DOI: 10.4467/27204383TER.22.019.16339

ORCID: 0000-0003-1514-7657

MICHAŁ PIEKARSKI

Możliwe scenariusze zagrożeń terrorystycznych na terytorium Rzeczpospolitej Polskiej w kontekście zagrożeń hybrydowych

Abstrakt

W artykule został omówiony problem wykorzystania zamachów terrorystycznych jako narzędzia wojny hybrydowej. Za pomocą scenariuszowej metody prognozowania dokonano analizy prawdopodobnego przebiegu ataków na terytorium Rzeczpospolitej Polskiej.

Słowa kluczowe:

terroryzm,
zamach terrorystyczny,
wojna hybrydowa

W związku z sytuacją na Ukrainie 28 lutego 2022 r. wprowadzono w Polsce, po raz pierwszy od chwili wejścia w życie *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[1], stopień alarmowy BRAVO na terenie dwóch województw – podkarpackiego i lubelskiego. W dniu 15 kwietnia 2022 r. przedłużono czas jego obowiązywania oraz rozszerzono zasięg terytorialny na cały kraj. W czasie pisania niniejszego artykułu czas obowiązywania był wydłużony do końca czerwca. Wprowadzenie stopnia alarmowego BRAVO jest interesujące pod kątem badań nad potencjalnymi zagrożeniami terrorystycznymi na terytorium Rzeczpospolitej Polskiej.

[1] Tekst jednolity: DzU z 2021 r. poz. 2234, ze zm.

Podjęcie takich decyzji oznacza bowiem, że zgodnie z ustawą zaistniało (...) *zwiększone i przewidywalne zagrożenie wystąpieniem zdarzenia o charakterze terrorystycznym*[2]. W tej sytuacji nasuwa się pytanie o to, jaki jest możliwy charakter tego rodzaju zagrożeń w świetle aktualnej sytuacji międzynarodowej, przede wszystkim agresywnej polityki Federacji Rosyjskiej.

Celem niniejszego artykułu jest wskazanie i omówienie scenariuszy zagrożeń terrorystycznych na terytorium RP w kontekście zagrożeń hybrydowych. Poszukiwanie odpowiedzi na postawione pytanie badawcze samo w sobie jest wyzwaniem metodologicznym, gdyż nie doszło do wystąpienia zdarzeń o charakterze terrorystycznym, a jedynie mamy do czynienia z podwyższonym ryzykiem ich zaistnienia. To oznacza, że odpowiedź będzie miała charakter prognostyczny. W związku z powyższym za podstawę metodologiczną badań przyjęto scenariuszową metodę prognozowania, która polega na analizowaniu za pomocą scenariuszy możliwego przebiegu przyszłych trendów i ocenie ich wpływu na aktualnie diagnozowany problem. Scenariusze są uporządkowanymi opisami trendów oraz ich wpływu na badany obszar, a wynikiem ich zastosowania jest opis możliwego stanu końcowego lub – częściej – kilku możliwych stanów końcowych. Metodę tę wykorzystuje się m.in. w analizach z zakresu bezpieczeństwa i gospodarki[3]. W literaturze przedmiotu podaje się kilka różnych, jakkolwiek pod pewnymi względami podobnych, etapów procesu tworzenia i analizy scenariusza. Przykładowo Jay Ogilvy wyróżnia ich osiem, począwszy od wstępnych działań, na implementacji wniosków kończąc. Są to:

1. Wskazanie kluczowego zagadnienia (ang. *focal issue)*.
2. Identyfikacja najważniejszych czynników.
3. Opis czynników zewnętrznych.
4. Wskazanie krytycznych niepewności.
5. Opis wewnętrznej logiki scenariusza.
6. Stworzenie samych scenariuszy.
7. Analiza implikacji i dostępnych opcji.
8. Analiza wczesnych wskaźników odróżniających scenariusze.

Dla porównania Hannah Kosow i Robert Gaßner podają pięć etapów.

---

[2] Ustawa o działaniach antyterrorystycznych, art. 15 ust. 4.

[3] Szerzej w: J. Ogilvy, *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015 r., https://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/?sh=2de3fee5411a [dostęp: 18 V 2022].

Należą do nich:

1. Identyfikacja pola scenariusza.
2. Identyfikacja najważniejszego czynnika.
3. Analiza najważniejszego czynnika.
4. Generowanie scenariuszy.
5. Transfer scenariuszy (aplikacja)[4].

W pierwszej kolejności trzeba zatem zidentyfikować główny temat scenariusza. W przypadku badań opisywanych w niniejszej pracy było to zadanie łatwe, gdyż został on sformułowany w pytaniu badawczym. Wynika z niego także najważniejszy czynnik mający wpływ na analizowane scenariusze, tj. możliwe wykorzystanie zamachów terrorystycznych w działaniach hybrydowych prowadzonych przez Rosję na terenie Polski. Konieczne jest więc przeanalizowanie zagadnienia działań hybrydowych oraz wykorzystania w nich narzędzi terrorystycznych. Umożliwi to skonstruowanie scenariuszy i poddanie ich analizie, a ponadto pozwoli na ocenę możliwego wykorzystania zasobów systemu bezpieczeństwa państwa, a przede wszystkim jego integralnej części – systemu antyterrorystycznego.

Opisu najważniejszych czynników oraz konstruowania scenariuszy dokonano na podstawie dwóch zbiorów informacji. Pierwszym są dostępne, wiarygodne informacje dotyczące dotychczasowej rosyjskiej polityki i sposobu użycia siły w stosunkach międzynarodowych. Drugim – informacje na temat możliwych sposobów dokonywania zamachów terrorystycznych, zarówno w szerszej, strategicznej skali, jak i na poziomie taktycznym i technicznym.

Metoda scenariuszowa była już zastosowana w analizie polskiego systemu antyterrorystycznego[5]. Za jej pomocą klarownie przedstawiono wyzwania związane ze współczesnym charakterem tego rodzaju zagrożeń. Dodatkową wartością jest łatwość wykorzystania tego rodzaju analiz w celach szkoleniowych i dydaktycznych[6].

[4] H. Kosow, R. Gaßner, *Methods of Future and Scenario Analysis. Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [dostęp: 22 VI 2022].

[5] M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020, s. 158–207.

[6] Por. J. Sovolainen i in., *Hybrid CoE Working Paper 5. Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans*, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [dostęp: 29 IV 2022].

Analiza zagrożeń hybrydowych w kontekście zagrożeń terrorystycznych – uwagi ogólne

W literaturze przedmiotu nie ma jednej, precyzyjnej, ogólnie przyjętej definicji zagrożeń hybrydowych. Na sposób ich postrzegania niewątpliwy wpływ miały dwa konflikty zbrojne. Pierwszym z nich była wojna Izraela z Hezbollahem, która przez część analityków została nazwana hybrydową[7]. Drugim, skutkującym częstszym i szerszym użyciem tego terminu, są wydarzenia w Ukrainie mające swój początek w 2014 r. Aneksja Krymu została bowiem przeprowadzona przy pomocy oddziałów wojskowych używających siły w ograniczonym zakresie, występujących początkowo bez oznaczeń przynależności państwowej. Po tym sukcesie Rosjanie rozpoczęli działania w Donbasie, w których posługiwali się nieregularnymi formacjami zbrojnymi, złożonymi zarówno z miejscowych prorosyjskich ochotników czy najemników, jak i z żołnierzy wojsk specjalnych oraz sił regularnych przysłanych z Rosji, mimo że oficjalnie nie brała ona czynnego udziału w tej wojnie[8]. Nie oznacza to jednak, że o zagrożeniach hybrydowych mówi się tylko w kontekście tych dwóch konfliktów. Powstają prace poświęcone szerszym analizom tego pojęcia i kontekstom jego stosowania. Na przykład Robert Seely w artykule z 2017 r. zwraca uwagę, że termin „hybrydowy" w odniesieniu do konfliktów zbrojnych jest używany najczęściej w jednym z trzech kontekstów: 1) „zamrożonych", długotrwałych konfliktów będących skutkiem polityki Rosji na obszarze postradzieckim, 2) wojen nowej generacji, często utożsamianych z tezami przypisywanymi rosyjskim wojskowym, zwłaszcza Siergiejowi Gierasimowowi, oraz 3) kinetycznych i niekinetycznych działań służb wywiadowczych określanych jako środki aktywne[9]. Charakteryzuje on również narzędzia wykorzystywane przez Rosję jako należące do jednego z sześciu obszarów: 1) rządzenie (obejmuje także sferę kultury, religii i prawa), 2) gospodarka i energia, 3) polityka i przemoc polityczna, 4) siła militarna, 5) dyplomacja oraz 6) działania informacyjne i dezinformacyjne. W tych szeroko ujętych kategoriach mieszczą się węższe formy działań – na przykład wykorzystywanie kultury, w tym organizacji kulturalnych, w celach politycznych, wykorzystywanie energii do szantażu energetycznego, zabójstwa na tle politycznym, tworzenie prorosyjskich

[7] F. Hoffman, *Conflict in the 21st Century: The Rise of the Hybrid Wars,* https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 29 IV 2022].

[8] Szerzej w: L.M. Nadolski, *Kampania zimowa w 2015 roku na Ukrainie,* Bydgoszcz 2017, s. 43–44.

[9] R. Seely, *Defining Contemporary Russian Warfare,* „The RUSI Journal" 2017, t. 162, nr 1, s. 50–59.

organizacji, także zbrojnych. Środki należące do wymienionych powyżej kategorii mogą być stosowane jednocześnie. Co ważne, dochodzi do zatarcia tradycyjnych podziałów między użyciem siły militarnej a użyciem środków pozamilitarnych oraz między pokojem a wojną. Taki sposób wykorzystania tych środków przez państwo prowadzi do zjawiska użycia jako broni (narzędzia polityki) licznych narzędzi i czynników, określanych w języku angielskim jako *weaponisation*. Jak pisze Mark Galeotti, może to się przejawiać m.in. w wykorzystywaniu pomocy humanitarnej i medycznej, zorganizowanych grup przestępczych, prawa międzynarodowego, kultury i informacji w celach politycznych[10]. Autorzy raportu *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*[11] wskazują, że zagrożenia hybrydowe mają następujące cechy:

- korzystają z szerokiego spektrum narzędzi wojskowych, politycznych, gospodarczych, cywilnych i informacyjnych,
- w nietradycyjny sposób atakują sfery funkcjonowania społeczeństwa podatne na atak,
- w nowatorski sposób synchronizują używane środki,
- w sposób intencjonalny wykorzystują niepewność, niejasność i sposób postrzegania otoczenia przez atakowane państwo, by ograniczyć ryzyko wykrycia,
- mogą zostać zauważone i zidentyfikowane w późnej fazie realizacji.

Te wszystkie czynniki nie lokują jednoznacznie zagrożeń terrorystycznych w obrębie działań hybrydowych. Na możliwość wystąpienia działań terrorystycznych jako elementu działań hybrydowych zwracają jednak uwagę różni badacze problemu. Przemysław Gasztold i Aleksandra Gasztold wskazują, że wspomniana już wojna Izraela z Hezbollahem była konfliktem pomiędzy państwem a organizacją stosującą metody terrorystyczne, która mogła być wykorzystywana przez inne państwo (Iran) do prowadzenia działań terrorystycznych przeciwko innym państwom[12].

[10] M. Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War*, New York–London 2022.

[11] P.J. Cullen, E. Reichborn-Kjennerud, *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf, s. 10 [dostęp: 20 V 2022].

[12] A. Gasztold, P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, „Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [dostęp: 28 V 2022].

Autorzy ci zauważają ponadto, że techniki typowe dla terroryzmu są stosowane podczas konfliktu zbrojnego w Ukrainie.

Interesujące spostrzeżenia na temat zagrożeń hybrydowych można odnaleźć również w literaturze z lat wcześniejszych. W artykule opublikowanym w 1998 r. Andrzej Makowski i Krzysztof Kubiak analizują możliwość wykorzystania czynnika militarnego w sposób niejawny i pośredni w działaniach prowadzonych tak, aby utrudnić lub uniemożliwić wskazanie ich faktycznego organizatora. Chodziło o działania wymierzone w ważne obiekty wojskowe i gospodarcze, osoby zajmujące kluczowe stanowiska w państwie w celu wywołania poczucia zagrożenia wśród mieszkańców atakowanego kraju, podważenia ich zaufania do władz i instytucji państwowych, skomplikowania sytuacji międzynarodowej i wywołania niepokojów społecznych[13]. Autorzy wspomnianego artykułu wskazują, że do takich działań mogą zostać zaangażowane osoby zamieszkujące terytorium danego państwa, które strona atakująca pozyska do współpracy, członkowie zagranicznych organizacji terrorystycznych lub przestępczych (de facto najemnicy), jak również żołnierze, zwłaszcza wojsk specjalnych, państwa atakującego, biorący udział w działaniach upozorowanych na akcje lokalnych ugrupowań ekstremistycznych. Uwagi te korespondują z treścią artykułu Łukasza Skonecznego z 2015 r.[14] Zauważył on, że działania hybrydowe mogą być stosowane właśnie po to, aby nie dopuścić do przekroczenia progu użycia siły, ponieważ byłoby to jednoznacznie zinterpretowane jako otwarta agresja, a więc zmuszałoby do zareagowania na przykład sojuszników zaatakowanego państwa. Użycie metod terrorystycznych, które ten autor także zalicza do grupy środków mogących mieć zastosowanie w działaniach hybrydowych, pozwala wykreować sytuację niejasną i niepewną pod względem reakcji.

Te ogólne analizy nie prowadzą jednak do szczegółowych wniosków na temat możliwych scenariuszy sytuacji kryzysowych. Terroryzm jest bowiem zjawiskiem zróżnicowanym i niejednolitym pod względem strategii oraz taktyk działania. Wynikają one przede wszystkim z ideologii organizacji stosujących metody terrorystyczne, środowiska, w którym działają, reakcji atakowanych państw oraz innych zmiennych. Na dobór taktyki mają z kolei wpływ m.in. bieżące uwarunkowania, przyjęta szersza strategia,

---

[13] A. Makowski, K. Kubiak, *Terroryzm jako sposób prowadzenia wojny?*, „Raport – wojsko – technika – obronność" 1998, nr 4, s. 41–43.

[14] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne: *Wojna hybrydowa*, s. 39–50.

sytuacja operacyjna, wyszkolenie i uzbrojenie[15]. Ważną zmienną jest prowadzenie działań terrorystycznych bezpośrednio lub pośrednio przez państwo. Bartosz Bolechów pisze o kilku stopniach wspierania działalności terrorystycznej przez państwo, tj.: pełnej kontroli (terroryzm państwowy), rekrutacji i szkoleniu osób do działań terrorystycznych przez organy państwowe, znacznym stopniu kontroli nad organizacją terrorystyczną, dostarczaniu wsparcia grupie wysoce autonomicznej, pomocy dla grupy faktycznie niezależnej, wsparciu biernym[16]. W przypadku działań hybrydowych najbardziej prawdopodobne są cztery pierwsze stopnie, zapewniające wpływ na dobór celów i metod działania. Wsparcie państwowe oznacza zapewnienie szkolenia, finansowania, wyposażenia, informacji rozpoznawczych, bezpiecznego schronienia oraz innych form pomocy (np. wsparcie ideologiczne lub dyplomatyczne)[17]. Płynie z tego ważny wniosek, że tego rodzaju działania wspomagane lub prowadzone przez aktora państwowego będą mogły być realizowane z wykorzystaniem większych zasobów niż zasoby będące w dyspozycji organizacji terrorystycznych niemających takiej protekcji. Należy zatem przyjąć, że w analizie poświęconej prowadzeniu działań terrorystycznych w ramach szerzej postrzeganych działań hybrydowych jednym z zasadniczych czynników, które muszą zostać uwzględnione, jest udział podmiotów mogących wspierać lub realizować ich działania hybrydowe oraz cele polityczne.

Działania hybrydowe w środowisku bezpieczeństwa Polski

Z analizy dotyczącej środowiska bezpieczeństwa Polski wynika, że obecnie jednym z głównych czynników, które je kształtują, są agresywne działania Federacji Rosyjskiej. W obowiązującej aktualnie *Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* wskazano, że (...) *Federacja Rosyjska prowadzi również działania poniżej progu wojny (o charakterze hybrydowym), niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także podejmuje wszechstronne i kompleksowe działania za pomocą środków*

[15] Szerzej w: B. Bolechów, *Polityka antyterrorystyczna w świetle badań nad terroryzmem*, Wrocław 2012, s. 134–174.

[16] Tamże, s. 173.

[17] Tamże, s. 174.

pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych[18]. Działania poniżej progu wojny, w tym działania o charakterze hybrydowym, pozostają, jak już wspomniano, istotnym środkiem prowadzenia polityki, służącym podmiotom państwowym i pozapaństwowym do osiągania swoich celów. W aktywności Rosji, także podczas wojny z Ukrainą, jest widoczna strategia zakładająca odtworzenie i utrzymanie jej dawnej potęgi, jak również postrzeganie Zachodu jako zagrożenia. Aby to zagrożenie zneutralizować, Rosja dąży do wyparcia albo ograniczenia amerykańskiej obecności w Europie oraz do zminimalizowania wpływów europejskich i kontrolowania tego kontynentu. Marek Menkiszak pisze, że Federacja Rosyjska wyznaczyła sobie cztery główne cele strategiczne. Są to:

1. *Strategiczna kontrola nad obszarem postradzieckim (z czasowym wyłączeniem państw bałtyckich).*
2. *Stworzenie buforowej strefy bezpieczeństwa w Europie Środkowej.*
3. *Minimalizacja wpływów i obecności USA w Europie.*
4. *Maksymalizacja wpływów Rosji w Europie*[19].

Ich osiągnięcie umożliwiłoby stworzenie nowej architektury bezpieczeństwa europejskiego, w której Rosja odgrywałaby ważną rolę gospodarczą i polityczną. Działania hybrydowe są jednym z narzędzi pozwalających na wywieranie presji na państwa regionu. Ich celem może być wymuszenie określonego zachowania na państwach sąsiadujących z Rosją oraz zniechęcenie państw sojuszniczych do udzielenia pomocy zaatakowanym. To może się przekładać na bardziej szczegółowe cele operacyjne dotyczące poszczególnych państw. Autor niniejszego opracowania w 2019 r. zidentyfikował na przykład następujące cele działań hybrydowych wymierzonych w Polskę:

1. Uniemożliwienie użycia polskich i sojuszniczych sił zbrojnych oraz infrastruktury (dróg, linii kolejowych, portów, lotnisk, miejsc postojowych) w działaniach pomocowych dla Litwy, Łotwy i Estonii.
2. Zmuszenie Polski do wycofania się z wszelkich działań sprzecznych z interesami Rosji.
3. Potencjalnie – zmuszenie Polski do umożliwienia ustanowienia połączenia lądowego Rosji z Obwodem Kaliningradzkim lub

[18] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf, s. 6 [dostęp: 22 VI 2022].

[19] M. Menkiszak, *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji*, Warszawa 2019, s. 12.

przynajmniej doprowadzenie do przerwania połączenia lądowego Polski z Litwą.

4. Potencjalnie – zmuszenie Polski do usunięcia sił amerykańskich i innych sił NATO ze swojego terytorium[20].

Warto zauważyć, że kryzys migracyjny w 2021 r. był elementem działań hybrydowych i wyraźnie wpisywał się w punkt drugi z wyżej wymienionych, gdyż inspirowana przez władze białoruskie – za ewidentną wiedzą i zgodą władz Rosji – migracja osób do Polski (oraz innych państw UE) była odwetem za wsparcie prodemokratycznych protestów na Białorusi. Podczas tego kryzysu nie tylko została wywarta bezpośrednia presja na państwa i społeczeństwa, w tym służby odpowiedzialne za ochronę granic, lecz także starano się stworzyć narrację pokazującą Polskę, Litwę i Łotwę jako państwa niechętne uchodźcom i łamiące prawa człowieka. Dążono również do spolaryzowania opinii publicznej na tle kryzysu i wywołania kolejnych podziałów wewnętrznych[21].

To oznacza, że działania terrorystyczne jako część działań hybrydowych mogą być prowadzone z zamiarem osiągnięcia podobnych celów i można dopatrywać się podobieństw między nimi a kryzysem migracyjnym. Widoczne są cztery elementy, które charakteryzują działania terrorystyczne będące częścią działań hybrydowych i czynią je podobnymi do innych stosowanych narzędzi, na przykład presji migracyjnej.

Po pierwsze, państwo, które staje się celem działań terrorystycznych, jest zmuszone zmierzyć się przede wszystkim z bieżącym zagrożeniem bezpieczeństwa wewnętrznego. Może to oznaczać przekierowanie zasobów systemu bezpieczeństwa państwa na działania antyterrorystyczne oraz kontrterrorystyczne, zwłaszcza jeśli siły i środki przeznaczone do wykonywania tych zadań okażą się lub mogą okazać się niewystarczające. Koszty związane z samymi atakami oraz utrzymywaniem zasobów potrzebnych do ich powstrzymywania mogą także być wyższe niż korzyści wynikające z polityki prowadzonej przez atakowane państwo, co będzie prowadzić do jej szybkiej zmiany.

Po drugie, ataki terrorystyczne mogą wywołać nowe podziały społeczne oraz pogłębić istniejące, zwłaszcza jeśli są prowadzone przez państwo,

[20] M. Piekarski, *Polish Armed Forces and hybrid war: current and required capabilities*, „The Copernicus Journal of Political Studies" 2019, nr 1, s. 43–64.

[21] Szerzej w: A.M. Dyner, *Kryzys graniczny jako przykład działań hybrydowych*, Polski Instytut Spraw Międzynarodowych, 2 II 2022 r., https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [dostęp: 22 VI 2022].

które pozoruje działania bytów faktycznie istniejących lub celowo wykreowanych (ataki pod fałszywą flagą).

Po trzecie, sposób reakcji państwa, który może prowadzić do ograniczenia praw, wolności i swobód obywatelskich, na przykład przez wprowadzanie zaostrzonych środków bezpieczeństwa, może skutkować kolejnymi podziałami społecznymi.

Po czwarte, należy mieć na uwadze, że działania prowadzone bezpośrednio przez aktora państwowego lub z jego wsparciem będą charakteryzować się potencjalnie szerszym zakresem środków bojowych, taktyk i technik działania, wykraczających poza obserwowane w ostatnich latach modus operandi sprawców zamachów terrorystycznych, którzy takim wsparciem nie dysponowali.

Te cztery elementy pozwalają doprecyzować scenariusze możliwych sytuacji kryzysowych. Nie jest bowiem zasadne analizowanie każdego możliwego przypadku zamachu terrorystycznego, lecz jedynie takich, które mieszczą się w tak zarysowanych warunkach brzegowych.

Możliwe scenariusze ataków

W niniejszej, zasadniczej części artykułu została przedstawiona analiza scenariuszy (z ich możliwymi wariantami) dotyczących wykorzystania terroryzmu jako narzędzia wojny hybrydowej. Scenariusze podzielono według kryterium potencjalnego celu ataku. Ten cel, a dokładniej jego rodzaj, jest czynnikiem porządkującym wewnętrzną logikę scenariusza, czyli możliwe korzyści i ograniczenia z punktu widzenia sprawców. Drugim czynnikiem ważnym dla wewnętrznej logiki scenariusza jest współistnienie innych form nacisku. Przy konstruowaniu scenariuszy wzięto pod uwagę stan prawny i organizacyjny w maju 2022 r. Pytaniem otwartym, na które w czasie powstawania artykułu nie można było udzielić odpowiedzi, jest wpływ konfliktu w Ukrainie na aktywność militarną i pozamilitarną Rosji.

Scenariusz 1. Zamach terrorystyczny wymierzony w infrastrukturę i sprzęt wojskowy

Słowo „wojna", będące jednym z członów pojęcia wojny hybrydowej, budzi skojarzenia z siłami zbrojnymi. Prawdopodobnym scenariuszem może zatem wydawać się atak na obiekty wojskowe. Instalacje wojskowe z definicji są ważne dla obronności państwa. Ich uszkodzenie lub zniszczenie oznacza

zmniejszenie potencjału obronnego państwa, a więc zwiększa podatność na presję militarną, w tym przypadku ze strony Rosji. Te same mechanizmy mogą zaistnieć w sytuacji ataku na przebywające w Polsce oddziały i pododdziały sił zbrojnych państw sojuszniczych. Należy jednak zauważyć, że osłabienie w ten sposób potencjału militarnego jest zadaniem trudnym. Przykładowo według dostępnych danych Siły Zbrojne Rzeczypospolitej Polskiej posiadały w 2021 r. 797 czołgów, 1611 bojowych wozów piechoty, 751 dział i moździerzy[22]. Trudno się spodziewać, aby jakiekolwiek działania terrorystyczne zdołały odczuwalnie osłabić ich potencjał. Część infrastruktury można względnie łatwo zastąpić inną. Na przykład zniszczone lub uszkodzone stałe stacje radiolokacyjne systemu Backbone mogą zostać zastąpione urządzeniami mobilnymi. Przy tym części obiektów nie byłoby łatwo zaatakować metodami typowymi dla organizacji terrorystycznych.

Sytuacja zmienia się, gdy możliwe cele zawęzi się jedynie do obiektów trudnych do łatwego zastąpienia, których uszkodzenie będzie miało wyraźny wpływ na zdolności SZ RP. Dla przykładu mniejszym zasobem pod względem liczebności są samoloty bojowe. Siły Powietrzne są wyposażone obecnie w 48 samolotów F-16C/D Block 52+, 29 samolotów MiG-29 oraz 18 samolotów Su-22M4/UM3K[23], przy czym dwa ostatnie typy zostaną wkrótce wycofane na rzecz 32 samolotów F-35A. Dokonanie ataku skutkującego zniszczeniem lub uszkodzeniem nawet tylko kilku samolotów bojowych spowoduje szkody w mieniu wojskowym, które należy szacować na dziesiątki milionów dolarów. Ponadto oznacza to trwałe lub czasowe wyłączenie z eksploatacji samolotów, których nie będzie można użyć do szkolenia i innych działań, na przykład rozpoznawczych lub ochrony własnej i sojuszniczej przestrzeni powietrznej.

Opisywany scenariusz miał swój odpowiednik w rzeczywistości. W 1981 r. celem ataku terrorystycznego stała się baza lotnicza Muñiz na wyspie Portoryko. Sprawcy zdołali podłożyć ładunki wybuchowe pod 11 samolotów typu A-7D i F-104[24]. Gdyby podobny atak zdarzył się w Polsce, zniszczenie lub uszkodzenie już ośmiu samolotów F-16 skutkowałoby wyeliminowaniem jednej szóstej posiadanych maszyn tego typu. Atak mógłby zostać dokonany przez infiltrację bazy lotniczej lub za pomocą

[22] *The Military Balance 2021*, The International Institute for Strategic Studies.

[23] Tamże.

[24] https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [dostęp: 28 V 2022].

bezzałogowych statków powietrznych, zwłaszcza jeśli sprawcy byliby w stanie rozpoznać dogodną okazję do tego rodzaju działań.

Potencjalnymi celami ataków w SZ RP mogą być również inne urządzenia i systemy występujące w niewielkiej liczbie i trudne do szybkiego odtworzenia. Oczywistym ograniczeniem jest w tym przypadku konieczność identyfikacji przez sprawców adekwatnych celów ataku (urządzeń, sprzętu wojskowego) oraz uzyskanie dostępu do atakowanego obiektu, aby m.in. pozyskać informacje na temat jego działalności oraz zabezpieczeń.

Należy przy tym mieć na uwadze nie tylko stricte materialne i wojskowe konsekwencje takiego scenariusza. Skuteczny atak będzie bowiem bardzo łatwy do wykorzystania w działalności propagandowej i dezinformacyjnej, eksponującej fakt, że doszło do zamachu na obiekt wojskowy i zniszczenia sprzętu wojskowego. Może to obniżyć poziom zaufania społecznego do sił zbrojnych oraz polityki obronnej państwa.

Scenariusz 1a. Zamach terrorystyczny wymierzony w personel wojskowy

Scenariusz zakłada atak wymierzony nie w sprzęt wojskowy, lecz w żołnierzy. Atak może zostać przeprowadzony na terenie wojskowym (jak w przypadku zamachu z Fort Hood w 2008 r.) lub poza terenami i obiektami wojskowymi (jak w przypadku ataków we Francji w 2013 r.)[25] i następnie wykorzystany propagandowo. Z punktu widzenia sprawców istotnym wariantem tego scenariusza jest możliwość dokonania ataku na osoby przebywające poza obiektami wojskowymi – w miejscach zamieszkania, miejscach publicznych (środki transportu, placówki handlowe) i innych łatwo dostępnych, gdyż ułatwia to jego zaplanowanie i przeprowadzenie. Także zdobycie informacji na temat celu (konkretnej osoby lub osób) może być prostsze. Celem może być przede wszystkim personel wymagający długotrwałego szkolenia i trudny do zastąpienia. Są to osoby takie, jak:

- kadra dowódcza, zwłaszcza osoby w stopniach generalskich,
- personel latający oraz żołnierze wojsk specjalnych, członkowie załóg jednostek pływających,
- osoby zajmujące specjalistyczne stanowiska, zwłaszcza związane z obsługą ważnych systemów uzbrojenia oraz wsparcia i zabezpieczenia i mające dostęp do informacji wrażliwych,

[25] Szerzej w: M. Piekarski, K. Wojtasik, *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020.

- osoby mogące w przyszłości zająć ważne stanowiska (osoby uczęszczające na kursy, szkolenia, kształcące się w akademiach wojskowych).

Atak na takie osoby oznacza, że podobnie jak w scenariuszu poprzednim jest możliwe zadanie poważnych strat siłom zbrojnym. Pozbawienie wojska osoby mającej specjalistyczną wiedzę i kwalifikacje może mieć negatywne skutki psychologiczne, podobnie jak w poprzednim scenariuszu. Należy zauważyć, że konsekwencje miękkie (psychologiczne i społeczne) będą poważniejsze niż twarde. Na przykład skuteczny zamach na dowódcę oddziału lub związku taktycznego spowoduje, że jego miejsce szybko zajmie osoba będąca na stanowisku zastępcy dowódcy. W przypadku innego personelu również jest mało prawdopodobne, aby jedna osoba była jedyną mającą unikalne kompetencje, w związku z czym będzie możliwe jej zastąpienie inną. Jednak skutki psychologiczne mogą być poważne zarówno dla sił zbrojnych, jak i dla społeczeństwa, gdyż atak na żołnierza, zwłaszcza zajmującego stanowisko dowódcze, może podważyć zaufanie społeczne do sił zbrojnych, a także mieć negatywny wpływ na morale żołnierzy.

W tym scenariuszu atak może mieć formę zabójstwa lub uprowadzenia osoby (na podobieństwo uprowadzenia gen. Jamesa Doziera w 1981 r. we Włoszech[26]). Ten drugi wariant należy ocenić jako bardziej skomplikowany i wiążący się z większym ryzykiem dla sprawców. Możliwe jest bowiem rozpowszechnianie wizerunku uprowadzonej osoby, zmuszenie jej do wygłoszenia oświadczenia o treści podyktowanej przez sprawców lub wręcz dokonanie egzekucji i upublicznienie jej nagrania. Co ważne, uprowadzona osoba może zostać nakłoniona lub zmuszona do ujawnienia informacji niejawnych. W tym scenariuszu zagrożone są także rodziny osób, które mogą być celem ataku. Ponadto należy brać pod uwagę ewentualność ataku wymierzonego w przebywających w Polsce żołnierzy sił zbrojnych państw sojuszniczych. Wówczas grupą docelową przekazu generowanego przez taki atak byłaby także opinia publiczna państw sojuszniczych.

Scenariusz 1b. Zamach terrorystyczny wymierzony w infrastrukturę i sprzęt służb policyjnych, wywiadowczych lub kontrwywiadowczych

Scenariusz jest odpowiednikiem scenariusza 1, z tą różnicą, że celem ataku są obiekty i wyposażenie wykorzystywane przez służby policyjne (Policję, Straż Graniczną) lub służby specjalne. Także w tym przypadku prawdopodobnym

[26] T. Philips, *The Dozier Kidnapping: Confronting the Red Brigades*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [dostęp: 28 V 2022].

celem są ważne urządzenia, trudne do szybkiego odtworzenia lub zastąpienia, jak również wywołanie zakłóceń w ich pracy, które utrudnią bieżące funkcjonowanie tych służb. Należy wskazać, że w przeciwieństwie do większości instalacji wojskowych obiekty służb policyjnych, takie jak placówki Straży Granicznej czy komendy Policji, są miejscem wykonywania czynności z udziałem osób cywilnych. Zamach wymierzony w siedzibę komendy Policji może więc znacznie obniżyć poziom zaufania do tej służby.

Scenariusz 1c. Zamach terrorystyczny wymierzony w personel służb policyjnych, wywiadowczych lub kontrwywiadowczych

Scenariusz jest odpowiednikiem scenariusza 1a. Jedyną różnicą jest tożsamość osoby lub osób, które są celem zamachu. Mogą to być przede wszystkim ludzie zajmujący ważne stanowiska w służbie śledczej lub kontrterrorystycznej Policji, komendanci Policji oraz osoby na kluczowych stanowiskach w służbach wywiadowczych i kontrwywiadowczych. Także w tym przypadku istotne może być psychologiczne i medialne znaczenie takiego ataku, podobnie jak w scenariuszu 1a.

Scenariusz 2. Atak na obiekt infrastruktury krytycznej

Scenariusz zakłada atak wymierzony w systemy oraz wchodzące w ich skład obiekty, urządzenia, instalacje i usługi, uznawane za infrastrukturę krytyczną w myśl przepisów *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[27], w tym zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, transportowe, zaopatrzenia w żywność i wodę, zapewniające ciągłość działania administracji publicznej.

Celem zamachu na takie obiekty może być zarówno zakłócenie lub uniemożliwienie ich funkcjonowania, jak i wywołanie lęku w społeczeństwie oraz podważenie zaufania obywateli do władz. Z tego powodu najbardziej prawdopodobnym celem ataku będą te obiekty i systemy, których zakłócenie okaże się najszybciej odczuwalne i możliwe do wykorzystania propagandowego. Można wskazać kilka możliwych wariantów tego scenariusza, które różnią się szczegółowym celem ataku.

Scenariusz 2a. Atak na infrastrukturę elektroenergetyczną

Scenariusz zakłada przeprowadzenie ataku wymierzonego w system elektroenergetyczny, a więc odpowiedzialny za wytwarzanie i dystrybucję

[27] Tekst jednolity: DzU z 2022 r. poz. 261, ze zm.

energii elektrycznej. Aby taki atak był skuteczny, sprawcy muszą zakłócić lub przerwać jeden z tych procesów. W Polsce energia elektryczna jest wytwarzana w elektrowniach różnego typu – cieplnych, wodnych, wiatrowych, jak również może być importowana z państw sąsiednich. Z uwagi na specyfikę obiektów energetycznych i ich zróżnicowanie zakłócenie lub przerwanie ich pracy może być trudne. Potencjalnie łatwiejszy byłby atak na sieć przesyłową. Jest ona położona na dużym obszarze i składa się z linii napowietrznych oraz punktów węzłowych (stacji elektroenergetycznych). Atak na takie instalacje, poprzez ostrzał z broni palnej, mechaniczne przewrócenie słupów czy podłożenie urządzeń wybuchowych, może doprowadzić do przerwania dostaw prądu do odbiorców, jak również spowodować przerwanie linii prowadzących z elektrowni[28]. W kontekście wojny hybrydowej należy uznać za prawdopodobne, że atak może zostać dokonany w sposób skoordynowany i doprowadzić do przerwania sieci zasilającej jedną lub nawet kilka dużych aglomeracji miejskich. Skonstruowanie urządzeń wybuchowych pozwalających na przerwanie linii z powodu wysadzenia słupów powinno być względnie łatwe w przypadku korzystania ze wsparcia służb wywiadowczych i wojsk specjalnych państwa, w tym przypadku Rosji, lub działań prowadzonych bezpośrednio przez te służby i wojska. Ataki na system elektroenergetyczny mogą być kontynuowane również po przywróceniu dostaw.

Konsekwencje tego rodzaju ataków mogą okazać się katastrofalne. Przerwanie dostaw energii do dużej aglomeracji miejskiej będzie oznaczać zahamowanie produkcji przemysłowej, działalności sektora usług, zakłócenie pracy szpitali oraz systemów komunikacyjnych i telekomunikacyjnych. Awaryjne, lokalne źródła zasilania (np. generatory) mogą zapewnić energię tylko niektórym odbiorcom i tylko przez określony czas. Prawdopodobne jest zaistnienie efektu kaskadowego, ponieważ wystąpią kolejne sytuacje kryzysowe. Przykładowo przerwanie dostaw prądu może wymusić ewakuację pacjentów szpitali, a jako że nie będą one mogły przyjmować nowych chorych, więc i te osoby będą musiały zostać przetransportowane do innych miast. Można spodziewać się także paraliżu systemu komunikacyjnego oraz innych systemów.

Atak tego rodzaju, nawet skutkujący tylko częściowym pozbawieniem zasilania, będzie wykorzystany w działaniach psychologicznych, mających

[28] Szerzej w: *IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector*, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [dostęp: 22 VI 2022].

na celu podważenie zaufania do władz państwowych oraz instytucji odpowiedzialnych za bezpieczeństwo państwa, i może mieć dalekosiężne skutki społeczne i polityczne.

Scenariusz 2b. Atak na infrastrukturę paliwową

Scenariusz zakłada atak wymierzony w instalacje i systemy służące do produkcji, transportu oraz dystrybucji paliw płynnych. Podobnie jak w przypadku infrastruktury energetycznej także te systemy składają się z miejsc wytwarzania lub importu paliw (rafinerie, kopalnie, platformy wydobywcze, terminale przeładunkowe) oraz infrastruktury transportowej. Zasadnicze różnice polegają w tym przypadku na możliwości magazynowania paliw (ropy naftowej, benzyny, gazu ziemnego) oraz zróżnicowaniu metod ich transportu (rurociągi, transport kolejowy, transport drogowy).

Szczególnie atrakcyjne z punktu widzenia sprawców mogą być ataki na infrastrukturę przeładunkową, magazyny paliw oraz transporty. Zakłócenie dostaw może nie tylko prowadzić do lokalnych braków paliw, lecz także mieć szersze konsekwencje. Przykładowo atak na morskie instalacje przeładunkowe gazu (terminal w Świnoujściu czy planowana instalacja pływająca w Zatoce Gdańskiej) może stanowić element działań powiązanych z presją ekonomiczną i polityczną, np. spowodowaniem kryzysu przez obce państwo występujące jednocześnie z ofertą wznowienia dostaw drogą lądową czy też innych korzyści[29].

Tego rodzaju zamach może być jedynie wstępem do akcji dezinformacyjnej, w której będą przedstawiane fałszywe informacje, sugerujące dużo większe straty i zakłócenia w dostawach paliw. To z kolei ma prowadzić do nieprzemyślanych działań osób prywatnych (np. wykupywania paliw w handlu detalicznym), co zaobserwowano po cyberataku na rurociąg Colonial Pipeline w USA.

Scenariusz 2c. Atak na infrastrukturę transportową

W tym scenariuszu atak jest wymierzony w obiekty i systemy związane z transportem drogowym, kolejowym, morskim i lotniczym. Może to być atrakcyjna opcja dla państwa prowadzącego działania hybrydowe z uwagi na znaczenie tych obiektów dla systemu obronnego państwa oraz funkcjonowania gospodarki. Dla przykładu, gdyby udało się zablokować ruch

[29] Szerzej w: M. Piekarski, *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską*, „Wschodnioznawstwo" 2020, t. 14, s. 177–195.

w porcie morskim takim jak Gdańsk, wywołałoby to poważne konsekwencje gospodarcze związane z opóźnieniami w transporcie towarów, które musiałyby oczekiwać na udrożnienie portu lub zostać przeładowane w innym miejscu, co jest czasochłonne. Do próby blokady szlaków komunikacyjnych może dojść w czasie kryzysu i wówczas atak miałby szersze konsekwencje.

Jest to widoczne w kontekście wojny w Ukrainie. Polska to w tym przypadku państwo tranzytowe, przez które są transportowane środki pomocy dla zaatakowanego kraju, w tym sprzęt wojskowy. Jednocześnie w początkowym etapie konfliktu przez Polskę przemieszczały się duże grupy uchodźców, jak również było przewożone zboże, którego Ukraina nie mogła eksportować z powodu zablokowania czarnomorskich portów. Podjęcie działań terrorystycznych mających na celu sparaliżowanie choćby jednego dużego węzła kolejowego, takiego jak węzeł krakowski czy wrocławski, mogłoby w takiej sytuacji mocno skomplikować te formy pomocy Ukrainie.

Scenariusz 3. Atak na cel symboliczny

Scenariusz zakłada przeprowadzenie ataku na cel mający znaczenie nie gospodarcze lub militarne, lecz przede wszystkim symboliczne. Mogą to być osoby, miejsca lub przedmioty, takie jak miejsca kultu religijnego, zabytki, pomniki, oraz wydarzenia typu manifestacje czy imprezy masowe.

Tego rodzaju atak ma na celu wywołanie polaryzacji w społeczeństwie. Szczególnie atrakcyjne dla sprawców jest przeprowadzenie ataku pod fałszywą flagą, a więc w sposób upozorowany na działania innego aktora (organizacji lub ruchu ekstremistycznego). Po ataku możliwe jest dokonanie kolejnego, również mającego sugerować działania osób o innej (przeciwnej) orientacji ideologicznej. Celem jest suponowanie istnienia konfliktu głębszego niż faktycznie istniejący, sprowokowanie faktycznych napięć i rozpętanie spirali przemocy. Należy w tym scenariuszu spodziewać się szczególnie nasilonych działań dezinformacyjnych. Możliwe jest, że wykorzystywane środki techniczne będą ograniczone, z uwagi na konieczność zachowania pozorów działań osób lub grup niezwiązanych z aktorem państwowym i niewspieranych przez niego. Można wskazać trzy warianty tego scenariusza.

Scenariusz 3a. Zamach na osobę powszechnie znaną

Scenariusz zakłada przeprowadzenie prowokacji z wykorzystaniem zabójstwa, spowodowania uszczerbku na zdrowiu lub uprowadzenia osoby powszechnie znanej ze swojej działalności politycznej, społecznej lub

medialnej. Bardziej istotna jest w tym przypadku rozpoznawalność takiej osoby (w tym wywołana kontrowersyjnymi wypowiedziami) niż zajmowane przez nią aktualnie stanowisko. Może to być ktoś, kto nigdy nie zajmował stanowisk państwowych ani nie zasiadał w parlamencie. Atak na taką osobę byłby upozorowany na działanie osób z przeciwnego końca spektrum ideologicznego, a jego celem byłoby sprowokowanie osób identyfikujących się z wartościami i poglądami prezentowanymi przez ofiarę do nadmiernej reakcji emocjonalnej, podsycanej przez działania dezinformacyjne. Mogą one sugerować błędne działania organów państwowych prowadzących czynności dochodzeniowo-śledcze i operacyjno-rozpoznawcze bądź brak takich działań, a nawet wskazywać na udział w zamachu osób powiązanych ze służbami państwowymi.

Scenariusz 3b. Zamach w trakcie uroczystości, manifestacji lub innego wydarzenia o charakterze publicznym

Scenariusz zakłada, że celem zamachu jest uroczystość, manifestacja czy inne wydarzenie zorganizowane przez władze państwowe, samorządowe, organizację pozarządową lub wyznaniową. Celem ataku byłoby przede wszystkim wywołanie strachu, możliwe jest także spowodowanie ofiar w ludziach. Także w tym scenariuszu sprawcy będą dążyć do upozorowania ataku na czyn dokonany przez inną niż wspierana przez Rosję organizację (ruch) ekstremistyczną, pozostającą w opozycji do podmiotu organizującego dane wydarzenie.

Z uwagi na prawdopodobieństwo dużej liczby zabitych i rannych taki atak może prowadzić do silnej polaryzacji oraz skrajnych reakcji i być wykorzystany w końcowej fazie działań hybrydowych. Możliwe jest także dokonanie zamachu w sposób, który podważyłby wiarygodność organów państwowych. Należy się zatem spodziewać, że atak podczas uroczystości katolickich zostałby upozorowany na atak lewicowych ekstremistów, a zamach podczas lewicowej manifestacji – na atak organizacji skrajnie prawicowej.

Scenariusz 3c. Zamach na obiekt symboliczny

Scenariusz zakłada zamach wymierzony nie w osoby, lecz w mienie w postaci obiektów, takich jak pomniki, muzea, świątynie i inne obiekty mające znaczenie symboliczne dla społeczeństwa lub jego części. W tym przypadku atak miałby na celu jedynie wywołanie rozgłosu i zainteresowania mediów oraz opinii publicznej, stymulowanych działaniami dezinformacyjnymi.

Te czynniki sprawiają, że może to być atak, który okaże się wstępem do dalszych działań.

Scenariusz 4. Atak wykazujący nieefektywność działania służb

Ostatni spośród analizowanych scenariuszy jest szczególnym przypadkiem ataku. Jego celem nie byłoby bowiem zadanie strat, lecz przede wszystkim wykazanie nieefektywności polskich służb policyjnych i sił zbrojnych. W planie ataku zostałyby uwzględnione zidentyfikowane wcześniej deficyty systemu bezpieczeństwa państwa. Możliwe są dwa warianty. Zdarzenie stanowiłoby tak poważne wyzwanie, że reakcja na nie byłaby niemożliwa lub byłaby pośpieszna i prowizoryczna. Takim przypadkiem mogłaby być sytuacja zakładnicza o wysokim stopniu skomplikowania, np. na pokładzie jednostki pływającej (np. promu pasażerskiego) lub dużego budynku użyteczności publicznej. Sprawcy mogą deklarować wolę przedostania się wraz z zakładnikami do Rosji lub na Białoruś bądź też doprowadzić – co jest mniej prawdopodobne – do sytuacji, w której siłowa próba jej rozwiązania skutkowałaby dużą liczbą ofiar śmiertelnych. W każdym przypadku w gruncie rzeczy chodziłoby nie o osiągnięcie celu taktycznego, lecz o wykazanie nieefektywności polskich władz i służb, które nie zdołały rozwiązać sytuacji w sposób korzystny dla Polski. Stanowiłoby to podstawę do działań dezinformacyjnych i politycznych, a być może także militarnych. Takie ryzyko istnieje zwłaszcza na obszarach morskich, gdzie jest możliwe nawet doprowadzenie do zainscenizowanej operacji „odbicia" przez siły rosyjskie rzekomo uprowadzonej jednostki. Skuteczna operacja, zakończona ujęciem lub zabiciem bezpośrednich sprawców zdarzenia przez rosyjskie wojska specjalne lub jednostki kontrterrorystyczne FSB, zostałaby następnie wykorzystana propagandowo i politycznie jako „dowód" na niezdolność Polski do zapewnienia bezpieczeństwa na obszarach morskich oraz potwierdzenie skuteczności aparatu bezpieczeństwa Rosji.

Podsumowanie

Najważniejszym wnioskiem płynącym z przedstawionych scenariuszy jest konieczność stałego uwzględniania zagrożeń o charakterze terrorystycznym w działaniach na rzecz budowania odporności na zagrożenia hybrydowe. Kolejnym jest to, że zagrożenia terrorystyczne jako element wojny hybrydowej będą pochodną działań obcego państwa, co oznacza, że

preferencje w zakresie wyboru celów oraz metod dokonywania ataków byłyby odmienne niż w innych znanych nurtach terroryzmu. O ile w przypadku ataków sprawców należących do organizacji islamskich fundamentalistów lub wspierających je typowym wyborem były cele miękkie (kluby nocne, zakłady pracy, środki transportu pasażerskiego), o tyle przy zagrożeniach hybrydowych bardziej prawdopodobne są ataki na obiekty infrastruktury krytycznej czy obiekty wojskowe, a tylko jeden zestaw scenariuszy uwzględnia ataki na cele miękkie i tylko jeden z tego zestawu – ataki mogące skutkować dużą liczbą ofiar wśród osób cywilnych.

Zasadne jest więc uwzględnienie scenariuszy omówionych w artykule zarówno w planowaniu działań antyterrorystycznych, organizowaniu działań kontrterrorystycznych, jak i szerzej – w przygotowaniach do przeciwdziałania zagrożeniom hybrydowym. Należy przy tym pamiętać, że omawiane scenariusze wskazują na konieczność hybrydowej reakcji na tego rodzaju zagrożenia. Oprócz samych działań antyterrorystycznych i kontrterrorystycznych niezbędne będzie prowadzenie innych działań, w tym z zakresu przeciwdziałania dezinformacji i walki informacyjnej.

Bibliografia

Bolechów B., *Polityka antyterrorystyczna w świetle badań nad terroryzmem*, Wrocław 2012.

Galeotti M., *The Weaponisation of Everything: A Field Guide to the New Way of War*, New York–London 2022.

Makowski A., Kubiak K., *Terroryzm jako sposób prowadzenia wojny?*, „Raport – wojsko – technika – obronność" 1998, nr 4, 41–43.

Menkiszak M., *Strategiczna kontynuacja, taktyczna zmiana. Polityka bezpieczeństwa europejskiego Rosji*, Warszawa 2019.

Nadolski L.M., *Kampania zimowa w 2015 roku na Ukrainie*, Bydgoszcz 2017.

Piekarski M., *Bezpieczeństwo dostaw surowców energetycznych do Polski drogą morską*, „Wschodnioznawstwo" 2020, t. 14, s. 177–195.

Piekarski M., *Polish Armed Forces and hybrid war: current and required capabilities*, „The Copernicus Journal of Political Studies" 2019, nr 1, s. 43–64.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*, Toruń 2020.

Seely R., *Defining Contemporary Russian Warfare*, „The RUSI Journal" 2017, t. 162, nr 1, s. 50–59.

Skoneczny Ł., *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", wydanie specjalne: *Wojna hybrydowa*, s. 39–50.

The Military Balance 2021, The International Institute for Strategic Studies.

Źródła internetowe

Cullen P.J., Reichborn-Kjennerud E., *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*, The Multinational Capability Development Campaign, 2017 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf [dostęp: 20 V 2022].

Dyner A.M., *Kryzys graniczny jako przykład działań hybrydowych*, Polski Instytut Spraw Międzynarodowych, 2 II 2022 r., https://www.pism.pl/publikacje/kryzys-graniczny-jako-przyklad-dzialan-hybrydowych [dostęp: 22 VI 2022].

Gasztold A., Gasztold P., *The Polish Counterterrorism System and Hybrid Warfare Threats*, „Terrorism and Political Violence" 2020, https://www.tandfonline.com/doi/abs/10.1080/09546553.2020.1777110?journalCode=ftpv20 [dostęp: 28 V 2022].

Hoffman F., *Rise of the hybrid wars*, https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [dostęp: 29 IV 2022].

https://www.globalsecurity.org/wmd/ops/secmuniz.pdf [dostęp: 28 V 2022].

IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector, https://info.publicintelligence.net/DHS-ElectricGridAttacks.pdf [dostęp: 22 VI 2022].

Kosow H., Gaßner R., *Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria*, https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf [dostęp: 22 VI 2022].

Ogilvy J., *Scenario Planning and Strategic Forecasting*, Forbes, 8 I 2015 r., https://www.forbes.com/sites/stratfor/2015/01/08/scenario=-planning-and-strategic-forecasting/?sh-2de3fee5411a [dostęp: 18 V 2022].

Philips T., *The Dozier Kidnapping: Confronting the Red Brigades*, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/phillips.pdf [dostęp: 28 V 2022].

Sovolainen J. i in., *Hybrid CoE Working Paper 5 Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans*, https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf [dostęp: 29 IV 2022].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [dostęp: 22 VI 2022].

Akty prawne

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. DzU z 2021 r. poz. 2234, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. DzU z 2022 r. poz. 261, ze zm.).