowego uruchamiania mechanizmów przeciwdziałania zagrożeniom.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń dla odporności państwa należałoby zaliczyć:
    - zagrożenia hybrydowe,
    - zagrożenia w obszarze ekonomicznym (energetyka, system finansowy),
    - zagrożenia w obszarze informacyjnym.

Odpowiedź 4.

a. Budowa odporności powinna koncentrować się na rozwoju mechanizmów pozwalających na wykrycie, identyfikację oraz atrybucję zagrożeń.
b. Kolejnym krokiem może być rozwój mechanizmów przeciwdziałania (neutralizacji) zagrożeń.

Odpowiedź 5.

a. W skali pięciostopniowej odporność Polski oceniam na 3. Zauważam potrzebę zwiększenia skuteczności mechanizmów przeciwdziałania zagrożeniom.

Protokół wywiadu nr 13

I. Dane ogólne eksperta

Stanowisko: szef oddziału NCBC[249]

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności to zdolność do zapewnienia, co najmniej minimalnego, akceptowalnego przez społeczeństwo, poziomu bezpieczeństwa i stabilności (przewidywalności) funkcjonowania państwa w ujęciu politycznym, ekonomicznym i militarnym.

Odpowiedź 2.

a. Posiadanie zdolności (a przez to odpowiednich organów państwa) do identyfikowania zagrożeń (również w perspektywie długofalowej) ich przeciwdziałaniu, łagodzeniu skutków zaistnienia oraz odtwarzaniu poziomu bezpieczeństwa poprzez specjalne plany i procedury.

Odpowiedź 3.

a. Do zasadniczych zagrożeń można zaliczyć niektóre sojusze państw trzecich, zawierane i rozwijane w sferach politycznych, militarnych i ekonomicznych. Z tymi zagrożeniami ściśle powiązane są zmiany przywództwa w innych państwach (nie tylko tych w bezpośrednim sąsiedztwie).
b. Do kolejnych kategorii zagrożeń (co wcale nie znaczy, że mniej ważnych) należy zaliczyć niekontrolowaną migrację, zmiany demograficzne czy też zmianę klimatu.

Odpowiedź 4.

a. Moim zdaniem budowę odpornego państwa należy rozpocząć od kształtowania odpowiedniego systemu prawnego. W dalszej kolejności powinno skupić się na budowaniu sojuszy lub dołączenia do nich.

Odpowiedź 5.

a. W skali od jeden do pięciu odporność Polski oceniam na 1.

[249] Obecnie Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni. Przyp. autora.

Protokół wywiadu nr 14

I. Dane ogólne eksperta

Stanowisko: szef wydziału w Sztabie Generalnym WP

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności państwa to zespół czynności realizowanych przez newralgiczne sektory państwa, przeciwdziałające możliwym wpływom na nie przez różne podmioty (zewnętrzne i wewnętrzne), a tym samym osłabiające je.

Odpowiedź 2.

a. Odporne państwo powinno cechować się:
   - posiadaniem własnych zasobów naturalnych,
   - niezależnością energetyczną,
   - silną gospodarką,
   - odpowiednią polityką zagraniczną,
   - silnymi siłami zbrojnymi,
   - zdolnością do radzenia sobie z konfliktami społecznymi,
   - zdolnością instytucji państwowych do funkcjonowania w warunkach niesprzyjających, a także posiadaniem przez nie zaufania społecznego,
   - ciągłością realizacji przyjętych programów strategicznych (w tym długoterminowych),
   - umiejętnością przeciwdziałania dezinformacji,
   - zamożnością społeczeństwa,
   - wysokim poziomem wykształcenia obywateli,
   - posiadaniem struktur organizacyjnych skutecznie przeciwdziałającym potencjalnym kryzysom.

Odpowiedź 3.

a. Zagrożenia, moim zdaniem, można podzielić na dwie grupy: wewnętrzne i zewnętrzne.
b. Do zagrożeń wewnętrznych zaliczyłbym przede wszystkim:

- słabo opłacane instytucje państwa,
- konflikty społeczne (w tym narodowościowe),
- niewydolność instytucji państwowych,
- prowadzenie dezinformacji,
- swoista „krótkowzroczność" elit rządzących (perspektywa 4-letnia).

c. Do kategorii zagrożeń zewnętrznych zaliczyłbym następujące:
   - terroryzm;
   - katastrofy naturalne, w tym epidemie,
   - niekontrolowane, wielkoskalowe migracje,
   - prowadzenie dezinformacji przez podmiot międzynarodowy,
   - „szantaż" energetyczny innego państwa.

Odpowiedź 4.

a. Budowa odpornego państwa oraz utrzymanie odporności na zakładanym poziomie wymagają wielkiego i nieustannego wysiłku zarówno wszystkich instytucji państwowych, jak i ogółu obywateli.
b. Należałoby się skupić na podjęciu wysiłków związanych z dywersyfikacją źródeł energii, budową potęgi ekonomicznej państwa i zwiększenia tym samym zamożności obywateli. To także określenie długoterminowych planów rozwoju państwa oraz ich przestrzeganie. Istotną kwestią jest także budowanie jedności społeczeństwa.
c. Kolejnymi przedsięwzięciami, związanymi z budową odpornego państwa są z całą pewnością zabiegi związane z przygotowaniem i szkoleniem instytucji państwa odpowiedzialnych za zarządzanie kryzysowe, a także posiadanie zdolności do przeciwdziałania dezinformacji, zarówno w wymiarze wewnętrznym, jak i zewnętrznym.

Odpowiedź 5.

a. Nie podejmuję się dokonania oceny odporności. Uważam jednak, że nadal należy podjąć szereg działań naprawczych w stosunku do wyspecyfikowanych wcześniej, przeze mnie, zagrożeń.

Protokół wywiadu nr 15

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istotą odporności państwa jest posiadanie zdolności do przeciwdziałania zagrożeniom płynności funkcjonowania wynikających z działania czynników zewnętrznych, kreowanych przez ludzi, wewnętrznych i naturalnych.

Odpowiedź 2.

a. Państwo powinno być zdolne do stworzenia i utrzymywania zorganizowanego systemu wykrywania i rozpoznania zagrożeń.
b. Ważnym czynnikiem charakteryzującym odporne państwo jest spójność społeczeństwa, którą to należy wykorzystać jako element przeciwdziałania zagrożeniom każdego rodzaju.
c. Każde odporne państwo powinno mieć zgromadzone rezerwy niezbędne do utrzymywania ciągłości funkcjonowania państwa (np. żywność, paliwa itd.). Jednocześnie powinien być rozwinięty i utrzymywany system ich systematycznego odnawiania.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń dla odporności państwa należą:
    - wpływ zewnętrznego podmiotu na podstawy funkcjonowania państwa,
    - czynniki naturalne powodujące klęski żywiołowe,
    - zagrożenia militarne i konflikt regionalny.

Odpowiedź 4.

a. Zorganizowanie systemu gromadzenia rezerw strategicznych zabezpieczających funkcjonowanie państwa to jedno z głównych zagadnień, od których powinno rozpocząć się dyskusję na temat budowy odpornego państwa.
b. Istotnym elementem wpływającym na budowę odpornego państwa jest stworzenie nowoczesnych i skutecznych w działaniu sił zbrojnych.

c. Budowanie obiektywnej świadomości społecznej, jako elementu wzmacniającego jedność narodową, powinno być jednym z naczelnych zadań każdej władzy. Społeczeństwo o dużym poczuciu jedności będzie zdolne do odpowiedniej i skutecznej reakcji na różnorodne zagrożenia.
d. Skuteczna polityka zagraniczna i umiejętność prowadzenia dialogu z państwami regionu oraz zdolność do współpracy międzynarodowej to główne filary państwa, które chce budować swoją odporność.
e. Odporne państwo to także takie, które potrafi zidentyfikować zagrożenia w odpowiednim miejscu i czasie.

Odpowiedź 5.

a. Obecnie obawiam się o odporność Polski z uwagi na powszechną dezinformację dotyczącą m.in. stanu wyjątkowego na granicy z Białorusią (moim zdaniem nieskutecznego), brak konsekwencji i klarowności w podejmowanych decyzjach, spór o elektrownię w Turowie. Te i inne sytuacje dowodzą, że nasza odporność jest zagrożona.

Protokół wywiadu nr 16

I. Dane ogólne eksperta

Stanowisko: oficer starszy w Centrum Operacji Powietrznych – Dowództwie Komponentu Powietrznego

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności zawiera się w posiadaniu zdolności do przeciwstawiania się kryzysom/problemom w każdym obszarze działalności państwa, przy minimalnych kosztach realizacji/niwelowania danego zagrożenia/kryzysu/sytuacji kryzysowej.

Odpowiedź 2.

a. Podstawową cechą jest posiadanie sprawnego, systematycznie sprawdzanego i odpornego na zakłócenia systemu bezpieczeństwa narodowego.
b. Odporne państwo powinno być niezależne energetycznie. Musi mieć zdywersyfikowane źródła dostaw surowców energetycznych. Jest to powiązane z prowadzaniem odpowiedniej polityki zagranicznej i utrzymywaniem sojuszy z różnymi podmiotami. Odporne państwo powinno mieć zdolność do atrybucji nowych technologii, co powiązane jest z posiadaniem wykształconej kadry naukowej i w ogólności wykształconego społeczeństwa.
c. Istotną cechą odpornego państwa jest także posiadanie zdolności do szybkiego oddziaływania na sytuacje kryzysowe, a także umiejętności do łagodzenia skutków wynikłych z zaistniałych wcześniej problemów.

Odpowiedź 3.

a. Do głównych zagrożeń należą:
    - terroryzm i przestępczość zorganizowana,
    - nielegalne, niekontrolowane migracje,
    - pandemie,
    - zagrożenia ekologiczne,

- dezinformacja,
- ekstremizm religijny.

Odpowiedź 4.

a. Budowanie struktur odpowiednich do zaplanowanych zadań powinno być podwaliną idei budowy odpornego państwa.
b. W dalszej kolejności należy zwrócić uwagę na potrzebę kreowania wysokiego morale i świadomości społeczeństwa, podnoszenia jakości systemu edukacji i inwestowania w nowe technologie.
c. Należy skupić się na budowie niezależności energetycznej.
d. Bardzo istotnym elementem wpływającym na budowę odpornego państwa, jest zdolność do kontynuacji polityki państwa przez kolejne pokolenia oraz umiejętność przystosowania się do zmieniających się warunków.

Odpowiedź 5.

a. Prezentujemy niewystarczającą zdolność do reagowania na sytuacje trudne/kryzysowe oraz niwelowania ich skutków.

Protokół wywiadu nr 17

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Sztabie Generalnym WP

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność to zdolność państwa do identyfikacji i przeciwdziałania zagrożeniom.

Odpowiedź 2.

a. Posiadanie zdolności do podejmowania właściwych decyzji w możliwie jak najkrótszym czasie to, moim zdaniem, jedna z głównych cech odpornego państwa.
b. System prawny państwa powinien być tak skonstruowany, aby zabezpieczał interesy państwa przed niepożądanymi działaniami czy też przed dającą się przewidzieć, zmieniającą się sytuacją geopolityczną.

Odpowiedź 3.

a. Do zasadniczych zagrożeń należą:
    - uzależnienie energetyczne, przemysłowe (w tym przemysł zbrojeniowy) od podmiotów zagranicznych (zarówno partnerów, jak i adwersarzy),
    - niekontrolowane migracje,
    - polityka klimatyczna,
    - dezinformacja.

Odpowiedź 4.

a. Odporność należy budować kompleksowo poprzez integrację wszystkich domen (PMESII). Budowę trzeba rozpocząć od identyfikacji zagrożeń, poprzez poszukiwanie rozwiązań, monitorowanie, implementację a kończąc na prowadzeniu obiektywnej oceny.

Odpowiedź 5.

a. Stan obecny – państwo podejmuje właściwe decyzje, aczkolwiek należy poszukiwać możliwości ich doskonalenia.

Protokół wywiadu nr 18

I. Dane ogólne eksperta

Stanowisko: specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność to umiejętność niepoddawania się działaniom adwersarzy czy czynnikom naturalnym oraz umiejętność odbudowy po wystąpieniu niekorzystnych zjawisk.

Odpowiedź 2.

a. Odporne państwo charakteryzuje się stabilnym, cieszącym się zaufaniem społecznym rządem oraz akceptowanym przez ogół społeczeństwa systemem prawnym.
b. Odporne państwo jest stabilne pod względem gospodarczym oraz społecznym. Społeczeństwo jest zjednoczone, a jego morale wysokie.
c. To także państwo zdolne do obrony swoich granic, posiadające nowoczesne siły zbrojne związane trwałymi sojuszami.

Odpowiedź 3.

a. Do zasadniczych zagrożeń należą:
    - terroryzm międzynarodowy i przestępczość zorganizowana,
    - niekontrolowane migracje,
    - zmiana klimatu.

Odpowiedź 4.

a. Budowa odporności zaczyna się od stworzenia systemu stabilnych i akceptowanych rządów, systemu gospodarczego niepodatnego na czynniki zewnętrzne. Generalnie, należy podjąć wszelkie działania zmierzające do budowy stabilnego państwa. Tylko takie państwo można nazwać odpornym.

Odpowiedź 5.

a. Dynamicznie zmieniająca się sytuacja geopolityczna wpływa na możliwość oceny odporności Polski. Moim zdaniem jest ona na stosunkowo niskim poziomie.

Protokół wywiadu nr 19

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Dowództwie Operacyjnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa to zdolność państwa (instytucji państwowych), gospodarki, sfery społecznej do przeciwdziałania skutkom zagrożeń zewnętrznych i wewnętrznych.

Odpowiedź 2.

a. Odporne państwo charakteryzuje się elastycznością instytucji państwowych, gospodarki na pojawiające się w szybkim tempie zmiany i szybką reakcją na te zmiany.
b. W odpornym państwie można zaobserwować ścisłą współpracę pomiędzy instytucjami państwowymi, w tym pomiędzy siłami zbrojnymi, policją i strażą graniczną a resortami cywilnymi.
c. Grupy społeczne i zawodowe nie są skonfliktowane, ich obraz nie jest zafałszowany, a społeczeństwo jest niespolaryzowane.

Odpowiedź 3.

a. Do zasadniczych zagrożeń zaliczyć należy:
    - brak długofalowej polityki asymilacji mniejszości narodowych, grup etnicznych i emigrantów,
    - umożliwianie tworzenia się na terytorium kraju organizacji, stowarzyszeń promujących kulturę, zwyczaje państw wrogo nastawionych do danego kraju. Te organizacje (stowarzyszenia) mogą być wykorzystywane do działań przeciwko danemu państwu,
    - zbyt długi okres wdrażania zmian będących odpowiedzią na symptomy zagrożenia.

Odpowiedź 4.

a. Budowę odporności należy rozpocząć od edukacji społeczeństwa, w tym sił zbrojnych w zakresie rozpoznania i reagowania na zagrożenia zewnętrzne oraz wewnętrzne. Proces ten powinien być obiektywny i dostosowany do poziomu percepcji odbiorcy.

Odpowiedź 5.

a. Obecny stan odporności Polski oceniam na 6 w skali od 1 do 10.

Protokół wywiadu nr 20

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Centrum Operacji Lądowych – Dowództwie Komponentu Lądowego

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa to zdolność do reagowania na sytuacje kryzysowe celem zapewnienia ciągłości realizacji zadań/obowiązków instytucji państwa.

Odpowiedź 2.

a. Cechą odpornego państwa powinien być spójny system prawny i sprawnie funkcjonująca administracja publiczna.
b. Społeczeństwo powinno być jednolite kulturowo i ideologicznie, o wysokim poziomie świadomości. Społeczeństwo takie powinno być zdolne do poświęceń na rzecz wspólnego dobra.
c. Państwo powinno harmonijnie rozwijać się gospodarczo oraz być zdolne do implementowania zdobyczy technologicznych.
d. Państwo powinno posiadać silną pozycję na arenie międzynarodowej i być zdolne do analizowania stanu bezpieczeństwa zewnętrznego i wewnętrznego, a w konsekwencji wprowadzania niezbędnych zmian.

Odpowiedź 3.

a. Do zasadniczych zagrożeń zaliczyć należy:
    - nielegalne migracje,
    - polaryzację społeczeństwa,
    - pandemie,
    - dezinformację,
    - uzależnienie od eksportu surowców energetycznych.

Odpowiedź 4.

a. Budowę odpornego państwa można realizować zgodnie z zaproponowanym algorytmem:
   - zdefiniowanie zagrożeń i określenie ich wpływu na funkcjonowanie państwa,
   - analiza kierunków rozwoju i trendów przyszłych kryzysów,
   - zdefiniowanie potrzeb niezbędnych do zapobiegania sytuacjom kryzysowym (oraz reakcji na te sytuacje),
   - określenie priorytetów działania w wyspecyfikowanych obszarach funkcjonowania państwa,
   - stworzenie warunków do realizacji określonych wcześniej działań,
   - ocena sprawności funkcjonowania systemu,
   - modyfikacja przyjętych założeń zgodnie z uzyskaną oceną.

Odpowiedź 5.

a. Stan odporności oceniam jako dostateczny.

Protokół wywiadu nr 21

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Wojsk Obrony Terytorialnej

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność to cecha i zdolność narodu do zatrzymania zewnętrznej presji, wpływów i ewentualnych ataków.

Odpowiedź 2.

a. Podstawowa cecha charakteryzująca odporne państwo to zjednoczone społeczeństwo o dużym poczuciu tożsamości narodowej.

Odpowiedź 3.

a. Założenia koncepcji Gierasimowa w sprawie prowadzenia i rozstrzygania konfliktów oraz realizacji celów w polityce międzynarodowej wskazują, na co powinniśmy zwrócić szczególną uwagę, tj. na konflikty wewnętrzne (każdego rodzaju, np. szczepionkowcy–antyszczepionkowcy, prokościelni–antykościelni itd.) prowadzące do polaryzacji społeczeństwa.
b. Kolejnym zidentyfikowaniem zagrożeniem jest potencjał protestów jako jeden z podstawowych środków osiągania celów.
c. Istotnym zagrożeniem jest także uzależnienie od gospodarki (wyspecjalizowane gałęzie) innych krajów.

Odpowiedź 4.

a. Jestem zdania, że warunkiem koniecznym w budowie odporności jest opracowanie założeń związanych z tzw. *Total Defence*, uświadomienie społeczeństwu celów i znaczenia podejmowanych działań, przekazywanie klarownego obrazu sytuacji bezpieczeństwa oraz zaangażowanie wszystkich graczy (cywilnych i wojskowych).

Odpowiedź 5.

a. W wielu kwestiach Polska odrobiła lekcję. Widoczny jest wzrost zainteresowania problemem odporności, a państwo podejmuje działania zmierzające do rozwoju obszarów istotnych z tego punktu widzenia. Z drugiej jednak strony uważam, że minimalizowany jest problem polaryzacji społeczeństwa, w którym dostrzegalne są głębokie podziały.

Protokół wywiadu nr 22

I. Dane ogólne eksperta

Stanowisko: wykładowca Akademii Wojsk Lądowych

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności określa zdolność danego systemu do przeciwstawienia się zagrożeniom, a w przypadku naruszenia ciągłości funkcjonowania do odbudowy stanu poprzedniego.

Odpowiedź 2.

a. Cechą charakterystyczną odpornego państwa jest jego zdolność do przetrwania wszelkich kryzysów oraz umiejętność odbudowy sektorów po wstrząsach lub upadku systemu. Kolejną cechą jest także posiadanie stabilnego systemu rządów z klarownym systemem prawnym.

Odpowiedź 3.

a. Zagrożenia można podzielić na: militarne, polityczne, ekonomiczne i społeczne. To oczywiście tylko kilka z nich, na których chciałbym się skupić. Wyspecyfikowane zagrożenia nie są zbiorem zamkniętym.
b. Do zagrożeń militarnych zaliczyłbym m.in.: budowę sił zbrojnych przez Rosję zdolnych w najbliższym czasie do przeprowadzenia agresji; wyścig zbrojeń; proliferacja broni masowego rażenia; zbrojne konflikty graniczne.
c. Zagrożenia polityczne to przede wszystkim: tworzenie się nowego porządku światowego, dążenie Rosji do restauracji poprzedniego imperium sowieckiego, „zagospodarowywanie" Afryki przez Rosję i Chiny.
d. Zagrożenia ekonomiczne – uzależnienie od surowców energetycznych, metali ziem rzadkich, wyczerpywanie się niektórych zasobów, niestabilny system finansowy spowodowany przez globalizację.
e. Zagrożenia społeczne – pandemie, zmiana klimatu (np. susze, powodzie), polaryzacja społeczeństw.

Odpowiedź 4.

a. Budowę odpornego państwa powinno się rozpocząć od stworzenia trwałego i stabilnego systemu prawnego.
b. W następnej kolejności należy podjąć działania zmierzające do podniesienia poziomu rozwoju gospodarczego kraju.
c. Przeprowadzenie obiektywnej oceny stanu odporności w zdefiniowanych obszarach.
d. Przystąpienie do realizacji zadań zmierzających do poprawy w ocenionych obszarach.

Odpowiedź 5.

a. Ocena stanu odporności jest zagadnieniem niezmiernie trudnym. Intuicyjnie mogę stwierdzić, że obecna sytuacja nie jest najlepsza. Uważam, że jest jeszcze bardzo dużo do zrobienia.

Protokół wywiadu nr 23

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Dowództwie Operacyjnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności to nic innego jak działania zmierzające do reakcji na negatywne zdarzenia oraz zminimalizowania ich skutków.

Odpowiedź 2.

a. Odporne państwo powinno cechować się rozwiniętym system współpracy cywilno-wojskowej z jasno określonymi zasadami.
b. System bezpieczeństwa państwa powinien być systematycznie testowany w celu wykrycia luk i niedostatków.
c. Aby budować odporne państwo, należy posiadać zabezpieczenie finansowe. W związku z tym gospodarka państwa powinna być oparta na zdrowych zasadach i dążyć do stałego rozwoju.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń zaliczyłbym te związane z sytuacją wewnętrzną danego państwa. To głównie sytuacja wewnętrzna danego kraju ma znaczący wpływ na odporność państwa – polaryzacja, niestabilne rządy czy niejasny system prawny to tylko kilka przykładów.
b. Z drugiej strony można mówić o grupie zagrożeń zewnętrznych – agresywny sąsiad, nieuregulowana sytuacja graniczna, migracje (zarówno te spowodowane zmianą klimatu, jak i te związane z sytuacją ekonomiczną), katastrofy naturalne.

Odpowiedź 4.

a. Biorąc pod uwagę zidentyfikowane zagrożenia, należy w pierwszej kolejności podjąć działania zmierzające do poprawy sytuacji wewnątrz kraju. Należy także dążyć do poprawy poziomu rozwoju gospodarczego, a w ten sposób doprowadzić do wzrostu zamożności społeczeństwa.

b. W dalszej kolejności widziałbym rozwój sił zbrojnych oraz pozostałych organów odpowiedzialnych za bezpieczeństwo kraju.

Odpowiedź 5.

a. Biorąc pod uwagę sytuację wewnętrzną w Polsce stan naszej odporności oceniam jako bardzo niski.

Protokół wywiadu nr 24

I. Dane ogólne eksperta

Stanowisko: wykładowca w Akademii Sztuki Wojennej

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności – zdolność podmiotu do przezwyciężania pojawiających się kryzysów i sprawnego powrotu do stanu poprzedniego.

Odpowiedź 2.

a. Odporne państwo to państwo o stabilnym i akceptowanym systemie rządów.
b. Odporność przejawia się także w utrzymaniu zdolności do gwarancji bezpieczeństwa przepływów strategicznych.
c. Wysoki poziom współpracy cywilno-wojskowej na rzecz zapewnienia bezpieczeństwa narodowego.
d. Zdolność do przewidywania zagrożeń i oceny ryzyka ich wystąpienia.
e. Systematycznie sprawdzany system bezpieczeństwa narodowego.

Odpowiedź 3.

a. Warto byłoby, rozważając problem identyfikacji zagrożeń wykorzystać metodę PMESII. Nie chciałbym szczegółowo rozpatrywać zagrożeń w każdym z obszarów i wskażę tylko tych kilka najistotniejszych z mojego punktu widzenia:
    - rozpad dotychczasowych systemów bezpieczeństwa w Europie,
    - przekierowanie głównego wysiłku USA na kwestię Chin,
    - konflikt regionalny w Europie,
    - wysoka inflacja,
    - polaryzacja społeczeństwa,
    - niekorzystne prognozy demograficzne,
    - niekontrolowane migracje.

Odpowiedź 4.

a. Sposoby budowy odporności zależą od wcześniej określonych zagrożeń i cech jakimi powinno charakteryzować się odporne państwo. W tym

przypadku, biorąc pod uwagę moje propozycje wskazane wcześniej, w pierwszej kolejności należy podjąć działania skupiające się na rozwoju i utrzymaniu stabilnego systemu politycznego.

b. W dalszej kolejności należy zająć się tworzeniem trwałych i działających sojuszy w regionie. Warto także zwrócić uwagę na potrzebę zwiększenia wydatków na obronę narodową.
c. Zasadne byłoby także podjęcie wysiłków na rzecz wspólnej, europejskiej polityki migracyjnej oraz skupienie wysiłków na rzecz przeciwdziałania skutkom zmiany klimatu.

Odpowiedź 5.

a. W skali od 1 do 10 odporność Polski oceniam na 4. Ocena jest pokłosiem moich obserwacji i dotychczasowych badań prowadzonymi w tym zakresie.

Protokół wywiadu nr 25

I. Dane ogólne eksperta

Stanowisko: adiunkt w Akademii Sztuki Wojennej

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność państwa – zdolność radzenia sobie z sytuacjami niekorzystnymi (kryzysem) oraz dalszego rozwoju.

Odpowiedź 2.

a. Odporne państwo jest zdolne do zarządzania sytuacjami kryzysowymi.
b. Stabilny rządy i akceptowany system prawny.
c. Umiejętność wyciągania wniosków z własnych i obcych doświadczeń.
d. Sprawny, ciągle rozwijany i testowany system bezpieczeństwa.

Odpowiedź 3.

a. Ocenę zagrożeń proponowałbym przeprowadzić zgodnie z klasyfikacją PMESII, czyli w obszarach: politycznym, militarnym, ekonomicznym, społecznym, informacyjnym a także infrastrukturalnym.
b. W obszarze politycznym – zmiana sojuszy w Europie i na świecie, polityka Rosji i Chin, problemy wewnętrzne w USA.
c. W obszarze militarnym – zbrojenia w Rosji, konflikty w Europie (nie chcę używać nazw regionalnych, bo można by je rozpatrywać jako mniej istotne), ciągłe demonstracje siły.
d. W obszarze ekonomicznym – spadek wzrostu gospodarczego, wzrost ceny surowców energetycznych, a także ich ograniczona dostępność, szara strefa w działalności gospodarczej.
e. W obszarze społecznym – niekorzystne tendencje demograficzne, niekontrolowane migracje, grupy przestępcze, społeczeństwa równoległe.
f. W obszarze informacyjnym – technologia (zarówno brak dostępu do niej, jak i zbytnie poleganie na niej), nieautoryzowany dostęp do baz danych, działalność przestępcza w cyberprzestrzeni, problemy moralne związaną z AI.

g. W obszarze infrastruktury – poziom ochrony elementów infrastruktury krytycznej (w Polsce, Europie i na świecie), przestarzałe elementy tej infrastruktury, stosunki własnościowe (brak możliwości kontroli państwowej w niektórych kluczowych elementach).

Odpowiedź 4.

a. Przestrzeganie prawa krajowego i międzynarodowego. System władzy – demokratyczny zgodnie z wolą społeczeństwa. Społeczeństwo niespolaryzowane, skupione wokół akceptowanego rządu.
b. Budowa sprawnego, nowoczesnego i chronionego systemu infrastruktury krytycznej.
c. Budowanie systemu trwałych i wiarygodnych sojuszy.
d. Tworzenie solidnych podstaw do rozwoju ekonomicznego państwa.
e. Inwestowanie w nowoczesne technologie.

Odpowiedź 5.

a. Długa droga do pokonania przed naszym krajem. Obecnie jesteśmy na początku drogi. Poziom naszej odporności jest ciągle zbyt niski.

Protokół wywiadu nr 26

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Sztabie Generalnym WP

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność – cecha jaką powinno się charakteryzować państwo umiejące wykorzystać posiadanie zasoby do przezwyciężenia wszelkich kryzysów.

Odpowiedź 2.

a. Odporne państwo powinno charakteryzować się trwałym rządem oraz być niezależne od wpływów zewnętrznych. Państwo takie powinno mieć zgromadzone zapasy w strategicznych obszarach funkcjonowania i mieć zdywersyfikowane źródła dostaw surowców energetycznych. Kolejną cechą powinno być posiadanie nowoczesnego systemu edukacji – kształcenie przyszłych pokoleń zdolnych do korzystania z zasobów technologicznych. Ponadto warto zwrócić uwagę na zdolność do funkcjonowania w różnych sojuszach czy też wspólnotach. Takie państwo powinno mieć dobrze rozwinięty system obrony narodowej.

Odpowiedź 3.

a. Do głównych zagrożeń należeć mogą:
   - uleganie wpływom zagranicznym,
   - nieumiejętność współpracy z innymi partnerami,
   - działalność Rosji i Białorusi,
   - zagrożenia ekologiczne,
   - dezinformacja,
   - wyczerpywanie się zasobów naturalnych.

Odpowiedź 4.

a. Ciągłe doskonalenie przyjętych procedur regulujących funkcjonowanie państwa.
b. Dążenie do budowy wykształconego społeczeństwa, umiejącego wykorzystywać nowoczesną technologię.

c. Wstępowanie do struktur gospodarczych i aktywna w nich działalność.
d. Tworzenie warunków do zatrudniania migrantów ze względu na niekorzystną sytuację demograficzną.
e. Tworzenie infrastruktury zdolnej do zabezpieczenia zgromadzonych rezerw strategicznych.

Odpowiedź 5.

a. Zdolność Polski do przezwyciężenia kryzysów jest na niezadawalającym poziomie.

Protokół wywiadu nr 27

I. Dane ogólne eksperta

Stanowisko: specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istota odporności państwa – zdolność do redukowania negatywnych skutków zdarzeń spowodowanych przez czynniki zewnętrzne i wewnętrzne, a wpływających na funkcjonowanie kluczowych elementów państwa.

Odpowiedź 2.

a. Odporne państwo – zapewnione bezpieczeństwo wewnętrzne (sprawne służby, sprawny system reagowania kryzysowego).
b. Odporne państwo – zapewnione bezpieczeństwo zewnętrzne (siły zbrojne, sojusze obronne).
c. Odporne państwo – zapewnione bezpieczeństwo energetyczne (linie dostaw, uniezależnienie się od Rosji).
d. Odporne państwo – bezpieczeństwo materiałowe (stan zapasów strategicznych).

Odpowiedź 3.

a. Jednymi z najistotniejszych zagrożeń są te związane z bezpieczeństwem energetycznym.
b. Kolejne zagrożenie wiąże się z bezpieczeństwem informacyjnym (usługi, banki, dezinformacja).
c. Wiele niebezpieczeństw wiąże się z ciągle obserwowanymi ruchami migracyjnymi z Afryki i Azji. Z tym zagadnieniem ściśle powiązana jest działalność niektórych państw, wykorzystujących migrantów jako swego rodzaju broń.

Odpowiedź 4.

a. Budowa odporności to ciągłe wyzwania zmierzające do doskonalenia stanu państwa. To także tworzenie alternatywnych sposobów przesyłu zasobów energetycznych, informacji.

b. Stworzenie systemu pozwalającego na sprawne zarządzanie państwem w każdych warunkach. System taki powinien być możliwie odporny na zakłócenia i próby ataków (sieci łączności, wymiana informacji, delegowanie uprawnień).
c. Kolejnym elementem mającym wpływ na odporność jest stworzenie systemu edukacji, dzięki któremu przybędzie wykształconych obywateli.

Odpowiedź 5.

a. Polska obecnie nie jest odporna na zagrożenia zarówno zewnętrzne, jak i wewnętrzne.

Protokół wywiadu nr 28

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 23.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Kluczem do sukcesu dla systemu odporności państwa to synapie działań (zdolności) zarówno układu militarnego, jak i pozamilitarnego. Kwestią do rozważenia jest to co rozumiemy pod pojęciem „układu pozamilitarnego". Z całą pewnością nie możemy myśleć tylko o policji czy straży granicznej, ale należy uwzględnić inne obszary funkcjonowania państwa.

Odpowiedź 2.

a. Odporne państwo umie wykorzystać posiadane zdolności do reagowania na kryzysy.
b. Działania są synchronizowane i koordynowane na poziomie państwa a zatem odpowiedzialność za to spada na odpowiednie ministerstwa. Oznacza to, że władza państwowa powinna być zdolna do realizacji wspomnianych wcześniej procesów.
c. Cechą odpornego państwa jest także umiejętność przygotowania systemu prowadzenia działań informacyjnych, psychologicznych, jak również w sferze kognitywnej.

Odpowiedź 3.

a. Do najistotniejszych zagrożeń należą:
    - działania informacyjne realizowane przez wrogie państwa lub podmioty niemilitarne (w tym aktorzy wewnętrzni), wywołujące bardzo często dezinformację i zmieniające sposób postrzegania rzeczywistości przez obywateli, takie działania w konsekwencji prowadzą polaryzacji społeczeństwa;
    - uzależnienie od surowców energetycznych sprowadzanych z Rosji;
    - zmiany klimatyczne;

- problemy demograficzne, które w konsekwencji doprowadzą do konieczności sprowadzania migrantów co z kolei powiązane jest z kolejnym zagrożeniem jakie niesie nielegalna migracja.

Odpowiedź 4.

a. Stworzenie funkcjonalnego systemu odporności powinno zawierać w sobie budowę funkcjonalnego i efektywnego systemu obronnego państwa, uwzględniającego problematykę służby zdrowia, ekonomii (finanse), logistyki (infrastruktura transportowa) oraz wspomnianych wcześniej policji i straży granicznej. Właściwie zbudowany system obronny z natury będzie odzwierciedlał potrzeby w zakresie odporności. Moim zdaniem nie powinniśmy rozpatrywać problematyki odporności bez rozpatrywania całego systemu obronnego.

Odpowiedź 5.

a. Biorąc pod uwagę moje wcześniejsze propozycje i pomysły uważam, że nie jesteśmy jeszcze odpornym państwem i musimy w wielu obszarach dążyć do poprawy.

Protokół wywiadu nr 29

I. Dane ogólne eksperta

Stanowisko: szef oddziału w Sztabie Generalnym WP

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Odporność objawia się zdolnością do skutecznego reagowania na występujące sytuacje kryzysowe, a jednocześnie do podejmowania działań, po ich wystąpieniu, zmierzających do przywrócenia stanu poprzedniego.

Odpowiedź 2.

a. Odporne państwo powinno cechować się stabilnym systemem władzy na wszystkich szczeblach. Należy zwrócić uwagę na przygotowanie zawczasu niezbędnych ustaw, rozporządzeń, aby wszystkie odpowiedzialne służby były świadome wyzwań, przed którymi staną.
b. Uwzględniając siedem filarów odporności określonych w czasie szczytu NATO, zwróciłbym uwagę na konieczność dokonania niezbędnych zmian w systemie służby zdrowia. W obecnej chwili poziom tych usług jest dość niski. W przypadku wystąpienia kryzysu lub działań wojennych na terenie Polski, zabezpieczenie medyczne będzie odgrywało decydującą rolę. Z drugiej strony zastanawiające jest, czy system ten będzie zdolny do pracy w warunkach wojennych, przyjmując, że część kraju może być pod tymczasową okupacją i wiele zadań spadnie na placówki rozmieszczone w zachodniej części kraju.
c. Kolejnym istotnym zagadnieniem jest opracowanie realistycznego planu ochrony infrastruktury krytycznej. Od jej stanu zależy przecież między innymi bezpieczeństwo energetyczne państwa. Podsumowując, odporne państwo powinno charakteryzować się trwałym system infrastruktury krytycznej, który jest właściwie zabezpieczony i zdolny do funkcjonowania w warunkach zakłóceń.

Odpowiedź 3.

a. Zagrożenia, przed jakimi stoi Polska, można podzielić na dwie grupy – militarne i pozamilitarne.
b. Do zagrożeń militarnych zaliczyłbym przede wszystkim: agresywną postawę Rosji, niebezpieczeństwo związane z koniecznością zabezpieczenia tzw. Przesmyku Suwalskiego, rozmieszczenie systemów A2AD na terenie obwodu kaliningradzkiego i w zachodniej części Rosji. Do tej kategorii zagrożeń można także zaliczyć niezdecydowaną postawę NATO i długi proces podejmowania decyzji.
c. Do zagrożeń pozamilitarnych zaliczam: niewystarczający poziom działalności niektóry resortów odpowiedzialnych za pewne obszary funkcjonowania państwa, postępujący poziom migracji do Europy wywołany w wielu przypadkach zmianami klimatycznymi. Do kolejnych wyzwań w tym obszarze można zaliczyć także problemy związane z uzależnieniem Europy od dostaw surowców z jednego tylko kierunku.

Odpowiedź 4.

a. Budowa odpornego państwa powinna rozpocząć się od opracowania zestawu aktów prawnych regulujących i określających zadania dla odpowiednich resortów. Co więcej, zadania te muszą być wykonalne, co wiąże się z zapewnieniem sił i środków (fundusze). W dalszej kolejności warto się zastanowić nad pracą w ramach np. Unii Europejskiej i opracowaniem wspólnych ram walki z nielegalną migracją i zmianami w klimatycznymi. Zdaję sobie sprawę, że takie działania są prowadzone, ale należałoby zwiększyć ich intensywność. Ważnym elementem jest także budowa nowoczesnych sił zbrojnych zdolnych do przeciwstawienia się wyzwaniom generowanym przez Rosję.

Odpowiedź 5.

a. W skali od jeden do pięciu odporność Polski oceniam na 2.

Protokół wywiadu nr 30

I. Dane ogólne eksperta

Stanowisko: starszy specjalista w Dowództwie Generalnym RSZ

Data wywiadu: 22.09.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Istotą odporności jest nabycie oraz posiadanie określonego zestawu sił i środków, wzajemnie ze sobą powiązanych, zorganizowanych systemowo w celu przeciwstawienia się wszelakim zagrożeniom, zarówno zewnętrznym, jak i wewnętrznym.

Odpowiedź 2.

a. Kluczowymi cechami odpornego państwa są przede wszystkim wszystkie elementy budujące silną gospodarkę narodową o zdrowych podstawach ekonomicznych. Kolejną cechą jest zdolność do prowadzenia niezależnej polityki zagranicznej (nie tylko w ramach sojuszy gospodarczych czy militarnych) zmierzającej do podniesienia rangi kraju na arenie międzynarodowej. Zamożność obywateli i postrzeganie państwa, jako silny i niezależny podmiot stanowi o jego odporności. Kolejnym wyznacznikiem jest poziom sił zbrojnych i innych służb wchodzących w system obrony narodowej.

Odpowiedź 3.

a. Do podstawowych zagrożeń bezpośrednio wpływających na odporność państwa można zaliczyć:
   - kwestie ekonomiczne – niska zamożność społeczeństwa, zadłużenie *per capita*, stosunki własnościowe, globalizacja (może być ona także traktowana jako szansa), przebywanie poza strefą euro;
   - kwestie społeczne – migracje i działania niektórych rządów państw, niekorzystna sytuacja demograficzna, niska świadomość społeczeństwa i jego polaryzacja oraz podatność na dezinformację;
   - kwestie militarne – postawa Rosji i Chin (Morze Południowochińskie), proliferacja broni masowego rażenia, działalność zorganizowanej

przestępczości, niskie wydatki na siły zbrojne, działalność szpiegowska i wywiadowcza;

- kwestie polityczne – duże różnice zdań wśród członków sojuszy (NATO i Unia Europejska), upartyjnienie struktur państwa, dojście do władzy w Europie skrajnych ugrupowań, ingerencje obcych podmiotów w wewnętrzne sprawy państwa.

Odpowiedź 4.

a. Budowa odpornego państwa powinna rozpocząć się od uświadomienia całego społeczeństwa o fakcie, że każdy jest odpowiedzialny za działania w tym obszarze. Moim zdaniem budowa odporności powinna być przedsięwzięciem angażującym ogół narodu. Nie można zamykać się tylko w swoich własnych, sektorowych „silosach".
b. W następnej kolejności należy przeprowadzić szczegółową analizę w celu zidentyfikowania mocnych i słabych stron, a także wyspecyfikować zagrożenia i szanse – przeprowadzić typową analizę SWOT.
c. Na podstawie wyników tej analizy zaproponować przedsięwzięcia, które należy zrealizować, zabezpieczając także odpowiednie środki finansowe.
d. Proces budowy odpornego państwa będzie z całą pewnością trwał długo i wymaga ponadpartyjnego porozumienia.

Odpowiedź 5.

a. Na dzień dzisiejszy ciężko określić poziom odporności Polski, gdyż jak do tej pory nie spotkałem się z wynikami takiej analizy i nie sądzę, że została ona przeprowadzona.

Załącznik 2.

WYNIKI BADAŃ OPINII EKSPERTÓW – MOŻLIWOŚCI BUDOWY SYSTEMU ANTYDOSTĘPOWEGO

Kwestionariusz wywiadu

I. Cel wywiadu

Celem wywiadu jest zbadanie opinii oraz poglądów dotyczących problematyki związanej z identyfikacją potrzeb i możliwości budowy narodowego systemu antydostępowego w kontekście budowania odporności państwa.

II. Tematyka i problemy

1. Czym Pana zdaniem powinien charakteryzować się skuteczny system antydostępowy?
2. Jakie elementy Pana zdaniem, powinny wchodzić w skład systemu antydostępowego?
3. W jaki sposób Pana zdaniem należy budować system antydostępowy?
4. W jaki sposób Pana zdaniem, skuteczny system A2/AD wpływa na budowanie odporności państwa, a w konsekwencji na jego bezpieczeństwo?
5. Jakie wskaźniki Pana zdaniem, mogą być przydatne do określenia poziomu odporności państwa?

III. Odpowiedzi na problemy – protokoły z przeprowadzonych wywiadów

Protokół wywiadu nr 31

I. Dane ogólne eksperta

Stanowisko: pracownik naukowy Chatham House – Królewskiego Instytutu Spraw Międzynarodowych, uczestnik Programu Rosja i Eurazja

Data wywiadu: 30.09.2021 r.

Miejsce wywiadu: VTC

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Tylko kilka słów można użyć, aby określić, czym system antydostępowy powinien się charakteryzować. Jeśli przystąpiono by do budowy takiego systemu, powinniście zwrócić uwagę, że powinien on być redundantny, zapewniający możliwość przetrwania oraz odporny na zakłócenia.
    - redundancja jako wielowarstwowe systemy rozmieszczone zgodnie z zasadami wzajemnej osłony,
    - przetrwanie jako zdolność do utrzymania mobilności i działania w trybie autonomicznym w celu uniknięcia luk w systemie, odporność, jako zdolność do obrony przed wszystkimi zagrożeniami i zaplanowanymi atakami (zwłaszcza walki elektronicznej i działaniami w cyberprzestrzeni).

Odpowiedź 2.

a. Zasadniczo narodowy system antydostępowy powinien obejmować elementy do prowadzenia: walki elektronicznej (EW) i jej przeciwdziałaniu, działań w cyberprzestrzeni (ofensywnych i defensywnych), a także posiadanie zdolności do działań w przestrzeni kosmicznej. Taki system powinien nie tylko chronić państwo przed konwencjonalnymi atakami rakietowymi, ale także działać w zakresie obrony asymetrycznej, takiej jak EW i cyber. Celem powinno być ograniczenie zdolności przeciwnika do zakwestionowania sojuszniczej i narodowej przewagi w powietrzu.
b. Aby to osiągnąć, narodowy system antydostępowy powinien obejmować wzmocnioną infrastrukturę C2/C4ISR (ang. *Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance*) –

dowodzenie, kontrola, łączność, komputery, wywiad, obserwacja i rekonesans.

Odpowiedź 3.

a. Na szczeblu państwowym takie przedsięwzięcie powinno być realizowane w ramach współpracy z NATO. W ostatecznym rozrachunku jest to wspólny wysiłek – nie tylko pod względem łączenia zasobów, ale także wykorzystywania technologii.

Odpowiedź 4.

a. Posiadanie zdolności do prowadzenia działań antydostępowych pomaga zwiększyć odporność i bezpieczeństwo kraju poprzez zwiększenie poziomu odstraszania przeciwnika. Jest to jednak obosieczne, ponieważ taki krajowy system nieuchronnie zantagonizuje i doprowadzi do wzrostu zagrożenia ze strony Rosji.

Odpowiedź 5.

a. Wykonano już wiele pracy nad pomiarem odporności. To, czego brakuje w badaniach, to określenie jej jakości („czy kraj stał się bardziej lub mniej odporny na zagrożenia zewnętrzne?"), zamiast skupienia się tylko na ilości (mierząc tylko samą odporność).

Protokół wywiadu nr 32

I. Dane ogólne eksperta

Stanowisko: profesor Wydziału Nauk Politycznych (Uniwersytet McGill Montreal)

Data wywiadu: 02.10.2021 r.

Miejsce wywiadu: VTC

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Skuteczny system antydostępowy to taki, który znacząco zniechęca (odstrasza) przeciwnika do prowadzenia działań przeciwko danemu państwu i jego zasobom. Aby można go było uznać za taki, „obszar jego oddziaływania" musi być dość duży (z konsekwencjami operacyjnymi, a nawet strategicznymi), a ryzyko, na jakie narażone są siły przeciwnika, musi być znaczące. W dużej mierze odnosi się to do domen powietrznych i morskich – nie sądzę, by jakiekolwiek obecne lądowe systemy zasługiwały na miano antydostępowych.
b. Należy zwrócić uwagę, że samo posiadanie systemu antydostępowego nie gwarantuje jednak ochrony przed wszystkimi atakami – przeciwnik nadal będzie w stanie używać broni dalekiego zasięgu, zwłaszcza przeciwko celom stałym.

Odpowiedź 2.

a. W skład systemu antydostępowego powinny wchodzić wszelkiego rodzaju sensory zdolne do wykrywania sił przeciwnika działających na danym obszarze, systemy uzbrojenia zdolne do skutecznego namierzania i niszczenia znacznych jego sił. Ponadto system powinien być redundantny oraz zapewniać możliwość wzajemnej osłony (strefy wykrywania i ognia powinny się zazębiać), aby w konsekwencji zapewnić jego odporność.

Odpowiedź 3.

a. Przede wszystkim należy rozpatrywać go jako zintegrowany, wielowarstwowy, odporny system obrony powietrznej dalekiego zasięgu, połączony z lądowymi zdolnościami przeciwokrętowymi na obszarach przybrzeżnych. Powinien on zawierać zarówno wzmocnione, jak i mobilne elementy zapewniające przeżywalność. Należy także zwrócić uwagę na

jakość sensorów – *ślepy system to bezużyteczny system*. Narodowy system antydostepowy powinien być także zdolny do zapewnienia ochrony elementów krajowej infrastruktury krytycznej.

Odpowiedź 4.

a. W takim zakresie, w jakim system antydostępowy chroni krajową infrastrukturę krytyczną (infrastrukturę energetyczną, komunikację, transport i łańcuch dostaw, potencjał rządowy i administracyjny), w takim zwiększa on odporność państwa. Jednak niektóre z tych elementów będą nadal podatne na ataki, które omijają (działania w cyberprzestrzeni) lub penetrują (wykorzystanie technologii *stealth* i ataki typu *stand-off*) elementy systemu antydostępowego, zwłaszcza że infrastruktura krajowa często składa się z „miękkich" celów w stałych o dobrze znanych lokalizacjach.

Odpowiedź 5.

a. Bardzo trudno to ocenić, ponieważ wiele zależy od czynników społecznych i politycznych – woli i morale narodu, przywództwa politycznego, domeny informacyjnej itp. Możliwe byłoby jednak wykorzystanie różnych narzędzi analitycznych (w tym gier wojennych) w celu zbadania, w jaki sposób systemy antydostępowe mogą zwiększyć poziom odporności.

Protokół wywiadu nr 33

I. Dane ogólne eksperta

Stanowisko: dziekan wydziału (Baltic Defence Academy, Tartu)

Data wywiadu: 01.10.2021 r.

Miejsce wywiadu: VTC

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Budowa systemu antydostępowego jest bardzo złożonym podejściem do obrony kraju lub określonej części jego terytorium i obejmuje zarówno elementy odstraszania, jak i odporności, aby zapobiec wszelkim atakom poprzez wykazanie zdolności i zdolności do zaangażowania sił przeciwnika w przypadku wejścia na własne terytorium lub wspólny obszar operacji. System antydostępowy koncentruje się na działaniach i zdolnościach dalekiego zasięgu, które mają na celu uniemożliwienie siłom przeciwnika wejścia na obszar operacyjny. System ten stanowi logiczną kontynuację operacji, koncentrując się na działaniach i zdolnościach krótszego zasięgu. Są one tworzone w celu ograniczenia swobody działania sił wroga na obszarze operacyjnym i uniemożliwienia kolejnym, nowowprowadzanym siłom dołączenia do wysuniętych oddziałów i wsparcia operacji. Zarówno działania w ramach ograniczania dostępu przeciwnika do określonego obszaru działań, jak i te koncentrujące się na ograniczeniu mu swobody działania na zajmowanym przez niego terenie mogą być prowadzone równolegle.

b. Dlatego też system antydostępowy powinien charakteryzować się posiadaniem zdolności pozwalających na zaangażowanie przeciwnika we wszystkich domenach pola walki, ze szczególną rolą poszczególnych rodzajów sił zbrojnych: powietrznych, lądowych, marynarki wojennej, sił specjalnych, wojsk obrony terytorialnej, wspieranych przez zdolności cybernetyczne i wojny elektronicznej. Takie wspólne, w miarę możliwości połączone, operacje spowodują znaczne straty przeciwnika i opóźnienia w jego działaniu, co może spowodować rewizję jego planów, ograniczyć postępy i powstrzymać agresję; równolegle stworzy to warunki dla sił

własnych do konsolidacji obrony i stworzenia warunków do rozpoczęcia kontrataku.

c. Koncepcja antydostępowa jest ściśle powiązana z pełnym wykorzystaniem czynników operacyjnych: czasu, siły i przestrzeni, z integralną rolą informacji jako czynnika krytycznego. Zostało to podkreślone przez Milana Vego, który stwierdził, że „bez zdolności do prowadzenia ruchów na dużą skalę na lądzie, morzu i w powietrzu, działania operacyjne są zasadniczo pustą koncepcją. Sukces każdej dużej operacji lub kampanii zależy od swobodnego przemieszczania sił w teatrze działań”[250].

Odpowiedź 2.

a. Jak wspomniano wcześniej, system antydostępowy powinien obejmować zdolności wszystkich rodzajów sił zbrojnych. Wszystkie one pełnią określone role związane z posiadanymi zdolnościami i realizowanymi zadaniami. Przykładem takiego rozwiązania jest Obwód Kaliningradzki jako część Rosyjskiego Zachodniego Okręgu Wojskowego. Są tam rozmieszczone wszystkie komponenty, a niewielka odległość od terytorium Rosji pozwala na wzmocnienie go w krótkim czasie siłami lub zdolnościami oferowanymi przez siły powietrzne oraz lądowe i morskie uderzenia rakietowe w krótkim czasie. Dodatkową zaletą jest fakt, że Białoruś jest częścią Organizacji Układu o Bezpieczeństwie Zbiorowym, a zatem zgodnie z jej artykułem 7 – jeśli zostanie aktywowana – może zostać wykorzystana jako dostarczyciel sił lub przynajmniej może zaoferować terytorium w celu rozmieszczenia rosyjskich wojsk. Zostało to przećwiczone podczas ostatnich ćwiczeń „Zapad". Siły kaliningradzkiego obszaru A2/AD obejmują Flotę Bałtycką, 11 Korpus Armijny, 132 Mieszaną Dywizję Lotniczą, Dywizję Obrony Powietrznej oraz zapewniają zdolność do użycia rakiet dalekiego zasięgu. System ten jest stale modernizowany i wzmacniany poprzez wdrażanie nowych systemów uzbrojenia pozwalających na zwiększenie zasięgu i precyzji uderzeń przeciwko siłom przeciwnika na lądzie, w powietrzu, a także na morzu.

[250] M. Vego, *Joint Operational Warfare: Theory and practice*, Naval War College, 2007, s. III-7.

b. Niedawna decyzja o utworzeniu 18 Dywizji Strzelców Zmotoryzowanych również wskazuje na rozwój zdolności do prowadzenia operacji ofensywnych/kontrataków, choć z ograniczonymi celami do osiągnięcia. Dlatego powinny posiadać wiarygodny system rozpoznania obejmujący obwód, aby pozyskiwać aktualne dane w czasie pokoju, aby je wykorzystać i umożliwić dalsze gromadzenie danych podczas kryzysu i wojny. Jednocześnie siły własne powinny rozwijać zdolności antydostępowe oraz prezentować gotowość i zdecydowanie do ich użycia w ramach odstraszania.

Odpowiedź 3.

a. Koncepcja ta opiera się na ocenie zagrożeń i prowadzi do rozwijania tych zdolności, które pozwolą uniemożliwić/utrudnić potencjalnemu wrogowi ingerencję w interesy i bezpieczeństwo narodowe. Koncepcja antydostępowa opiera się na zrozumieniu, że bezpieczeństwo narodowe jest nie tylko domeną wojskową i obejmuje wszystkie domeny zarządzania. W związku z tym, taka koncepcja jak i koncepcja Obrony Totalnej (ang. *Total Defence*) proszą się o rozwój systemu antydostępowego znacznie szerzej, przygotowując cały naród do obrony i oporu. Odnosi się to do przygotowania społeczeństwa w czasie pokoju do reagowania w przypadku kryzysu i wojny. W kontekście wojskowym decydująca rola należy do Ministerstwa Obrony i Szefa Sztabu Generalnego. Ze względu na specyfikę posiadania zarówno Dowództwa Operacyjnego, jak i Dowództwa Generalnego, ich rola musi być starannie określona i oparta na czytelnych aspektach prawnych, jasno określających podział obowiązków. Są one wspólnie odpowiedzialne i rozliczane za efektywne funkcjonowanie systemu antydostępowego. Zaletą jest przynależność do sojuszy wojskowych jako wiarygodny i odpowiedzialny partner, ponieważ pozwala to na otrzymywanie wsparcia w domenie wojskowej (NATO) i pozamilitarnej (UE). Dodatkową zaletą jest partnerstwo strategiczne, np. z USA.

b. Ministerstwo jest odpowiedzialne za politykę strategiczną, ale także rozwój zdolności w oparciu o właściwą ocenę zagrożeń, a nie pochopne decyzje, po których następują zamówienia związane z cyklem funkcjonowania poszczególnych zdolności. Odpowiedni dowódcy mają wprowadzać takie zdolności do służb w oparciu o jasne zrozumienie specyfiki potrzeb

antydostępowych i obszarowo zidentyfikowanych oraz roli służb w osiąganiu wspólnych efektów operacji.

Odpowiedź 4.

a. Odpowiedź na to pytanie jest raczej jasna, ponieważ starannie i celowo opracowany system antydostępowy ma znaczący i bezpośredni wpływ na bezpieczeństwo. Dlatego kluczowe jest pokazanie narodowej zdolności do odstraszania oraz zaprezentowanie potencjału odporności. Chodzi o to, że przeciwnik musi zrozumieć, że wszelkie agresywne działania nie będą opłacalne, a potencjalne zyski będą niższe niż koszty. Istnieje wiele dróg zmierzających do osiągnięcia obu tych celów, które muszą być profesjonalnie określone i wdrożone jako długoterminowe plany zaopatrzenia, a nie pochopne decyzje. Istnieją dobre przykłady rozwijania odporności społeczeństwa – wystarczy wspomnieć o nowo utworzonych Wojskach Obrony Terytorialnej (WOT) – ale znowu wiąże się to z właściwym zrozumieniem ich roli i posiadanych możliwości. Tak więc integracja całego społeczeństwa, wspierana przez edukację związaną z bezpieczeństwem i obronnością, jest niezbędna do budowania narodowej odporności i obronności.

Odpowiedź 5.

a. Stan odporności powinien być weryfikowany w oparciu o jakość przygotowania ludności i odpowiednich służb krajowych, a także jakość aktów prawnych formułujących obowiązki i gotowość infrastruktury. Bardzo ważna jest stała weryfikacja poszczególnych służb i współpracy między agencyjnej w oparciu o ćwiczenia o różnorodnej formie. W odniesieniu do sił zbrojnych opiera się na ich gotowości w ramach ich poszczególnych rodzajów, jak również zdolności do prowadzenia operacji połączonych. Obejmuje wszystkie rodzaje sił zbrojnych; obecnie ważnym zadaniem jest pełna integracja WOT z pozostałymi rodzajami SZ RP. Ćwiczenia mogą dostarczyć wielu informacji pozwalających na ocenę stanu, po którym musi nastąpić uczciwe i pragmatyczne podejście do zidentyfikowanych w ich trakcie wniosków i podjęcie działań naprawczych.
b. Istnieją pewne wskaźniki pozwalające na rozpoznanie poziomu odporności państwa. Można to zrobić za pomocą ankiet wśród ogółu populacji i ankiet

wśród specjalnie ukierunkowanych grup społecznych. Ankiety mogą być powiązane z różnymi możliwymi zagrożeniami dla kraju, a nie tylko ograniczone do sfery wojskowej. Pytania mogą być związane z takimi problemami jak: postrzeganie zagrożeń; ocena sytuacji w sąsiedztwie; postrzeganie konkretnych narodów; zaufanie do rządu i sił zbrojnych i innych służb; znaczenie sojuszy (NATO, UE), gotowość do aktywnej obrony kraju; gotowość do przyczynienia się do odporności itp.

Protokół wywiadu nr 34

I. Dane ogólne eksperta

Stanowisko: pracownik naukowy, University of Granada (Spain) – Political Science Department

Data wywiadu: 02.12.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Skuteczny system A2/AD powinien być integralny i zdolny do pokrycia wielodomenowego spektrum. Musi umożliwiać Siłom Zbrojnym RP manewrowanie, a także wyjście spod uderzeń przeciwnika. Istotnym elementem jest zdolność do odstraszania przeciwnika, co można osiągnąć poprzez budowę kompletnego i integralnego systemu (lądowego, powietrznego, morskiego i cybernetycznego). System A2/AD powinien być zrównoważony, co oznacza, że państwo musi przyjąć długoterminową perspektywę i wziąć pod uwagę możliwość braku wsparcia ze strony innych krajów w przypadku ataku. Oznacza to również, że część zdolności technologicznych i projektów powinna być wytwarzana w kraju.

Odpowiedź 2.

a. Elementy wchodzące w skład skutecznego systemu A2/AD powinny umożliwiać działanie w wielowymiarowym konflikcie. Najbardziej typowe elementy są związane ze środowiskiem przestrzeni powietrznej (pociski ziemia–powietrze, pociski woda–powietrze i środki typu powietrze–powietrze). W tej dziedzinie interesujące może być zbadanie innych systemów obronnych, takich jak bardzo skuteczna izraelska Żelazna Kopuła. Mogłyby one zostać zaadaptowane zarówno do ochrony obiektów cywilnych i wojskowych przed nalotami, jak i do odstraszania sił powietrznych przeciwnika. System A2/AD w domenie powietrznej być może powinien być rozwijany w tym samym czasie, co system schronów na ziemi, a także systemy radarowe.
    - Na lądzie, oprócz sił konwencjonalnych, istotne może być dokonanie przeglądu projektów urbanistycznych. Projektowanie infrastruktury publicznej (koleje, drogi i mosty) w celu zapobiegania lub spowalniania

ruchów przeciwnika może być środkiem zapobiegawczym, aby zyskać czas na reakcję na zagrożenie lądowe. Utrzymanie mobilności własnych sił lądowych mogłoby zmienić zasady gry w przypadku bezpośredniej konfrontacji z agresorem na terytorium kraju.

- Jeśli chodzi o domenę morską, walka podwodna w połączeniu z możliwościami przybrzeżnymi byłaby istotna, aby odeprzeć atak wroga na Polskę od strony północnej. Ponieważ domena morska nie jest moim obszarem specjalizacji (bardziej skupiam się na domenie lądowej), wskazane byłoby skontaktowanie się ze specjalistami Marynarki Wojennej w celu przeanalizowania możliwości rozwoju A2/AD w tym obszarze.
- Wymiar cybernetyczny powinien być przekrojowy w stosunku do trzech tradycyjnych domen. Pozwoliłoby to nie tylko uniemożliwić dostęp do terytorium kraju, ale także zapobiec wykorzystaniu zdolności A2/AD przez przeciwnika. Jest to istotne dla zdolności C4ISR Sił Zbrojnych RP i zapewni przewagę strategiczną oraz operacyjną.

Odpowiedź 3.

a. Aby zbudować zdolności A2/AD na poziomie państwowym, należy przyjąć jasne podejście strategiczne. Czy będzie ono defensywne czy ofensywne? A może będzie się koncentrować na działaniach prewencyjnych? Z innej perspektywy, czy celem jest uniemożliwienie przeciwnikowi działania na terytorium kraju? A może umożliwienie siłom zbrojnym rozmieszczenia poza granicami kraju? Odpowiedzi na te pytania są kluczowe, ponieważ warunkują środki i elementy systemu A2/AD, a także strategię komunikacyjną.
b. Po przyjęciu podejścia strategicznego propozycją może być rozwój zrównoważonego systemu A2/AD opartego na produkcji krajowej. Być może długoterminowe podejście można zorganizować w trzech głównych fazach (1) współpraca z wojskowymi i cywilnymi organizacjami sojuszniczymi, (2) rozwój krajowego przemysłu obronnego, który może być konkurencyjny na arenie międzynarodowej/regionalnej oraz (3) uzyskanie autonomii technicznej i strategicznej. Drugą i trzecią fazę można osiągnąć poprzez pogłębioną współpracę z cywilnymi instytucjami naukowymi w Polsce, głównie uniwersytetami, ośrodkami badawczymi lub *think tankami*.

c. Elementom tym powinna towarzyszyć bezpośrednia i pośrednia kampania komunikacji społecznej w celu uzyskania poparcia społecznego dla inicjatywy systemu A2/AD. Działania w wymiarze komunikacyjnym warunkują nie tylko akceptację obywateli danego kraju, ale także poparcie społeczeństw sojuszniczych. Oprócz tradycyjnych mediów szczególnie istotne są media społecznościowe (Twitter, Instagram, produkcje Netflix). Podczas syryjskiego konfliktu influencerzy odgrywali kluczową rolę w tworzeniu poparcia dla krajowych operacji wojskowych i decyzji politycznych. W przypadku A2/AD interesujące może być rozwijanie tych relacji z państwem w celu uzyskania wsparcia dla realizacji projektu, a także uzasadnienia działań w przypadku agresji.
d. Narracje i percepcja są kluczowym elementem i powinny być budowane, zanim przeciwnik zwycięży w obszarze komunikacji. Bezpośrednia komunikacja z instytucjami publicznymi okazała się w niektórych przypadkach nieskuteczna, więc preferowane byłoby podejście pośrednie. Na przykład w Hiszpanii bezpośrednie wiadomości od rządu lub wojska nie mają takiego samego efektu jak komunikacja pośrednia od osób mających wpływ na społeczeństwo, uniwersyteckich ośrodków badawczych lub po prostu obywateli

Odpowiedź 4.

a. Udzielenie konkretnej odpowiedzi na to pytanie w przypadku Polski jest szczególnie trudne. Wymagana jest dogłębna znajomość dynamiki społeczno-politycznej Polski, a także interakcji między różnymi podmiotami w środowisku cywilno-wojskowym. Na poziomie operacyjnym i strategicznym wpływ A2/AD na budowanie odporności państwa musi zostać przetestowany w prawdziwym konflikcie, a wtedy może być już za późno. Pomimo tych czynników mamy kilka przykładów, że odstraszanie działa, unikając eskalacji konfliktu, a także zapewnia poczucie bezpieczeństwa ludności kraju. Najlepszym przykładem jest izraelski system obronny; pozwala on uniknąć wysokiego odsetka palestyńskich rakiet, a także skutecznie chroni granice państwa.
b. Z perspektywy budowania odporności państwa, posiadanie systemu A2/AD pomogłoby zwiększyć zdolność odstraszania Polski. Brak systemu

oznaczałby słabość wobec przeciwnika, zwiększając szanse na bezpośredni konflikt i prawdopodobnie negatywnie może wpłynąć na prowadzenie operacji obronnej. Wojska Lądowe są podstawowym elementem Sił Zbrojnych RP, więc ich ochrona przed atakami z powietrza powinna być głównym priorytetem, a system A2/AD na to pozwoli. Kruchość bezpieczeństwa zostałaby pozytywnie zredukowana poprzez ustanowienie integralnego systemu obrony.

Odpowiedź 5.

a. Z mojego punktu widzenia wskaźniki przydatne do określenia poziomu odporności państwa nie powinny być związane wyłącznie z wymiarami wojskowymi. Jak wskazałem wcześniej, wymiar społeczny i komunikacyjny byłby kluczowym elementem w przypadku konfliktu, a także w budowaniu odporności państwa. Propozycją mogą być następujące elementy:

Obszary	Wskaźniki	Pozyskiwanie danych
Społeczno-polityczny	Społeczna akceptacja Sił Zbrojnych	Badania (ankiety) (Hiszpania, Francja, Wielka Brytania, Izrael prowadzą takie badania
	Zaufanie do systemu bezpieczeństwa i instytucji publicznych	Badania (ankiety)
	Polaryzacja społeczeństwa	Badania (ankiety)
	Polityczne wsparcie inicjatyw rządowych	Propozycje legislacyjne Oświadczenia polityczne
	Wspólne postrzeganie interesów bezpieczeństwa przez wszystkie siły polityczne	Propozycje legislacyjne Oświadczenia polityczne
	Poziom rekrutacji	Dane z ośrodków rekrutacyjnych
Operacyjny	Rozwijanie zdolności przez przeciwnika	Dane rozpoznawcze
	Czas reakcji na zagrożenia bezpieczeństwa	Wnioski i doświadczenia (np. z ćwiczeń)

Obszary	Wskaźniki	Pozyskiwanie danych
	Utrzymanie logistyki w SZ RP	Wnioski i doświadczenia (np. z ćwiczeń)
	Zdolność do przemieszczania sił zbrojnych	Wnioski i doświadczenia (np. z ćwiczeń)
Strategiczny	Stopień wsparcia dyplomatycznego z zagranicy	
	Stopień wsparcia militarnego z zagranicy	
	Stopień wsparcia socjalnego z zagranicy	
	Swiadomość zagrożeń	Badania (ankiety)

Protokół wywiadu nr 35

I. Dane ogólne eksperta

Stanowisko: wykładowca operacji połączonych – Wydział Studiów Wojskowych (Baltic Defence College, Estonia)

Data wywiadu: 01.12.2021 r.

Miejsce wywiadu: Bydgoszcz

II. Odpowiedzi na problemy

Odpowiedź 1.

a. Skuteczny system A2/AD powinien posiadać następujące cechy: uniemożliwia/utrudnia dostęp we wszystkich domenach przestrzeni walki (w tym w spektrum elektromagnetycznym), jest interoperacyjny z sojuszniczymi systemami A2/AD, jego elementy dowodzenia są rozproszone w celu zwiększenia zdolności do przetrwania oraz wykazuje manewrowość zarówno w sferze fizycznej, jak i spektrum elektromagnetycznym.

Odpowiedź 2.

a. Najkrócej rzecz ujmując, powinien posiadać wszystkie elementy, które umożliwiają mu funkcjonowanie na wszystkich poziomach wojny i we wszystkich obszarach walki.

Odpowiedź 3.

a. Budowa skutecznego systemu antydostępowego wymaga koordynacji na poziomie krajowym. Konieczne jest całościowe podejście ze strony władz państwowych, co wymaga koordynacji i harmonizacji szczególnie na poziomie politycznym, wojskowym i gospodarczym. Bez planowania strategicznego, powiązanego ze wsparciem budżetowym i utrzymaniem, zdolności te będą daleko niewystarczające.

Odpowiedź 4.

a. Ta kwestia jest poza obszarem moich badań i nie chciałbym wprowadzić pewnego zamieszania. Mogę jednak dodać, że system antydostępowy jest tylko jednym z elementów w powiązaniu bezpieczeństwa państwa i odporności narodowej.

Odpowiedź 5.

a. Podobnie jak w poprzednim pytaniu nie mogę udzielić satysfakcjonującej odpowiedzi ze wspomnianych wcześniej powodów. Zwróciłbym jednak uwagę, że celowe byłoby zbadanie strategicznych czynników wpływających na odporność i ich wpływ.