JAROSŁAW ŁUKASZ KEPLIN

https://doi.org/10.4467/20801335PBW.23.018.18760
https://orcid.org/0000-0003-1865-2261

Budowanie odporności państwa na działania hybrydowe

Abstrakt

Zapewnienie bezpieczeństwa w coraz bardziej złożonym i niepewnym świecie wymaga od państw sprostania wielu wyzwaniom. Należą do nich konieczność utrzymania kooperatywnego charakteru w przestrzeni międzynarodowej oraz potrzeba realizacji swoich celów strategicznych. Często następstwem takich działań są intencjonalne lub nieintencjonalne zagrożenia, które mogą skutecznie zdestabilizować nie tylko pojedyncze państwo, lecz także cały region. Ich pojawienie się może być efektem braku odporności na wrogie działania podmiotów państwowych lub niepaństwowych, które dla osiągnięcia swoich celów podejmują m.in. działania hybrydowe. Terminy „odporność państwa" i „działania hybrydowe" w literaturze przedmiotu są jednak niewystarczająco jasne i opisywane w sposób bardziej konceptualny niż definicyjny. W dokumentach zarówno narodowych, jak i NATO brakuje powszechnie uznanych definicji tych pojęć. Celem artykułu jest przedstawienie koncepcji budowania odporności państwa na działania hybrydowe.

Słowa kluczowe

działania hybrydowe, zagrożenia hybrydowe, wojna hybrydowa, bezpieczeństwo państwa, odporność państwa.

Świat w XXI w. jest postrzegany przez społeczność międzynarodową głównie przez pryzmat zjawiska globalizacji, kształtowanego przez trzy zasadnicze procesy – zacieśnianie więzi międzynarodowych, ograniczanie wpływu państw na gospodarkę i postęp technologiczny[1]. To sprawia, że rządy państw i ich społeczeństwa dostrzegają nowe możliwości związane m.in. ze swobodą przepływu towarów i usług, a także siły roboczej oraz z rozwojem nowych technologii. Z jednej strony te procesy bez wątpienia przyczyniają się do wzrostu gospodarczego państw i rozszerzenia konkurencyjności pomiędzy nimi. Z drugiej strony globalizacja ma skutki negatywne, powoduje np. dysproporcje w poziomie zamożności społeczeństw, zmniejszenie roli państw narodowych przy wzroście znaczenia instytucji ponadnarodowych.

Jednym ze skutków globalizacji jest zmiana charakteru zagrożeń – coraz częściej przyjmują one nietypową postać nowych form terroryzmu lub terroru czy też cyberataków. Inne mają mniej jawny charakter i są ukierunkowane na wywieranie nacisku, w tym gospodarczego lub społecznego, przy użyciu m.in. zmanipulowanych mediów jako *proxy*[2]. Za ich pomocą próbuje się wpłynąć na sytuację gospodarczą państw czy nastroje społeczeństwa, co może prowadzić do podważania tak podstawowych wartości, jak poszanowanie godności ludzkiej, wolności i demokracji.

Dotychczas normy prawa międzynarodowego były tworzone przez rządy państw. Obecnie biorą w tym aktywny udział wyspecjalizowane organizacje pozarządowe i eksperci powołani przez organy międzynarodowe. W szczególnych sytuacjach, w przypadku niedostosowania się państw do norm prawa międzynarodowego, organizacje te mogą wprowadzać sankcje. Próbują one zatem wpłynąć na sytuację polityczną i gospodarczą danego kraju i zmusić go do podporządkowania się normom prawnym. W praktyce wiąże się to z naciskiem ze strony organu zlecającego dotyczącym interpretacji norm, co stanowi przekroczenie jego kompetencji. Organizacje międzynarodowe mogą zatem mieć wpływ na działania państw, a interes tych organizacji może być wskazywany jako wyższa konieczność[3].

---

[1] D.J. Mierzejewski, *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Toruń 2011, s. 23–24.

[2] Pojęcie *proxy* oznacza pośrednika, który realizuje cel w imieniu rzeczywistego agresora lub wywiera presję na wskazany podmiot. Dzięki temu inicjator działania może zachować anonimowość.

[3] Przykładem organizacji, która może istotnie wpływać na zachowania państw, jest Unia Europejska. Rada wraz z Parlamentem Europejskim oraz Komisją mogą wydawać rozporządzenia i dyrektywy, które dla państw członkowskich stają się częścią prawa krajowego. W zakresie skarg i naruszeń norm przez państwa orzeczenia wydajeTrybunał Sprawiedliwości Unii Europejskiej. W ograniczonym zakresie prawo wpływania na działania państw ma Rada Bezpieczeństwa ONZ. Zob. szerzej: J. Ciechański, *Enklawy transnarodowe w zdecentralizowanym prawie międzynarodowym*, w: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (red.), Warszawa 2006, s. 346–348.

Należy przy tym podkreślić, że instytucje międzynarodowe są – poza państwami – tymi podmiotami, które dążą do ustabilizowania i unormowania sytuacji międzynarodowej[4].

Globalizacja i rosnąca współzależność pomiędzy różnymi podmiotami prawa międzynarodowego skutkują często brakiem możliwości przewidzenia zjawisk, a ich zasięg nie jest ograniczany przez bariery geograficzne, systemy polityczne i gospodarcze. Presja globalizacji powoduje, że we współczesnym świecie państwa nie są w stanie samodzielnie funkcjonować gospodarczo, a ich współzależność może być przyczyną kryzysów lub konfliktów. Część badaczy, m.in. Kenichi Ohmae, postrzega globalizację przez pryzmat państw narodowych, które częściowo utraciły kontrolę nad swoim terytorium, co prowadzi do utraty przez nie suwerenności i osłabienia struktur państwowych. Z kolei Susan Strange argumentuje, że proces deterytorializacji to integralna część procesu globalizacji, prowadzącego do „końca" państw na mapach politycznych świata. Dowodzi to erozji rdzenia władzy państwa narodowego nad jego strukturami terytorialnymi[5]. David Kilcullen przekonuje natomiast, że współczesne państwa narodowe są potężne, ale mniej elastyczne – wolniej adaptują się do zmian niż ich niepaństwowi przeciwnicy[6].

Zagrożenia wynikające z globalizacji powodują, że tworzy się nowe środowisko bezpieczeństwa, a dotychczasowe warunki i formy realizacji celów strategicznych przez podmioty państwowe[7] i niepaństwowe[8] ulegają transformacji. Do najbardziej istotnych podmiotów niepaństwowych należy zaliczyć organizacje pozarządowe,

---

[4] I. Popiuk-Rysińska, *Instytucje międzynarodowe*, w: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (red.), Warszawa 2006, s. 353.

[5] Zob. szerzej: Ch. Fjäder, *The nation-state, national security and resilience in the age of globalisation*, „Resilience: International Policies, Practices and Discourses" 2014, t. 2, nr 2, s. 114–129. https://doi.org/10.1080/21693293.2014.914771.

[6] D. Kilcullen, *The Accidental Guerrilla*: *Fighting Small Wars in the Midst of Big One*, New York 2009, s. 284.

[7] Aktorzy państwowi (państwa) są zaliczani do podmiotów prawa międzynarodowego. Charakteryzuje je terytorium, suwerenna władza, społeczeństwo, system karny, zdolność do nawiązywania i utrzymywania stosunków dyplomatycznych z innymi państwami. Zob. hasło: państwo, *Słownik terminów z zakresu bezpieczeństwa narodowego*, wyd. 6, Warszawa 2008, s. 96.

[8] Aktor niepaństwowy jest definiowany jako podmiot istotny dla stosunków międzynarodowych, niezależny od finansowania i kontroli rządów centralnych, działający w przestrzeni transnarodowej, nieposiadający swojego terytorium, społeczeństwa, geograficznie rozproszony oraz strukturalnie i organizacyjnie złożony. Poprzez swoje działania może wpływać na politykę państw oraz systemy gospodarcze i społeczeństwo. Zob. szerzej: A. Antczak, *Rola aktorów niepaństwowych w kształtowaniu bezpieczeństwa*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 3, s. 143–145. https://doi.org/10.14746/ssp.2017.3.7; K. Rokiciński, *Ewolucja postrzegania zagrożeń asymetrycznych*, w: *Acti Labores Lucundi. Studia ofiarowane Leopoldowi Ciborowskiemu w siedemdziesiątą rocznicę urodzin*, M. Zieliński, B. Pączek (red.), Gdynia 2014, s. 196.

korporacje transnarodowe o rozproszonej anonimowej własności, czyli niepaństwowe elementy funkcjonujące w przestrzeni globalnej, ponadpaństwowej czy też transnarodowej. Niewątpliwie w uwarunkowaniach geopolitycznych istniejących w XXI w. identyfikuje się nowe zagrożenia, będące (…) *rezultatem wielu zjawisk i procesów, które pozostawały do niedawna poza głównym nurtem zainteresowania polityków i analityków. Te zjawiska wymagają zasadniczego przeorientowania nie tylko odpowiednich doktryn, planowania działań, wyposażenia sił zbrojnych czy odpowiedniej infrastruktury, ale zasadniczo samego myślenia o budowaniu bezpieczeństwa*[9]. Truizmem jest stwierdzenie, że zapewnienie bezpieczeństwa państwa to proces trudny i złożony, a koncepcje dotyczące odporności często traktuje się jako strategie sprostania tym wyzwaniom. Aktualne pozostaje jednak przekonanie, że państwa są odpowiedzialne za zapewnienie bezpieczeństwa swoich granic, organizację struktur państwowych, gospodarkę i rozwój społeczeństwa.

Celem artykułu jest przedstawienie sposobu pojmowania i budowania odporności państwa w kontekście działań hybrydowych. Osiągnięcie celu ukierunkowała następująca hipoteza robocza: działania hybrydowe mogą istotnie wpływać na stan bezpieczeństwa państwa, a budowanie odporności jest skutecznym remedium na taki rodzaj zagrożeń. W związku z tym sformułowano problem badawczy: w jaki sposób rozumieć i budować odporność państwa na działania hybrydowe?

Rozwiązanie wskazanego problemu badawczego wymagało skorzystania z różnych metod badawczych. Do najważniejszych należy zaliczyć: metodę monograficzną, analizę literatury przedmiotu, analizę systemową, wykładnię językową, wywiad ekspercki[10], wnioskowanie indukcyjne i eliminacyjne, uogólnienie i analogię. Zastosowanie tych metod pozwoliło na przedstawienie propozycji koncepcji budowania odporności państwa na działania hybrydowe.

Rozumienie współczesnego środowiska bezpieczeństwa

Spośród definicji bezpieczeństwa tworzonych przez polskich teoretyków należy przytoczyć stanowisko Ryszarda Zięby, który uważa, że bezpieczeństwo sprowadza się do potrzeb egzystencjalnych takich podmiotów, jak jednostka, grupy społeczne i struktury organizacyjne państw. Jak tłumaczy, (…) *w najogólniejszym znaczeniu bezpieczeństwo można określić jako pewność istnienia i przetrwania, posiadania*

[9] G. Ciechanowski, *Wstęp*, w: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (red.), Szczecin 2017, s. 7–8.

[10] Wywiady zostały przeprowadzone w latach 2015–2022 z przedstawicielami Rządowego Centrum Bezpieczeństwa, Centrum Doktryn i Szkolenia Sił Zbrojnych oraz Akademii Marynarki Wojennej.

oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń, ale także powstaje wskutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego[11]. Ogólną definicję terminu „bezpieczeństwo" można odszukać w *Słowniku terminów z zakresu bezpieczeństwa narodowego*, w którym jest on wyjaśniany jako (…) *stan, który daje poczucie pewności, i gwarancje jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka. Jest to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład: zdrowia, pracy, szacunku, uczuć, dóbr materialnych*[12]. Przy wyjaśnianiu istoty zjawiska bezpieczeństwa należy mieć na uwadze jego związek ze zjawiskiem zagrożenia[13]. Uzyskanie pożądanego stanu bezpieczeństwa wymaga od podmiotu wcześniejszej aktywności, pozwalającej mu na swobodę w realizacji własnych interesów w środowisku, w którym funkcjonuje, co w konsekwencji zapewni rozwój i przetrwanie tego podmiotu. Aby podmiot mógł doświadczyć bezpieczeństwa, musi zatem eliminować ryzyko wystąpienia zagrożeń przez podejmowanie wyzwań i wykorzystanie szans w środowisku bezpieczeństwa.

Warto podkreślić, że w czasie zimnej wojny bezpieczeństwo europejskie było postrzegane przez pryzmat zagrożeń militarnych. Po rozpadzie dwubiegunowego układu świata zakres pojęciowy terminu „bezpieczeństwo" się rozszerzył. Istotny wkład w kształtowanie się sposobu postrzegania bezpieczeństwa wniósł Barry Buzan, przedstawiciel szkoły kopenhaskiej. Przyjął on, że problemy bezpieczeństwa należy rozpatrywać w zakresie szerszym niż tylko polityczno-militarny[14].

Analizując wydarzenia, które zaszły od lat 90. XX w., nie sposób nie zauważyć, że pojęcie bezpieczeństwa jest wciąż redefiniowane. Obecnie powstają nowe dziedziny bezpieczeństwa, np. bezpieczeństwo cybernetyczne, infrastruktury krytycznej, energetyczne, ekonomiczne, społeczne, morskie, humanitarne, socjalne i wiele innych, a zakres znaczeniowy tych pojęć wciąż się rozszerza. Zarysowała się zatem tendencja polegająca na tym, że przez zagrożenie bezpieczeństwa państwa rozumie się wszystko to, co może w jakikolwiek sposób zakłócić funkcjonowanie państwa i jego społeczeństwa. Dlatego też współcześnie uważa się, jak wskazuje Marian Kopczewski, że podmiotem bezpieczeństwa są wszystkie jednostki mające własne

[11] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, R. Zięba (red. nauk.), Warszawa 2008, s. 16.

[12] Hasło: bezpieczeństwo, *Słownik terminów z zakresu bezpieczeństwa narodowego*, wyd. 6, Warszawa 2008, s. 14.

[13] R. Zięba, *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004, s. 28.

[14] Za: A. Sekściński, *Bezpieczeństwo wewnętrzne w ujęciu teoretycznym. Geneza i współczesne rozumienie w naukach politycznych*, „Kwartalnik Naukowy OAP UW e-Politikon" 2013, nr 6, s. 47–48.

interesy i wyrażające ambicje ich realizowania[15]. Przyczyną przyjęcia takiego stanowiska jest m.in. konieczność uwzględnienia w dyskursie o bezpieczeństwie, oprócz współzależności między podmiotami prawa międzynarodowego, przede wszystkim norm dotyczących wojny, kontroli zbrojeń i znaczenia podmiotów pozarządowych[16]. Współczesny wymiar bezpieczeństwa to nie tylko przetrwanie, integralność terytorialna, suwerenność państwa, lecz także zapewnienie społeczeństwu odpowiedniej jakości życia, odpowiedniego poziomu gospodarczego państwa oraz ochrona środowiska naturalnego[17]. Zagrożeń nie można traktować wybiórczo. Konieczne jest dokonywanie diagnozy zmian zachodzących w przestrzeni międzynarodowej również w perspektywie długoterminowej.

Od 24 lutego 2022 r. świat skupia się na wydarzeniach w Ukrainie, ale tak samo ważny pozostaje problem sytuacji politycznej na Białorusi, która również stanowi determinantę bezpieczeństwa Polski oraz kształtowania się relacji z Federacją Rosyjską (FR). W rozważaniach na temat bezpieczeństwa nie można pominąć stanu relacji turecko-rosyjskich czy napięć w stosunkach Unii Europejskiej (UE) z państwami członkowskimi. Nie bez znaczenia są również ambicje państw dotyczące Arktyki i możliwości jej militarnego wykorzystania, a w kształtującym się nowym ładzie globalnym – przyszłość relacji USA–Chiny. Realizacja celów strategicznych na arenie międzynarodowej determinuje wielowymiarową grę o utrzymanie status quo w zakresie zachowania zdolności obronnych i umiejętnego dostosowania się do wyzwań[18]. Świadomość występowania zagrożeń i konieczność zadbania o własne interesy narodowe wyznaczają kierunek działań podejmowanych przez państwa na arenie międzynarodowej. W rezultacie jedne państwa adaptują się do zmieniającego się otoczenia strategicznego, a inne próbują zmniejszyć podatność na zagrożenia.

---

[15] M. Kopczewski, *Bezpieczeństwo wewnętrzne państwa – wybrane elementy*, „Doctrina. Studia społeczno-polityczne" 2013, nr 10, s. 107.

[16] E. Cziomer, M. Lasoń, *Podstawowe pojęcia i zakres bezpieczeństwa międzynarodowego i energetycznego*, w: *Międzynarodowe bezpieczeństwo energetyczne w XXI wieku*, E. Cziomer (red.), Kraków 2008, s. 16.

[17] M. Lasoń, *Bezpieczeństwo w stosunkach międzynarodowych*, w: *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy*, E. Cziomer (red. nauk.), Kraków 2010, s. 10–11.

[18] J. Raubo, *GlobState III, czyli zrozumieć świat i wykorzystać wiedzę do budowania sił zbrojnych*, Defence24, 13 XII 2020 r., https://defence24.pl/sily-zbrojne/globstate-iii-czyli-zrozumiec-swiat-i-wykorzystac-wiedze-do-budowania-sil-zbrojnych-komenatrz [dostęp: 7 VII 2022].

Problem w zakresie definiowania odporności państwa i działań hybrydowych

Problem budowania odporności państw na działania hybrydowe był omawiany wielokrotnie podczas kolejnych szczytów NATO[19]. W Brukseli w 2021 r. podano w komunikacie, że ataki hybrydowe i cyberataki na państwa Sojuszu mogą doprowadzić do uruchomienia art. 5 Traktatu północnoatlantyckiego[20]. W *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020* problemowi odporności państwa i obronie powszechnej poświęcono cały podrozdział. W punkcie 2.2 zostało jasno określone, że należy (…) *budować odporność państwa na zagrożenia, w tym o charakterze hybrydowym, zapewniać powszechny charakter obrony cywilnej i ochrony ludności*[21]. We wspomnianym dokumencie pojęcie zagrożeń o charakterze hybrydowym zostało wymienione pięciokrotnie, jednak nie pojawiły się w nim ani jego definicja, ani wyjaśnienie, co się do nich zalicza. Wyraz „odporność" został użyty aż jedenastokrotnie w odniesieniu do podejmowania działania (…) *na rzecz zwiększenia odporności państwa i społeczeństwa na współczesne zagrożenia*[22]. Zwiększenie odporności państwa jest rozumiane jako (…) *tworzenie systemu obrony powszechnej, opartego na wysiłku całego narodu,* oraz (…) *budowanie zrozumienia dla rozwoju odporności i zdolności obronnych Rzeczypospolitej Polskiej*[23]. Ma to polegać m.in. na: budowaniu systemu obrony powszechnej, odporności na zagrożenia o charakterze hybrydowym, rozwijaniu zdolności systemu ochrony zdrowia oraz struktur administracji publicznej, a także w zakresie zapobiegania zagrożeniom o charakterze terrorystycznym i reagowania na nie, zwalczania przestępczości zorganizowanej, z uwzględnieniem działalności przestępczej w cyberprzestrzeni[24]. W dalszej części omawianego dokumentu termin „odporność" jest używany w odniesieniu do zwiększenia bezpieczeństwa ekonomicznego, w tym finansowego, poprzez podejmowanie działań poprawiających odporność na międzynarodowe kryzysy finansowe, zwłaszcza takich, które służą

[19] W Newport w Walii w 2014 r., w Warszawie w 2016 r., w Brukseli w 2018 r. i w Londynie w 2019 r.

[20] Zob. szerzej: W. Lorenz, *Szczyt NATO w Brukseli – przełomowy moment dla Sojuszu*, PISM, 15 VI 2021 r., https://www.pism.pl/publikacje/Szczyt_NATO_w_Brukseli__przelomowy_moment_dla_Sojuszu [dostęp: 10 VII 2022]. Zob. także: R. Opas, *Użyją art. 5? Stoltenberg nie wyklucza*, Wiadomości WP, 11 X 2022 r., https://wiadomosci.wp.pl/uzyja-art-5-stoltenberg-nie-wyklucza-6821910367021888a [dostęp: 11 X 2022].

[21] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 15 [dostęp: 15 X 2022].

[22] Tamże, s. 10.

[23] Tamże, s. 15.

[24] Tamże, s. 15–20.

wzmacnianiu stabilności systemu finansów publicznych. Te działania dotyczą również aktywności dyplomatycznej, prawnej i administracyjnej, która zwiększa odporność państwa na ryzyko wykorzystywania dostaw surowców energetycznych jako instrumentu nacisku politycznego ze strony innych państw[25]. Problem budowania odporności struktur państwowych na skutki działań hybrydowych to częsty element debaty publicznej, podejmowanej również przez Biuro Bezpieczeństwa Narodowego[26]. Potrzebę budowy odporności na zagrożenia militarne, niemilitarne i hybrydowe podkreśla także Rządowe Centrum Bezpieczeństwa (RCB)[27]. Podaje ono, że w sytuacji pogarszającego się bezpieczeństwa w regionie odporność państwa na pojawiające się zagrożenia jest jednym z podstawowych warunków zapewnienia mu ochrony[28]. Z tego względu odporność państwa na zagrożenia o charakterze hybrydowym zajmuje ważne miejsce w debatach narodowych i międzynarodowych oraz w strategiach bezpieczeństwa. Nadal jednak brakuje terminów „odporność państwa" i „działania hybrydowe", które byłyby powszechnie uznawane i stosowane w dokumentach NATO i UE oraz w dokumentach narodowych. Sformułowane dotychczas definicje są niejednoznaczne, często mają charakter koncepcyjny i pozostawiają dowolność interpretacyjną, co nie sprzyja poznaniu naukowemu. Sposób postrzegania tych pojęć zależy od percepcji interpretatora jako określonego podmiotu, który na bazie swojej wiedzy formułuje teorię stanowiącą rezultat czynności interpretacyjnych związanych z podejmowanym problemem. Zgodnie z zasadami konstrukcji definicji powinna ona określać sens, znaczenie definiowanego wyrazu lub wyrażenia, być precyzyjna, jednoznaczna i logiczna[29].

---

[25] Tamże, s. 33–34.

[26] P. Soloch, P. Pietrzak, *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski*, „Bezpieczeństwo Narodowe" 2016, nr 37–40, s. 31.

[27] M. Kubiak, *Zarządzanie kryzysowe a bezpieczeństwo narodowe w dobie zagrożeń hybrydowych*, „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa" 2018, nr 24, s. 4. Biuletyny analityczne RCB są dostępne pod adresem: https://www.gov.pl/web/rcb/biuletyn-analityczny-rzadowego-centrum-bezpieczenstwa (dop. red.); *Budowanie odporności państw członkowskich sojuszu – implementacja wytycznych NATO*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/budowanie-odpornosci-panstw-czlonkowskich-sojuszu-implementacja-wytycznych-nato/ [dostęp: 20 XII 2018]; *Odporność na zagrożenia tematem seminarium RCB*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odpornosc-na-zagrozenia-tematem-seminarium-rcb/ [dostęp: 20 XII 2018]; A. Zasadzińska-Baraniewska, *Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa*, „Biuletyn Kwartalny Rządowego Centrum Bezpieczeństwa" 2017, nr 19, s. 4.

[28] *Odporne NATO*, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odporne-nato/ [dostęp: 20 XII 2020].

[29] M. Bartoszewicz, *Definicje legalne w świetle zasady określoności prawa*, w: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (red.), Wrocław 2018, s. 355–356.

Z uwagi na brak formalnych definicji w zakresie odporności państwa oraz w celu uściślenia przedmiotu rozważań warto wprowadzić definicję projektującą, która może posłużyć doprecyzowaniu badanego problemu.

Na wstępie trzeba zauważyć, że pojęcie odporności funkcjonuje również w innych dziedzinach wiedzy, takich jak nauki inżynieryjne i medycyna. W inżynierii mechanicznej dotyczy zrozumienia zachowania i podatności materiałów na odkształcenia pod wpływem użytych różnych sił zewnętrznych. W tym kontekście jest to miara odporności danego materiału na działania siły, aby mógł on wytrzymać bez pęknięcia lub trwałej zmiany kształtu. Miarą odporności w takiej sytuacji jest zatem czas powrotu materiału do pierwotnego kształtu po ustaniu siły oddziaływania[30]. W naukach medycznych zagadnieniem odporności organizmu zajmuje się immunologia. Na gruncie tej nauki odporność dotyczy (…) *procesów, dzięki którym ustrój ludzki utrzymuje równowagę środowiska wewnętrznego w przypadku zadziałania substancji obcej o właściwościach antygenowych pochodzenia zewnętrznego lub wewnątrzustrojowego*[31]. Z kolei *Słownik języka polskiego PWN* słowo „odporny" definiuje jako (…) *niewrażliwy na wpływy fizyczne lub moralne* oraz jako (…) *nieulegający zakażeniom drobnoustrojami chorobotwórczymi*[32]. Według *Słownika angielsko-polskiego* „odporny" to (…) *prężny, zdolny do szybkiego powrotu (np. do zdrowia)*, a „być odpornym" znaczy: *opierać się, stawiać opór, powstrzymywać się*[33].

W odniesieniu do odporności państwa sformułowania zawarte w przytoczonych definicjach można rozumieć następująco:

- „niewrażliwy" – odporny na oddziaływania, nieulegający wpływom, zdolny do utrzymania status quo;
- „stawiający opór" – zdolny do pokonywania zagrożeń.

Poprzez analogię do definicji przyjętych na gruncie nauk inżynieryjnych i medycznych oraz słownikowych autor sformułował definicję odporności państwa jako zdolność do przeciwstawienia się ofensywnym działaniom agresora/ów lub możliwość przystosowania się do nowych warunków z zachowaniem perspektywy dotychczasowego poziomu bezpieczeństwa, jednocześnie gwarantując przetrwanie i niezachwiany rozwój[34]. Z tej definicji wynika, że odporność państwa jest

[30] *Wytrzymałość materiałów – rodzaje, co to jest?*, EBMIA, 30 VIII 2021 r., https://www.ebmia.pl/wiedza/porady/obrobka-porady/wytrzymalosc-materialow-rodzaje/ [dostęp: 23 VII 2022].

[31] Hasło: immunologia, https://mediweb.pl/slownik-nauk-i-specjalnosci-lekarskich [dostęp: 20 VIII 2022].

[32] Hasło: odporność, *Słownik języka polskiego PWN*, https://sjp.pwn.pl/slowniki/odporno%C5%9B%C4%87.html [dostęp: 20 VIII 2022].

[33] Hasło: odporny, w: *Oxford Wordpower. Słownik angielsko-polski z indeksem polsko-angielskim*, Oxford University Press 2002, s. 643.

[34] Autor sformułował tę definicję na podstawie: J. Mokrzycki, C. Pawlak, *Budowanie odporności państwa gwarancją jego bezpieczeństwa*, w: *Kształtowanie przestrzeni bezpieczeństwa państwa*, G. Ciechanowski,

rozumiana jako zdolność do stawiania oporu oraz reagowania na sytuacje kryzysowe i umiejętność zarządzania nimi. Jest to zatem także zdolność adaptacji do nowej sytuacji. Na tak pojmowaną odporność państwa składają się zdolności w sferach cywilnej i wojskowej. To potwierdza, że budowanie odporności państwa jest doskonaleniem – w obliczu nowych zagrożeń – jego zdolności. Oznaczają one m.in. skuteczne radzenie sobie z działaniem agresora oraz umiejętność podtrzymania zaufania własnego społeczeństwa do władz państwowych i społeczności międzynarodowej w sytuacji wystąpienia zagrożenia[35]. Problemem przy tak skonstruowanej definicji odporności państwa pozostaje to, jak mierzyć lub oceniać odporność państwa i za pomocą jakich narzędzi powinno się to robić. Bez wypracowania systemu wskaźników i mierników rzetelna ocena stanu rzeczywistego jest niemożliwa. Ich odpowiednie dobranie pozwala na uzyskanie wiedzy, w jaki sposób i na jaką skalę analizowane zagrożenie czy zjawisko powoduje zmiany w środowisku bezpieczeństwa. Zatem każdy wskaźnik i miernik powinien być warunkowany celowością jego wprowadzenia. Należy ustalić, dlaczego są one wprowadzane, co zamierza się mierzyć, czego oczekuje się od miernika i wskaźnika, przy jednoczesnym wskazaniu sposobu mierzenia bądź szacowania i podania źródła danych. To prowadzi do wypracowania i przyjęcia metodyki. Dopiero wtedy można stwierdzić, w jakim obszarze należy poprawić odporność.

W odniesieniu do nabywania odporności na działania hybrydowe koniecznością jest zrozumienie ich – czym one są lub nie – i powiązanie ich z obszarami funkcjonowania państwa. Należy zauważyć, że stosowanie terminu „działania hybrydowe" można ujmować w co najmniej trzech wymiarach: **epistemologicznym** – jako sposób poznania naukowego, **ontologicznym** – wskazując na istotę ich bytu, czasu i przestrzeni, **przedmiotowym** (zakresowym) – czym one są[36].

Z dotychczas przeprowadzonych badań w zakresie zagrożeń o cechach hybrydowych i działań hybrydowych wynika, że te pojęcia zdobyły rozgłos po bezkrwawej aneksji Krymu przez FR, będącej skutkiem niezdolności państw i NATO

K. Ligęza, A. Rurak (red. nauk.), Gdynia 2019, s. 38. Definicja została opracowana również w dokumencie: *Koncepcja Kompleksowego Wzmacniania Odporności RP* przygotowanym przez Rządowe Centrum Bezpieczeństwa. Za: G. Matyasik, *Jak wygląda polska odporność?*, INFOSECURITY24, 4 IV 2023 r., https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [dostęp: 10 IX 2023].

[35] *Commitment to enhance resilience*, North Atlantic Treaty Organization, 8 VII 2016 r., https://www.nato.int/cps/en/natohq/official_texts_133180.htm [dostęp: 21 VIII 2022].

[36] Podobnego podziału dokonał Bogdan Zdrodowski w podejściu poznawczym dotyczącym bezpieczeństwa. Zob. szerzej: B. Zdrodowski, *Istota bezpieczeństwa*, w: *Wybrane problemy bezpieczeństwa wewnętrznego państwa*, A. Misiuk (red.), t. 34, Warszawa 2014, s. 34.

do rozpoznania sytuacji w środowisku bezpieczeństwa[37]. Brak precyzyjnych definicji określających ten rodzaj zagrożeń generuje nieporozumienia i wywołuje publiczny spór w tak ważnym obszarze, jak bezpieczeństwo państwa, które należy do wartości najwyżej cenionych i chronionych. Problem nieprecyzyjnego formułowania definicji działań hybrydowych i zagrożeń o cechach hybrydowych został dostrzeżony również przez wielu badaczy i teoretyków wojskowych, którzy uważają, że używanie tych terminów jest nieprzydatne, a czasami nawet niebezpieczne. Zwracają uwagę, że definicje w obszarze hybrydowości, szczególnie te opublikowane po 2014 r., odnoszą się wprost do działań FR, a nie do zjawiska rozumianego holistycznie[38].

Przedstawione dotychczas definicje są na tyle ogólne, że mogą obejmować wiele różnych zjawisk i stwarzać możliwości różnej ich interpretacji na zasadzie *catch-all*, co sprawia, że tradycyjnie pojmowany podział na czas pokoju oraz czas wojny i konfliktu ulega rozmyciu[39]. W takiej sytuacji zagrożenia hybrydowe mogą być wszystkim dla wszystkich. Dlatego państwo i jego struktury muszą być świadome współczesnych zagrożeń i przygotowane na różne wyzwania, a nie tylko na jeden typ zagrożenia.

Analiza problemu wskazuje, że agresor podejmuje działania z wyprzedzeniem, a czas przygotowań może trwać od kilku do nawet kilkunastu lat. Pozwala mu to

---

[37] Wydarzenia w Ukrainie w 2014 r., a w szczególności aneksja Krymu, zostały zidentyfikowane przez licznych badaczy i ekspertów w obszarze bezpieczeństwa jako wojna hybrydowa lub zagrożenia hybrydowe. Obok tych dwóch popularnych terminów pojawiły się inne, mniej powszechne, takie jak działania hybrydowe, konflikt hybrydowy, atak hybrydowy, konflikt czwartej generacji i działania w szarej strefie, które były jedną z wielu prób wyjaśnienia hybrydowości współczesnych konfliktów. Zob. A. Rácz, *Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist*, Helsinki 2016, s. 40; S. Bolzen, „*Die NATO muss auf grüne Männchen vorbereitet sein*", Die Welt, 17 VIII 2014 r., http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.ht ml/ [dostęp: 27 I 2015]; C. Pawlak, J. Keplin, *Aneksja Krymu w kontekście działań hybrydowych*, „Kwartalnik Bellona" 2016, nr 3, s. 23–24; J. Keplin, *Działania hybrydowe jako niewidzialne zagrożenia*, w: *Wojna Federacji Rosyjskiej z Zachodem*, M. Banasik (red.), Warszawa 2022, s. 167–168; T. Usewicz, J. Keplin, *Hybrid Actions and Their Effect on EU MaritimeSecurity*, „Journal on Baltic Security" 2023, t. 9, nr 1, s. 32–68. https://doi.org/10.57767/jobs_2023_001; J. Keplin, *Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2022, t. 8, nr 2, s. 54–68. https://doi.org/10.34739/dsd.2022.02.04.

[38] Zob. P. Ochmann, J. Wojas, *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego" 2018, nr 2, s. 101–102. https://pressto.amu.edu.pl/index.php/spp/article/view/21068/20355 [dostęp: 1 XII 2022]; A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, s. 17.

[39] E. Reichborn-Kjennerud, P. Cullen, *What is Hybrid Warfare?*, Norwegian Institute of International Affairs, 2016 r., https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf, s. 1–2 [dostęp: 1 XII 2022].

na doprecyzowanie celu strategicznego i celów pośrednich, a także prognozowanie pożądanych efektów i przyjęcie wstępnej strategii. W pierwszej kolejności agresor będzie koncentrował się na identyfikacji i analizie celu w zakresie:

- podatności oraz słabości państwa w różnych obszarach jego funkcjonowania,
- mocnych stron jako ograniczeń lub utrudnień w osiągnięciu celu (przynależność do sojuszy, sytuacja gospodarcza, społeczna i inne)[40].

Działania będą obejmować zsynchronizowane użycie wielu narzędzi[41] dostosowanych do podatności obszarów. Należy dodać, że środkiem znacznie ułatwiającym odniesienie sukcesu będą działania informacyjne. Takie stanowisko pokrywa się z poglądami Carla von Clausewitza, według którego osiąganie celów strategicznych może być realizowane za pomocą środków innych niż wojna. Jako ważne narzędzie wymienia on politykę[42]. Agresor, wykorzystując elementy polityki, może realizować swoje cele w sposób ukryty lub jawny. Dlatego każda skuteczna strategia powinna uwzględniać złożoność środowiska, wskazywać sposoby pozwalające na odniesienie zwycięstwa i unikać przy tym nadmiernego upraszczania problemu. Każde pominięcie istotnych elementów przez stronę zaatakowaną powoduje, że agresor zyskuje przewagę sytuacyjną. Z tego względu istotne jest ciągłe monitorowanie zagrożeń zarówno w wymiarze wewnętrznym, jak i zewnętrznym. Ich analiza jest kluczowym etapem do określenia potencjalnego ryzyka, ponieważ pozwala na zrozumienie motywacji agresora. Ponadto rozważanie jego intencji, potencjalnych interesów, potrzeb, metod działania, a także woli w osiąganiu celów głównych lub pośrednich stanowi najważniejszy element efektywnego zarządzania bezpieczeństwem państwa. Istotne jest również określenie rzeczywistych zdolności i zasobów agresora, czy są one wystarczające do osiągnięcia celu. Zatem ciągłe monitorowanie zagrożeń pozwala na szybkie reagowanie i dostosowanie adekwatnych narzędzi do zidentyfikowanego niebezpieczeństwa, pozwala na skuteczną reakcję na zmieniającą się sytuację, co z kolei przyczynia się do zachowania stabilności i suwerenności państwa.

Należy dodać, że zrównoważony rozwój społeczno-gospodarczy wymaga odpowiedniego poziomu bezpieczeństwa, czyli zdolności zapewnienia niezagrożonego wykorzystania możliwości (potencjału) w budowaniu efektywnej gospodarki

[40] J. Keplin, *Analityczny model działań hybrydowych narzędziem wspomagającym bezpieczeństwo państwa*, w: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (red.), Szczecin 2017, s. 127–138.

[41] Takie jak np. dyplomatyczne, ekonomiczne, informacyjne, sankcje, embargo i inne.

[42] Zob. szerzej: M. Mazur-Bubak, *Wybrane teorie leżące u podstaw współczesnego paradygmatu wojny*, „Internetowy Magazyn Filozoficzny Hybris" 2015, nr 30, s. 82–83, https://dspace.uni.lodz.pl/xmlui/handle/11089/20342 [dostęp: 20 XI 2022].

jako podstawy tworzenia dobrobytu państwa i jego społeczeństwa[43]. Współczesne zagrożenia, które są efektem działań hybrydowych, mogą być generowane zarówno przez podmioty państwowe[44], jak i niepaństwowe[45]. Jak tłumaczy Ryszard Zięba, (…) *współczesne zagrożenia i niebezpieczne zjawiska stanowią odbicie zmian, jakie ciągle się dokonują w życiu narodów i państw, a także są efektem działań podejmowanych przez państwa i aktorów niepaństwowych w celu zapewnienia własnych interesów*[46]. Oznacza to, że światowy porządek się zmienia, a panujące zasady ulegają modyfikacjom. Zauważalna staje się rywalizacja o zasoby surowców energetycznych i rosnące zapotrzebowanie na żywność, wodę, a także na nowe technologie.

Podmioty niepaństwowe, takie jak organizacje pozarządowe (ang. *Non Government Organization,* NGO), korporacje międzynarodowe i transnarodowe, a w szczególnej sytuacji indywidualne osoby, mogą wpływać na politykę państwa, systemy gospodarcze i społeczeństwo, a ich działalność lobbingowa może kształtować przepisy prawa międzynarodowego, które mogą służyć interesom tych podmiotów. Ponadto angażowanie NGO jako *proxy* umożliwia agresorowi unikanie odpowiedzialności i ukrywanie nielegalnych działań. W takim wypadku udowodnienie agresji okazuje się bardzo trudne. Krzysztof Liedel uważa, że w zbliżających się dziesięcioleciach państwa będą opierać swoje bezpieczeństwo na zapisach aktów prawnomiędzynarodowych, a ich skuteczność będzie zależała od ich interpretacji na arenie międzynarodowej[47]. Stwarza to potrzebę modyfikacji poglądów na temat bezpieczeństwa państwa, jego zagrożeń i gwarancji. Tymi zagrożeniami są np. wrogie działania informacyjne lub ekonomiczne, których celem są oddziaływanie na społeczeństwo czy też uzależnienie gospodarcze i technologiczne lub uzależnienie dostaw surowców od innych państw albo korporacji i wpływanie w ten sposób na politykę państwa będącego obiektem tych działań. Środowisko bezpieczeństwa państwa może zatem zostać zdestabilizowane w wyniku użycia przez

---

[43] H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2017, s. 8.

[44] Najczęstszymi zagrożeniami stwarzanymi przez podmioty państwowe są: dążenia rewizjonistyczne, inicjowanie bądź podsycanie konfliktów wewnętrznych, stosowanie presji politycznych i ekonomicznych, dążenie do uzależnienia innego państwa od surowców energetycznych, działania informacyjne i dezinformacyjne, które mogą być prowadzone m.in. w cyberprzestrzeni.

[45] Do zagrożeń ze strony aktorów niepaństwowych najczęściej zalicza się działania grup terrorystycznych (np. dżihad), działania zorganizowanych grup przestępczych, zorganizowany handel narkotykami i bronią, wrogie działania korporacji usiłujących wpływać na politykę państwa.

[46] R. Zięba, *Współczesne wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego*, „Stosunki Międzynarodowe – International Relations" 2016, t. 52, nr 3, s. 9. https://doi.org/10.7366/020909613201601.

[47] K. Liedel, *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 52.

agresora różnorodnych, skoordynowanych form oddziaływania, o różnym stopniu intensywności i w różnych obszarach funkcjonowania państwa. Można spodziewać się poszerzenia zakresu zagrożeń oraz ich transformacji, co będzie utrudniać ich identyfikację i reakcję na nie. Zdaniem Tomasza Schumana najczęściej wykorzystywanym sposobem oddziaływania na państwo jest szantaż, zastraszanie polityków i mediów, aby oni sami zdestabilizowali i rozbili swój kraj[48]. W warunkach braku powszechnej gwarancji bezpieczeństwa państwa i stosunkowo łatwego prowadzenia agresywnej polityki przez różne podmioty typowe jest stosowanie miękkich środków oddziaływania. Po pierwsze, dużego znaczenia nabierają działania informacyjne, które przy wykorzystaniu nowoczesnych technologii są jednym ze skuteczniejszych narzędzi. Niezwykle ważny jest obszar systemów teleinformatycznych, będących przestrzenią, w której są prowadzone działania hybrydowe. Ataki w cyberprzestrzeni nie muszą mieć destrukcyjnych skutków dla systemów IT wykorzystywanych w infrastrukturze krytycznej czy bankach, ale mogą spowodować dyskomfort sytuacyjny i wywołać obawy[49]. Po drugie, celem może być kradzież i ujawnienie informacji istotnych dla bezpieczeństwa państwa. Po trzecie, działanie może polegać na wprowadzaniu fałszywych informacji do przestrzeni informacyjnej, a także na użyciu fałszywych certyfikatów bezpieczeństwa w celu nie tylko osiągnięcia korzyści materialnych, lecz także zastraszenia[50]. Należy dodać, że część

[48] „T. Schuman" to pseudonim byłego agenta KGB Jurija Bezmienowa, pracownika Agencji Prasowej Novosti w New Delhi, w której był odpowiedzialny za prowadzenie propagandy na rzecz sowieckiego reżimu. Był specjalistą w zakresie technik dezinformacyjnych, jawnej i ukrytej propagandy, a także dywersji ideologicznej (ros. *активные мероприятия*). W 1970 r., po wykryciu jego wrogiego stosunku do ZSRR, zbiegł do USA. Przekazał Amerykanom wiele znaczących informacji na temat technik służących dokonaniu przewrotu ideologicznego i sposobów destabilizacji poprzez zakłócenie funkcjonowania pojedynczych obszarów (np. dyplomatycznego, ekonomicznego) za sprawą przejęcia kontroli nad kluczowymi sektorami związanymi z tymi obszarami, aż do spowodowania kryzysu całego państwa. Swoimi refleksjami podzielił się w książce. Zob. szerzej: T. Schuman (Yuri Bezmenov), *Love Letter to America*, Los Angeles 1984, s. 17–19.

[49] Działania w cyberprzestrzeni dotyczą ataków przeprowadzanych nie tylko przez określone podmioty państwowe i niepaństwowe, lecz także przez hakerów działających często z pobudek emocjonalnych oraz z chęci zaimponowania. Stanowią oni spory odsetek atakujących. Działania w cyberprzestrzeni mogą polegać również na wykradaniu danych wrażliwych i włamaniach na konta bankowe i być kwalifikowane jako przestępstwa pospolite. Zob. szerzej: K. Rokiciński, *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, R. 46, nr 1, s. 165.

[50] Holenderska firma DigiNotar została zaatakowana przez przestępców internetowych. Z DigiNotar skradziono ponad 500 certyfikatów SSL, w tym wystawione dla CIA i Mossadu. W rezultacie firma ogłosiła bankructwo. Podobnego działania doświadczył Distribute.it. – australijski dostawca hostingu oraz Cloud Nine – angielski dostawca internetu. Zob. szerzej: A. Jadczak, *Zaatakowana przez hakerów DigiNotar ogłosiła upadłość*, Computer World, 23 IX 2011 r., https://www.computerworld.pl/news/Zaatakowana-przez-hakerow-DigiNotar-oglosila-upadlosc,375383.html [dostęp: 4 I 2019].

zagrożeń w obszarze IT wynika z braku akceptowalnego poziomu bezpieczeństwa danych zgromadzonych w systemach informatycznych wykorzystywanych do realizacji istotnych zadań publicznych[51]. Marian Cieślarczyk podkreśla, że (…) *aktualnie znacząca część społeczeństw nie nadąża za rozwojem nowoczesnych technologii* (…) *i nie jest w stanie przewidzieć konsekwencji związanych z ich wykorzystaniem, co wiąże się z dużym ryzykiem*[52].

Ważne jest również zwrócenie uwagi na państwa, które próbują odbudować swoją pozycję mocarstwową i dążą do tworzenia świata wielobiegunowego. Nie ma nic nowego w podejmowaniu działań hybrydowych, ale globalizacja, nowoczesne technologie czy cyfryzacja znacznie zwiększyły ich skuteczność i możliwości oddziaływania na wybrane cele. Należy podkreślić, że działaniami hybrydowymi nie są regularne działania dyplomatyczne, umowy gospodarcze, a z całą pewnością nie są nimi konflikt i wojna pomiędzy państwami. Działania hybrydowe mogą natomiast istnieć pomiędzy tymi dwoma ostatnimi stanami. Są one wykorzystywane jako tańsza alternatywa dla klasycznego konfliktu zbrojnego, trwają znacznie dłużej przy odczuwalnie niższych kosztach. W działaniach hybrydowych zagrożenia z nich wynikające rozpoznaje się wcześniej niż agresora jako sprawcę. Agresor, przyjmując różne cele oraz sposoby wykorzystania *proxy*[53], czyni swoje działania trudnymi do wykrycia.

Podejmując próbę wyjaśnienia działań hybrydowych, należy pamiętać, że nie ograniczają się one do aktywności militarnej. Agresor chce wpłynąć na politykę państwa, jego społeczeństwo i gospodarkę w warunkach pokoju, przeciwdziałanie tym zagrożeniom czy też odpowiedź na nie będzie zatem inna niż obejmująca siłę militarną. Można postawić tezę, że każde wykorzystanie narzędzi[54] w warunkach pokojowego funkcjonowania państwa jest rozumiane jako celowe działania aktora państwowego lub niepaństwowego, których następstwem będzie oczekiwana reakcja w obszarze poddanym oddziaływaniu, np. zmiana polityki państwa czy zachowania społeczeństwa, odbiór informacji zgodny z wolą inicjatora takich działań.

---

[51] *NIK o bezpieczeństwie danych*, Najwyższa Izba Kontroli, 16 V 2016 r., https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-danych.html [dostęp: 18 XI 2018].

[52] M. Cieślarczyk, *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i odporności państwa*, Siedlce 2009, s. 14.

[53] Istotne jest wykorzystanie *proxy*, np. organizacji pozarządowej lub korporacji transnarodowej, do osiągnięcia celu, przez co faktyczny agresor nie zostanie wykryty, a wina za agresywne działania może zostać przypisana innemu podmiotowi.

[54] W stosunkach między podmiotami prawa międzynarodowego do tych narzędzi zalicza się m.in. politykę, zawieranie umów, wykorzystanie innych podmiotów prawa międzynarodowego (*proxy*), działania informacyjne, dezinformacyjne, próby uzależnienia od surowców energetycznych lub innych dóbr.

W rzeczywistości działania hybrydowe są trudne do rozpoznania, a stwarzają realne zagrożenie.

Zgodnie z przyjętym sposobem rozumowania działania hybrydowe można zdefiniować następująco:

> (…) są to działania zmierzające do osiągnięcia celów politycznych i strategicznych przez agresora z możliwością utrzymania dotychczasowych stosunków gospodarczych i/lub dyplomatycznych. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany oraz skoordynowany, łącząc różne środki wywierania nacisku i uzależniania zależne od agresora. Mogą być one prowadzone w środowisku politycznym, ekonomicznym, militarnym i społecznym, w tym mniejszości narodowych, etnicznych i religijnych, z jednoczesnym zróżnicowaniem ich co do czasu, przestrzeni (obszaru geograficznego) i intensywności oraz przy wykorzystaniu proxy. Działania te realizowane są w warunkach normalnego stanu funkcjonowania państwa[55].

Odporność państwa na działania hybrydowe

Współcześnie państwo jest uważane za gwaranta ogólnego dobrobytu swoich obywateli. Cel ten osiąga m.in. przez realizację polityki w zakresie świadczeń socjalnych, zabezpieczenia społecznego, dostępu do edukacji, egzekwowania prawa, bezpieczeństwa publicznego, ochrony infrastruktury krytycznej oraz w innych ważnych dziedzinach. Takie podejście do roli państwa w zakresie zapewniania bezpieczeństwa wskazuje zatem na złożone społeczno-polityczne i społeczno-gospodarcze ramy, które powinny zostać uwzględnione przez instytucje państwowe. W odniesieniu do odporności państwa wprowadza to do dyskursu kryteria zarówno materialne[56], jak i niematerialne[57], które są trudno mierzalne. Ponadto wymusza to dokładne określenie rodzaju odporności państwa wymagającej poprawy i udoskonalenia, gdyż żadne państwo nie jest odporne we wszystkich dziedzinach

[55] *Koncepcja udziału Sił Zbrojnych RP w przeciwdziałaniu zagrożeniom hybrydowym*, Centrum Doktryn i Szkolenia, Bydgoszcz 2017, s. 8. Przedstawiona definicja jest efektem prac nad tą koncepcją. Autor niniejszego artykułu był szefem zespołu projektowego do spraw jej opracowania.

[56] Na przykład potencjał militarny, surowce energetyczne, woda, rudy metali itp.

[57] Na przykład wola działania i determinacja państwa w osiąganiu celów strategicznych, aspiracje państw, ideologie, strategie, trwałość sojuszu, informacje, zdolność społeczeństwa do neutralizowania zagrożeń itp.

bezpieczeństwa[58]. Dlatego istotne jest ustalenie, jaki jest cel tych działań oraz na co ta odporność ma być budowana[59]. Wymaga to dokonania wyboru priorytetów, a zatem pociąga za sobą użycie adekwatnych zasobów[60].

W odniesieniu do działań hybrydowych kluczowe jest zrozumienie, że są one wymierzone w wiele dziedzin bezpieczeństwa państwa, zatem odporność należy rozpatrywać z uwzględnieniem specyfiki tych dziedzin. Zagrożenia te są złożone, charakteryzują się wysoką dynamiką zmian, co powoduje, że ich wykrywalność jest utrudniona. Wymaga to przygotowania nowych rozwiązań wspomagających system wczesnego ostrzegania[61]. Lech Wojciech Zacher wskazuje, że istotna jest świadomość dotycząca wystąpienia potencjalnych zagrożeń, kryzysów i katastrof, bez której nie ma możliwości wspierania globalnego bezpieczeństwa[62]. Podobnie uważa Jack Williams[63] i dodaje, że każdą istotną informację powinno się analizować w celu dokonania świadomej oceny tego, co może się wydarzyć w przyszłości. Jego zdaniem oceny zagrożeń są zawsze przewidywalne, a opisywanie prognozowanego wydarzenia nie jest rezultatem analizy danych wywiadowczych, lecz zastosowania kilku technik analitycznych w celu połączenia w złożonym systemie ogromnej ilości informacji[64].

---

[58] Priorytetem jest określenie tych obszarów bezpieczeństwa państwa, które są najbardziej wrażliwe na współczesne zagrożenia – np. ekologiczne, od terroryzmu i sabotażu, po awarie systemów technicznych, w zakresie utrzymania łańcuchów dostaw surowców energetycznych i inne.

[59] Koncepcja budowania odporności państwa na działania hybrydowe powstała m.in. w ramach projektu Countering Hybrid Warfare realizowanego w ramach Wielonarodowej Kampanii Rozwoju Zdolności (ang. *Multinational Capability Development Campaign*), w którym autor brał udział. Projekt miał dwie edycje – w latach 2015–2016 oraz 2017–2018. Efektem prac był m.in. dokument: *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*, https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf [dostęp: 7 X 2022].

[60] Ch. Fjäder, *The nation-state*…, s. 122.

[61] P. Cullen, *Hybrid threats as a new 'wicked problem' for early warning*, Hybrid CoE, 4 VI 2018 r., https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ [dostęp: 12 X 2018].

[62] L.W. Zacher, *Trwały rozwój – utopia czy realna możliwość?*, „Problemy Ekorozwoju – Problems of Sustainable Development" 2008, t. 3, nr 2, s. 66.

[63] Profesor Jack F. Williams zajmuje się m.in. ryzykiem w branży energetycznej. Był dyrektorem i liderem w Binder Dijker Otte & Co. (BDO) Consulting, gdzie pełnił funkcję doradcy finansowego, księgowego i eksperta ds. wykrywania oszustw finansowych. Ponadto był konsultantem rządu federalnego Stanów Zjednoczonych Ameryki oraz sektora prywatnego w zakresie analizy zagrożeń, oceny ryzyka, ochrony infrastruktury. Obecnie m.in. wykłada w St. John's University School of Law Bankruptcy Policy Institute.

[64] J.F. Williams, *Critical Energy Infrastructure Protection Policy Research Series: Al-Qaida threats and strategies: the religious justification for targeting the international energy economy*, The Canadian

Na podstawie przeprowadzonej krytycznej analizy literatury przedmiotu autor wnioskuje, że jednym z działań mogących w istotny sposób wesprzeć budowanie odporności państwa na działania hybrydowe jest dążenie do efektywnego rozpoznania i identyfikacji zagrożeń tych istniejących, ale niewykrytych, jak również przyszłych, które będą skutkiem podjętych decyzji politycznych oraz efektem zmian zachodzących w środowisku bezpieczeństwa. Nie sposób nie zgodzić się z Krzysztofem Ligęzą, który zwraca uwagę, że nie ma możliwości rozpoznania wszystkich zagrożeń, gdyż część z nich pojawia się niespodziewanie, zarówno co do czasu, jak i miejsca. Dodaje, że istotą bezpieczeństwa jest myślenie wyprzedzające o rodzaju zagrożeń i odpowiednie przygotowanie się do minimalizowania skutków w przypadku ich wystąpienia[65].

Przytoczone argumenty dowodzą, że odpowiednio wypracowane metody i narzędzia mogą wesprzeć proces opracowania realnych scenariuszy, tak by móc przygotować się na potencjalne wydarzenia. Jest to zgodne z tezą przyjętą przez Zachera, zakładającego, że (…) *najważniejszym celem myślenia o przyszłości jest nie tyle jej odkrycie, ile przygotowanie się do rozmaitych opcji, wobec których może nam się przydarzyć stanąć w zmaganiu z nieznanym losem*[66]. Halina Świeboda wskazuje, że myślenie wyprzedzające wpisuje się w proces projektowania przyszłych działań[67]. Z tego względu każdy odpowiednio przygotowany scenariusz jest źródłem wiedzy i przyczynia się do stworzenia odpowiedniego systemu prognozowania wraz z koncepcją systemu wczesnego ostrzegania, czego rezultatem powinno być wypracowanie strategii przeciwdziałania niekorzystnym zjawiskom. Celowe jest opracowanie takiego narzędzia analitycznego, które uwzględni trendy oraz zjawiska zachodzące w środowisku bezpieczeństwa. Wymaga to systemowego postrzegania obiektu i przedmiotu badań przy uwzględnieniu czynników wynikających z globalizacji oraz uwarunkowań wewnętrznych państwa. Identyfikowanie zagrożeń, prognozowanie sytuacji wewnętrznej państwa, a także stosunków międzynarodowych wiąże się ze zbiorem twierdzeń i założeń, które je wyjaśniają, i powinny być one wykorzystane podczas przygotowywania takiego narzędzia analitycznego[68].

Centre of Intelligence and Security Studies at Carleton University, marzec 2008 r., http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.612.473&rep=rep1&type=pdf, s. 18 [dostęp: 17 XI 2018].

[65] K. Ligęza, E. Iwanina-Szopińska, *Zabezpieczenie logistyczne ludności poszkodowanej w sytuacjach kryzysowych w aspekcie zapewnienia bezpieczeństwa*, w: *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, M. Kopczewski, I. Grzelczak-Miłoś, M. Walachowska (red. nauk.), Poznań 2013, s. 353–364.

[66] L.W. Zacher, *Problemy i metody przewidywania przyszłości (przegląd tendencji w literaturze)*, w: *Czy warto myśleć o przyszłości?*, Warszawa 1996, s. 28.

[67] H. Świeboda, *Prognozowanie zagrożeń bezpieczeństwa*…, s. 11.

[68] M. Sułek, *Prognozowanie i symulacje międzynarodowe*, Warszawa 2010, s. 13.

Należy również zwrócić uwagę na to, że w XXI w. obserwuje się większą podatność społeczeństwa na zagrożenia związane z rozwojem cywilizacyjnym, napięciami politycznymi, ekonomicznymi, społecznymi oraz informacyjnymi. Problem stanowi to, jak wyedukować społeczeństwo, które jest często nieświadome zagrożeń, aby stało się na nie odporne. Dlatego do zadań współczesnego państwa należy również przygotowanie społeczeństwa do pojawienia się zmian lub negatywnych zdarzeń w obszarze bezpieczeństwa. Istotne jest zdiagnozowanie poziomu zdolności danej społeczności do reagowania na określone zagrożenia zarówno na poziomie całej populacji, jak i grup społecznych oraz pojedynczych osób. W tym wypadku ważny jest sposób, w jaki państwo dokona deskrypcji tych negatywnych zdarzeń i jak przedstawi ich wpływ na społeczeństwo i aktualną sytuację w państwie. Właściwy przekaz informacji przyczyni się do nabywania odporności w zakresie potencjalnych niebezpieczeństw w wyniku zwiększenia świadomości na ich temat, a tym samym do zyskiwania zdolności adaptacyjnych w sytuacji pojawienia się niespodziewanych zagrożeń. Odporne społeczeństwo dysponuje umiejętnością radzenia sobie z nimi oraz potrafi sprawnie powrócić do właściwego funkcjonowania[69].

Przedstawione dwa podejścia – rozumiane jako konieczność rozwoju narzędzi służących do rozpoznania i identyfikacji zagrożeń oraz budowanie świadomości społeczeństwa – determinują sposób projektowania polityki państwa i strategii osiągania celów w różnych obszarach jego funkcjonowania. W efekcie państwo nabywa umiejętność radzenia sobie z wstrząsami i kryzysami. W związku z tym konieczne jest rozwijanie dyplomacji, która może wesprzeć wysiłki na rzecz stworzenia wspólnej płaszczyzny w zakresie realizacji podobnych celów w przestrzeni międzynarodowej, a w konsekwencji zapewniania pokoju na świecie[70]. Budowanie i umacnianie zaufania ze strony innych państw mają szczególne znaczenie dla stworzenia trwałej odporności państwa w przestrzeni międzynarodowej, zwłaszcza na działania hybrydowe. W relacjach międzynarodowych jest istotna świadomość konsekwencji podejmowanych decyzji. Każda decyzja polityczna, a przede wszystkim wprowadzenie nowych norm prawa międzynarodowego, przynosi określone skutki w obszarach funkcjonowania państwa, a także powoduje interakcje między podmiotami prawa międzynarodowego. W szczególnej sytuacji może dojść do zagrożenia egzystencji konkretnego podmiotu, co skłoni go do natychmiastowego i nadzwyczajnego użycia narzędzi, dzięki którym zabezpieczy on swoje interesy.

---

[69] K. Górska-Rożej, *Kształtowanie odporności na zagrożenia w społecznościach lokalnych*, „Przegląd Policyjny" 2018, nr 1, s. 57. https://doi.org/10.5604/01.3001.0013.6643.

[70] J. Pospisil, F.P. Kühn, *The Resilient State: New Regulatory Modes in International Approaches to State Building?*, „Third World Quarterly" 2016, t. 37, nr 1, s. 5–7. https://doi.org/10.1080/01436597.2015.1086637.

Te podejścia powinny mieć bezpośrednie przełożenie na rozwój koncepcji, strategii i doktryn. Ich jakość merytoryczna, sposób ujęcia problemu, a także trafność przyjętych ocen będą wpływać na budowanie odporności państwa.

Podsumowanie

Przedstawione opinie ekspertów potwierdzają, że obecnie państwa oraz ich społeczeństwa są bardziej narażone na nowe formy zagrożeń niż kilka dekad wcześniej. Wynika to głównie z rozwoju nowych technologii, w szczególności infrastruktury ułatwiającej dostęp do informacji i ich wymianę. Nowa przestrzeń cybernetyczna, nazywana również piątym wymiarem walki, stanowi dogodne środowisko dla cyberprzestępstw i cyberataków, które mogą zagrażać bezpieczeństwu państwa i społeczeństwu.

W nowych uwarunkowaniach geopolitycznych uwidacznia się agresja podprogowa, w której adwersarze celowo utrzymują swoje działania na poziomie poniżej progu wojny. Ich celem jest osiągnięcie przyjętych założeń z jednoczesnym generowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa oraz służbach i instytucjach odpowiedzialnych za bezpieczeństwo w państwie. Ponadto nagminne naruszanie norm prawa międzynarodowego, granic terytorialnych suwerennych państw oraz praw człowieka wymaga interwencji organizacji międzynarodowych i innych państw, które często kończą się niepowodzeniem. Istotny problem stanowi również to, że państwa coraz trudniej osiągają swoje cele strategiczne, które wielokrotnie są sprzeczne z celami innych podmiotów lub różnią się od nich, lub pozostają nieznane. Takie podejście do budowania odporności na działania hybrydowe powoduje ograniczenie współpracy pomiędzy państwami i aktorami niepaństwowymi, a zatem trudność w utrzymaniu dotychczasowego ładu globalnego. W związku z tym budowanie odporności na działania hybrydowe wymaga dobrego zrozumienia przyczyn luk i podatności na zagrożenia w obszarach funkcjonowania państwa, które mogą zostać wykorzystane przez potencjalnego agresora. Należy przypomnieć, że zagrożenia nie generują się samoistnie – aby powstawały, muszą zaistnieć odpowiednie warunki. Zawsze musi być przyczyna w postaci celowego działania agresora, własnych niedoskonałości i sprzyjającego środowiska.

Ważne jest również zrozumienie, że aby działania hybrydowe mogły być skuteczne, musi zaistnieć triada: **celowość działań agresora – podatności atakowanego – zdolności agresora**. Dowodzi to, że zagrożenia będące skutkiem działań hybrydowych są zmienne, co utrudnia atakowanemu ich rozpoznanie i reakcję na nie, na które to działania potrzeba czasu. Wymaga to większej uwagi oraz

skoncentrowania się na poziomie strategiczno-politycznym. Z tego względu w odpowiedzi na konkretne zagrożenia konieczne jest wdrażanie odpowiednich regulacji prawnych i zasad bezpieczeństwa. Powinno uwzględnić się w tych działaniach postęp technologiczny, a także współpracę sektora prywatnego z instytucjami państwowymi, ośrodkami naukowymi i NGO. Można założyć, że budowanie odporności państwa to także poszerzanie wiedzy w zakresie współczesnych zagrożeń.

Z uwagi na niepewność i złożoność globalnych współzależności odporność państwa należy postrzegać jako jego celową działalność, ukierunkowaną na rozpoznawanie czynników powodujących zagrożenia oraz skupioną na budowaniu sprawnych struktur państwowych, które mają umiejętność nawiązywania relacji również z podmiotami niepaństwowymi funkcjonującymi w kraju i poza jego granicami. Tylko takie działania zagwarantują zdolność państwa do jego ochrony przed współczesnymi zagrożeniami lub zredukują ryzyko ich wystąpienia.

Bibliografia

Antczak A., *Rola aktorów niepaństwowych w kształtowaniu bezpieczeństwa*, „Środkowoeuropejskie Studia Polityczne" 2017, nr 3, s. 143–158. https://doi.org/10.14746/ssp.2017.3.7.

Bartoszewicz M., *Definicje legalne w świetle zasady określoności prawa*, w: *Dookoła Wojtek… Księga pamiątkowa poświęcona Doktorowi Arturowi Wojciechowi Preisnerowi*, R. Balicki, M. Jabłoński (red.), Wrocław 2018, s. 355–364.

Bezpieczeństwo międzynarodowe po zimnej wojnie, R. Zięba (red. nauk.), Warszawa 2008.

Ciechanowski G., *Wstęp*, w: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (red.), Szczecin 2017, s. 7–8.

Ciechański J., *Enklawy transnarodowe w zdecentralizowanym prawie międzynarodowym*, w: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (red.), Warszawa 2006, s. 346–348.

Cieślarczyk M., *Teoretyczne i metodologiczne podstawy badania problemów bezpieczeństwa i odporności państwa*, Siedlce 2009.

Cziomer E., Lasoń M., *Podstawowe pojęcia i zakres bezpieczeństwa międzynarodowego i energetycznego*, w: *Międzynarodowe bezpieczeństwo energetyczne w XXI wieku*, E. Cziomer (red.), Kraków 2008, s. 13–28.

Fjäder Ch., *The nation-state, national security and resilience in the age of globalisations*, „Resilience: International Policies, Practices and Discourses" 2014, t. 2, nr 2, s. 114–129. https://doi.org/10.1080/21693293.2014.914771.

Górska-Rożej K., *Kształtowanie odporności na zagrożenia w społecznościach lokalnych*, „Przegląd Policyjny" 2018, nr 1, s. 54–65. https://doi.org/10.5604/01.3001.0013.6643.

Gruszczak A., *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, W. Sokała, B. Zapała (red.), Warszawa 2011, s. 9–17.

Keplin J., *Analityczny model działań hybrydowych narzędziem wspomagającym bezpieczeństwo państwa*, w: *Współczesne zagrożenia bezpieczeństwa*, G. Ciechanowski, M. Romańczuk (red.), Szczecin 2017, s. 127–138.

Keplin J., *Działania hybrydowe jako niewidzialne zagrożenia,* w: *Wojna Federacji Rosyjskiej z Zachodem*, M. Banasik (red.), Warszawa 2022, s. 163–186.

Keplin J., *Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2022, t. 8, nr 2, s. 54–68. https://doi.org/10.34739/dsd.2022.02.04.

Kilcullen D., *The Accidental Guerrilla*: *Fighting Small Wars in the Midst of Big One*, New York 2009.

Kopczewski M., *Bezpieczeństwo wewnętrzne państwa – wybrane elementy*, „Doctrina. Studia społeczno-polityczne" 2013, nr 10, s. 103–122.

Kubiak M., *Zarządzanie kryzysowe a bezpieczeństwo narodowe w dobie zagrożeń hybrydowych*, „Biuletyn Kwartalny Biura Analiz i Reagowania RCB" 2018, nr 24, s. 3–5.

Lasoń M., *Bezpieczeństwo w stosunkach międzynarodowych*, w: *Bezpieczeństwo międzynarodowe w XXI wieku. Wybrane problemy*, E. Cziomer (red. nauk.), Kraków 2010, s. 9–32.

Liedel K., *Zagrożenia hybrydowe. Jak zmienia się środowisko bezpieczeństwa RP?* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne: *Wojna hybrydowa*, s. 51–58.

Ligęza K., Iwanina-Szopińska E., *Zabezpieczenie logistyczne ludności poszkodowanej w sytuacjach kryzysowych w aspekcie zapewnienia bezpieczeństwa*, w: *Paradygmaty badań nad bezpieczeństwem. Zarządzanie kryzysowe w teorii i praktyce*, M. Kopczewski, I. Grzelczak-Miłoś, M. Walachowska (red. nauk.), Poznań 2013, s. 353–364.

Mazur-Bubak M., *Wybrane teorie leżące u podstaw współczesnego paradygmatu wojny*, „Internetowy Magazyn Filozoficzny Hybris" 2015, nr 30, s. 74–93.

Mierzejewski D.J., *Bezpieczeństwo europejskie w warunkach przemian globalizacyjnych*, Toruń 2011.

Mokrzycki J., Pawlak C., *Budowanie odporności państwa gwarancją jego bezpieczeństwa*, w: *Kształtowanie przestrzeni bezpieczeństwa państwa*, G. Ciechanowski, K. Ligęza, A. Rurak (red. nauk.), Gdynia 2019, s. 35–46.

Ochmann P., Wojas J., *Wojna hybrydowa jako przykład umiędzynarodowionego konfliktu wewnętrznego*, „Studia Prawa Publicznego" 2018, nr 2, s. 101–121. https://doi.org/10.14746/spp.2018.2.22.5.

Pawlak C., Keplin J., *Aneksja Krymu w kontekście działań hybrydowych*, „Kwartalnik Bellona" 2016, nr 3, s. 23–32.

Popiuk-Rysińska I., *Instytucje międzynarodowe*, w: *Stosunki międzynarodowe. Geneza, struktura, dynamika*, E. Haliżak, R. Kuźniar (red.), Warszawa 2006, s. 353–375.

Pospisil J., *The Resilient State: New Regulatory Modes in International Approaches to State Building?*, „Third World Quarterly" 2016, t. 37, nr 1, s. 1–16. https://doi.org/10.1080/01436597.2015.1086637.

Rácz A., *Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist*, Helsinki 2016.

Rokiciński K., *Ewolucja postrzegania zagrożeń asymetrycznych*, w: *Acti Labores Lucundi. Studia ofiarowane Leopoldowi Ciborowskiemu w siedemdziesiątą rocznicę urodzin*, M. Zieliński, B. Pączek (red.), Gdynia 2014.

Rokiciński K., *Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich*, „Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, R. 46, nr 1, s. 151–171.

Schuman T., *Love Letter to America*, Los Angeles 1984.

Sekściński A., *Bezpieczeństwo wewnętrzne w ujęciu teoretycznym. Geneza i współczesne rozumienie w naukach politycznych*, „Kwartalnik Naukowy OAP UW e-Politikon" 2013, nr 6, s. 42–79.

Słownik angielsko-polski, Oxford 2002.

Słownik terminów z zakresu bezpieczeństwa narodowego, wyd. 6, Warszawa 2008.

Soloch P., Pietrzak P., *Szczyt NATO w Warszawie: uwarunkowania, rezultaty, wnioski dla Polski*, „Bezpieczeństwo Narodowe" 2016, nr 37–40, s. 13–31.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2022.

Sułek M., *Prognozowanie i symulacje międzynarodowe*, Warszawa 2010.

Świeboda H., *Prognozowanie zagrożeń bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2017.

Usewicz T., Keplin J., *Hybrid Actions and Their Effect on EU MaritimeSecurity*, „Journal on Baltic Security" 2023, t. 9, nr 1, s. 32–68. https://doi.org/10.57767/jobs_2023_001.

Zacher L.W., *Problemy i metody przewidywania przyszłości (przegląd tendencji w literaturze)*, w: *Czy warto myśleć o przyszłości?*, Warszawa 1996, s. 1–105.

Zacher L.W., *Trwały rozwój – utopia czy realna możliwość?*, „Problemy Ekorozwoju – Problems of Sustainable Development" 2008, t. 3, nr 2, s. 63–68.

Zasadzińska-Baraniewska A., *Zarządzanie kryzysowe wobec nowego typu zagrożeń – spotkanie eksperckie w Rządowym Centrum Bezpieczeństwa*, „Biuletyn Kwartalny Biura Analiz i Reagowania RCB" 2017, nr 19, s. 3–5.

Zdrodowski B., *Istota bezpieczeństwa*, w: *Wybrane problemy bezpieczeństwa wewnętrznego państwa*, A. Misiuk (red.), t. 34, Warszawa 2014, s. 32–50.

Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego. Koncepcje – struktury – funkcjonowanie*, Warszawa 2004.

Zięba R., *Współczesne wyzwania i zagrożenia dla bezpieczeństwa międzynarodowego*, „Stosunki Międzynarodowe – International Relations" 2016, t. 52, nr 3, s. 9–31. https://doi.org/10.7366/020909613201601.

Źródła internetowe

Bolzen S., *Die NATO muss auf grüne Männchen vorbereitet sein*, Die Welt, 17 VIII 2014 r., http://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.ht ml/ [dostęp: 27 I 2015].

Budowanie odporności państw członkowskich sojuszu – implementacja wytycznych NATO, Rządowe Centrum Bezpieczeństwa, 21 XII 2017 r., https://rcb.gov.pl/budowanie-odpornosci-panstw-czlonkowskich-sojuszu-implementacja-wytycznych-nato/ [dostęp: 20 XII 2018].

Commitment to enhance resilience, North Atlantic Treaty Organization, 8 VII 2016 r., https://www.nato.int/cps/en/natohq/official_texts_133180.htm [dostęp: 21 VIII 2022].

Cullen P., *Hybrid threats as a new 'wicked problem' for early warning*, Hybrid CoE, 4 VI 2018 r., https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ [dostęp: 12 X 2018].

https://mediweb.pl/slownik-nauk-i-specjalnosci-lekarskich [dostęp: 20 VIII 2022].

Jadczak A., *Zaatakowana przez hakerów DigiNotar ogłosiła upadłość*, Computer World, 23 IX 2011 r., https://www.computerworld.pl/news/Zaatakowana-przez-hakerow-DigiNotar-oglosila-upadlosc,375383.html [dostęp: 4 I 2019].

Lorenz W., *Szczyt NATO w Brukseli – przełomowy moment dla Sojuszu*, PISM, 15 VI 2021 r., https://www.pism.pl/publikacje/Szczyt_NATO_w_Brukseli__przelomowy_moment_dla_Sojuszu [dostęp: 10 VII 2022].

Matyasik G., *Jak wygląda polska odporność?*, INFOSECURITY24, 4 IV 2023 r., https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/jak-wyglada-polska-odpornosc [dostęp: 10 IX 2023].

MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf [dostęp: 7 X 2022].

NIK o bezpieczeństwie danych, Najwyższa Izba Kontroli, 16 V 2016 r., https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-danych. html [dostęp: 18 XI 2018].

Odporne NATO, Rządowe Centrum Bezpieczeństwa, https://archiwum.rcb.gov.pl/odporne-nato/ [dostęp: 20 XII 2020].

Odporność na zagrożenia tematem seminarium RCB, Rządowe Centrum Bezpieczeństwa, https://rcb.gov.pl/odpornosc-na-zagrozenia-tematem-seminarium-rcb/ [dostęp: 20 XII 2018].

Opas R., *Użyją art. 5? Stoltenberg nie wyklucza*, Wiadomości WP, 11 X 2022 r., https://wiadomosci.wp.pl/uzyja-art-5-stoltenberg-nie-wyklucza-6821910367021888a [dostęp: 11 X 2022].

Raubo J., *GlobState III, czyli zrozumieć świat i wykorzystać wiedzę do budowania sił zbrojnych*, Defence24, 13 XII 2020 r., https://defence24.pl/sily-zbrojne/globstate-iii-czyli-zrozumiec-swiat-i-wykorzystac-wiedze-do-budowania-sil-zbrojnych-komenatrz [dostęp: 7 VII 2022].

Reichborn-Kjennerud E., Cullen P., *What is Hybrid Warfare?*, Norwegian Institute of International Affairs, 2016 r., https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf [dostęp: 1 XII 2022].

Słownik języka polskiego PWN, https://sjp.pwn.pl/slowniki/odporno%C5%9B%C4%87.html [dostęp: 20 VIII 2022].

Williams J.W., *Critical Energy Infrastructure Protection Policy Research Series: Al-Qaida threats and strategies: the religious justification for targeting the international energy economy*, The Canadian Centre of Intelligence and Security Studies at Carleton University, marzec 2008 r., http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.612.473&rep=rep1&type=pdf [dostęp: 17 XI 2018].

Wytrzymałość materiałów – rodzaje, co to jest?, EBMIA, 30 VIII 2021 r., https://www.ebmia.pl/wiedza/porady/obrobka-porady/wytrzymalosc-materialow-rodzaje/ [dostęp: 23 VII 2022].

Kmdr por. rez. dr Jarosław Łukasz Keplin

Doktor w dziedzinie nauk społecznych w dyscyplinie nauki o bezpieczeństwie, adiunkt w Zakładzie Bezpieczeństwa Wewnętrznego Katedry Bezpieczeństwa Narodowego na Uniwersytecie Pomorskim w Słupsku. Służył m.in. w Dywizjonie Okrętów Podwodnych, 3 Flotylli Okrętów, pracował w Centrum Doktryn i Szkolenia Sił Zbrojnych. Uczestnik misji poza granicami państwa. Jego zainteresowania naukowe obejmują m.in. zagadnienia związane z bezpieczeństwem w wymiarze narodowym i międzynarodowym, problemy identyfikacji i analizy zagrożeń oraz formy oddziaływania państw i aktorów niepaństwowych na bezpieczeństwo państwa.