mgr Natalia Domasiak
Akademia Sztuki Wojennej w Warszawie
ORCID: 0009-0001-5162-6498

https://doi.org/10.29316/9788368103205_9

ROLA SŁUŻB SPECJALNYCH W ZAPEWNIANIU BEZPIECZEŃSTWA POLSKI W DOBIE ZAGROŻEŃ HYBRYDOWYCH

THE ROLE OF SPECIAL SERVICES IN ENSURING POLISH SECURITY IN THE ERA OF HYBRID THREATS

Streszczenie

Autorka analizuje istotę i charakter zagrożeń hybrydowych, podkreślając ich wielowymiarowość oraz trudność w wykryciu i przypisaniu odpowiedzialności za ich realizację. Przedstawiono definicje zagrożeń hybrydowych według NATO, Unii Europejskiej oraz polskich instytucji, wskazując na ich wspólne cechy: skoordynowanie działań państwowych i niepaństwowych, wykorzystanie zarówno środków militarnych, jak i niemilitarnych oraz prowadzenie operacji poniżej progu otwartej wojny. Autorka omawia również rolę polskich służb specjalnych – zarówno cywilnych (ABW, AW), jak i wojskowych (SKW, SWW) – w systemie bezpieczeństwa państwa. Służby te realizują zadania z zakresu rozpoznawania, zapobiegania

Summary

The author conducts an analysis of the essence and nature of hybrid threats, emphasising their multidimensionality and the complexity of detecting and attributing responsibility for their implementation. Definitions of hybrid threats are presented, drawn from the perspectives of NATO, the European Union, and Polish institutions. These definitions highlight common features, including coordination of actions between states and non-state actors, the utilisation of both military and non-military means, and the execution of operations that fall below the threshold of open warfare. The author also discusses the role of Polish special services – both civilian (ABW, AW) and military (SKW, SWW) – in the state security system. The aforementioned

i zwalczania zagrożeń hybrydowych, takich jak cyberataki, dezinformacja, sabotaż czy operacje wywiadowcze. Wskazano także na konkretne przykłady działań hybrydowych wymierzonych przeciwko Polsce, w tym kryzys migracyjny na granicy polsko-białoruskiej oraz operacje dywersyjne i propagandowe inspirowane przez rosyjskie służby specjalne. Podkreślono, że skuteczna ochrona przed zagrożeniami hybrydowymi wymaga ścisłej współpracy służb specjalnych, nowoczesnych technologii oraz ciągłego doskonalenia metod rozpoznania i przeciwdziałania tego typu zagrożeniom

Słowa kluczowe: służby specjalne, zagrożenia hybrydowe, bezpieczeństwo państwa

services are responsible for the identification, prevention and combating of hybrid threats, including, but not limited to, cyber-attacks, disinformation, sabotage, and intelligence operations. It was further noted that there were specific instances of hybrid actions against Poland, including the migration crisis on the Polish-Belarusian border and diversionary and propaganda operations inspired by Russian special services. It was emphasised that effective protection against hybrid threats requires close cooperation between special services, modern technologies, and continuous improvement in methods of identifying and countering such threats.

Keywords: special services, hybrid threats, state securit

Wstęp

Współczesne środowisko bezpieczeństwa charakteryzuje się rosnącą złożonością i nieprzewidywalnością zagrożeń. Jednym z kluczowych wyzwań XXI wieku są zagrożenia hybrydowe, które wymykają się tradycyjnym klasyfikacjom konfliktów. Termin „zagrożenia hybrydowe" obejmuje szerokie spektrum działań prowadzonych poniżej progu otwartej wojny, łączących elementy konwencjonalne i niekonwencjonalne, militarne i niemilitarne, realizowanych przez aktorów państwowych i niepaństwowych w sposób skoordynowany i zsynchronizowany, a ich celem jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. W obliczu tych wyzwań kluczową rolę odgrywają służby specjalne, które odpowiadają za identyfikację, analizę i przeciwdziałanie zagrożeniom hybrydowym, chroniąc bezpieczeństwo państwa zarówno w wymiarze wewnętrznym, jak i zewnętrznym. Do zadań służb należy zapewnienie odporności na nowe, nieliniowe formy agresji, które coraz częściej stają się narzędziem walki we współczesnym świecie.

Zagrożenia hybrydowe – istota i charakter

Współczesne środowisko bezpieczeństwa państwowego charakteryzuje się rosnącą złożonością i nieprzewidywalnością zagrożeń. Jednym z najbardziej dynamicznie rozwijających się wyzwań są zagrożenia hybrydowe, które wymykają się tradycyjnym klasyfikacjom konfliktów i działań zbrojnych. Termin ten odnosi się do szerokiego spektrum działań prowadzonych poniżej progu otwartej wojny, łączących metody konwencjonalne i niekonwencjonalne, militarne i niemilitarne, realizowanych przez aktorów państwowych i niepaństwowych w sposób skoordynowany i zsynchronizowany. Celem tych działań jest nie tylko zadanie bezpośrednich szkód, ale przede wszystkim destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach.

Według NATO są to działania militarne i niemilitarne oraz jawne i niejawne środki, obejmujące dezinformację, ataki cybernetyczne, presję ekonomiczną, użycie nieregularnych grup zbrojnych i wojsk regularnych. Mają na celu rozmywanie granicy między wojną i pokojem oraz dezorientowanie społeczeństw[1].

Z kolei Unia Europejska definiuje zagrożenia hybrydowe jako połączenie działań konwencjonalnych i niekonwencjonalnych (militarnych i niemilitarnych), stosowanych w skoordynowany sposób przez aktorów państwowych i niepaństwowych, ukierunkowanych na osiągnięcie celów politycznych”[2].

Słownik terminów z zakresu bezpieczeństwa definiuje zagrożenia hybrydowe jako „zagrożenia generowane przez działania hybrydowe – godzące w interesy podmiotu bezpieczeństwa”[3]. Przez działania hybrydowe rozumiane są „działania mające na celu osiągnięcie zamierzeń politycznych i strategicznych z możliwością utrzymywania dotychczasowych stosunków gospodarczych i/lub dyplomatycznych, prowadzone przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, łączące różne środki wywierania nacisku oraz uzależniania od potencjalnego agresora”[4].

---

1 *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm, [dostęp: 23.04.2025].

2 *A Europe that Protects: Countering Hybrid Threats*, https://www.eeas.europa.eu/node/46393_en, [dostęp: 16.04.2025].

3 J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020 r., s. 276.

4 Ibidem, s. 53.

Rządowe Centrum Bezpieczeństwa wskazuje, że „działania hybrydowe to działania zmierzające do osiągnięcia celów politycznych i strategicznych agresora. Prowadzone są w sposób wielowymiarowy, skryty, utrudniający identyfikację przeciwnika i przypisanie odpowiedzialności za nie sprawcy. Działania te prowadzone są przez podmioty państwowe i/lub niepaństwowe w sposób zaplanowany i skoordynowany, często rozłożone w dłuższym czasie oraz łączą różne środki wywierania nacisku i uzależniania od potencjalnego agresora. Mogą być prowadzone przy użyciu środków politycznych, ekonomicznych, prawnych, militarnych i społecznych, w tym z wykorzystaniem różnego rodzaju kanałów komunikacji społecznej. Mogą również być prowadzone pośrednio, z wykorzystaniem lokalnych podmiotów, organizacji i osób prywatnych, co utrudnia wykrycie i przeciwdziałanie im”[5]. Przykładami działań hybrydowych są „operacje informacyjne, psychologiczne, działania o charakterze terrorystycznym, kryminalnym, działania mające na celu zakłócenie funkcjonowania sieci i systemów informatycznych, systemu energetycznego, systemu dostarczania paliw, systemów funkcjonowania i usług telekomunikacyjnych, systemu gazowego, zdarzeń związanych ze skażeniem chemicznym na lądzie, w wodzie i powietrzu, skażeniem promieniotwórczym, zakłócenia porządku publicznego, dezinformacji. Trudność w wykryciu i zdefiniowaniu, czy dane zdarzenie wystąpiło w obszarze działań hybrydowych, spowodowana jest często charakterem tych działań, tzn. działania hybrydowe mają zwykle charakter „pełzający”. Sprzyja to trudności w ich początkowym rozpoznaniu i zdefiniowaniu. Działania te poddają się ocenie w perspektywie dłuższego przedziału czasowego”[6].

Strategia Bezpieczeństwa Narodowego z 2020 r. wskazuje, że działania o charakterze hybrydowym będą pozostawać istotnym środkiem polityki, służącym zarówno podmiotom państwowym, jak i pozapaństwowym do osiągania ich celów. Działania te, możliwe, że zostaną przeniesione do przestrzeni kosmicznej[7].

Rosyjska koncepcja prowadzenia działań hybrydowych „polega na używaniu całego spektrum instrumentów politycznych, ekonomicznych i społecznych w celu m.in. manipulowania poglądami ludności w państwach

[5] Krajowy Plan Zarządzania Kryzysowego, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego, [dostęp: 15.04.2025].

[6] Ibidem.

[7] Strategia Bezpieczeństwa Narodowego z 2020 roku, s. 7.

uznawanych za wrogie. Do najważniejszych obszarów rosyjskiej aktywności należą wojna informacyjna, cyberataki oraz instrumentalizacja migracji”[8].

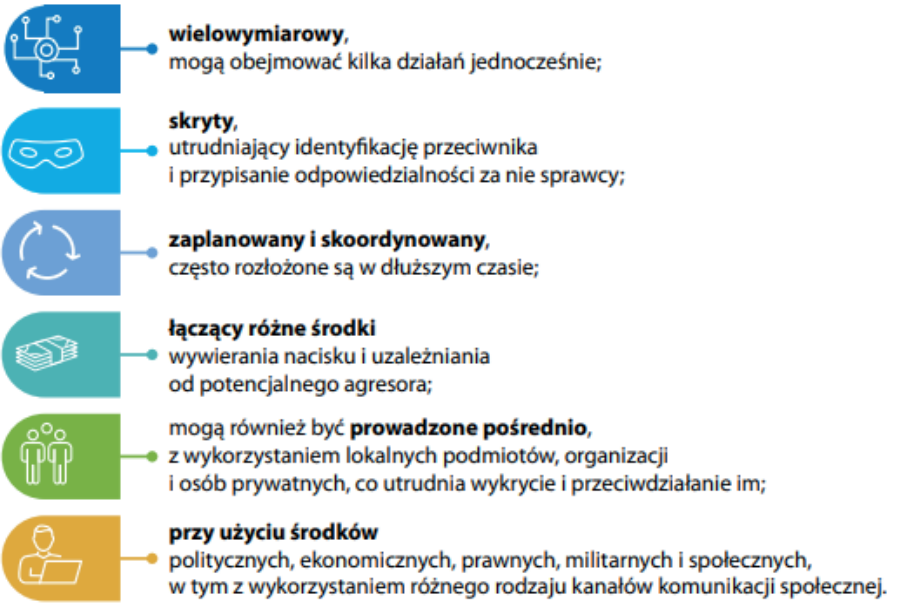
Termin zagrożenie hybrydowe odnosi się do działań podejmowanych przez podmioty państwowe lub niepaństwowe, których celem jest osłabienie lub zaszkodzenie celowi poprzez łączenie jawnych i tajnych środków militarnych i niemilitarnych[9]. Są one zaprojektowane tak, aby były trudne do wykrycia lub identyfikacji. Zagrożenia te są ukierunkowane na krytyczne słabe punkty i mają na celu wprowadzenie zamieszania, aby utrudnić szybkie i skuteczne podejmowanie decyzji. Zagrożenia hybrydowe mogą obejmować cyberataki na krytyczne systemy informatyczne, zakłócenia w świadczeniu kluczowych usług, takich jak dostawy energii czy usługi finansowe, podważanie zaufania publicznego do instytucji rządowych czy pogłębianie podziałów społecznych. Jako przykład zagrożeń hybrydowych możemy uznać operacje kinetyczne np. wykorzystanie nieoznakowanych żołnierzy do opanowania jakiegoś terytorium, cyberataki na infrastrukturę krytyczną, sabotaż, jak i niekinetyczne tj. dezinformacja, propaganda, presja ekonomiczna, operacje informacyjne, protesty itp.

Najwyższa Izba Kontroli do kontroli nt. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi przyjęła, że „działania hybrydowe (w czasie pokoju) to konwergencja różnych typów działań poniżej progu wojny, zagrażających lub mogących zagrażać bezpieczeństwu państwa i jego obywateli, prowadzonych z wykorzystaniem narzędzi klasycznych (np. dezinformacja), jak również nowoczesnych (np. cyberataki), mających na celu wywoływanie i podtrzymywanie sytuacji kryzysowych bez użycia regularnych środków militarnych. Spektrum środków wykorzystywanych w działaniach hybrydowych jest praktycznie nieograniczone i można zaliczyć do nich m.in. przestrzeń polityczną, dyplomatyczną, dezinformacyjno-propagandową, gospodarczą, kulturalną, terrorystyczną oraz humanitarną. Zagrożenia hybrydowe są różnorodne i ciągle się zmieniają, wykorzystując synergię tworzoną przez wiele podmiotów i działań. Działania hybrydowe mogą prowadzić zarówno agenci służb specjalnych obcego państwa i osoby z nimi współpracujące, jak również na przykład (świadomie bądź nie) organizacje,

[8] A. M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE, Działania hybrydowe Rosji przeciw państwom NATO i UE*, https://pism.pl/publikacje/dzialania-hybrydowe--rosji-przeciw-panstwom-nato-i-ue, [dostęp: 15.04.2025].

[9] *Hybrid threats*, https://www.hybridcoe.fi/hybrid-threats/, [dostęp: 15.04.2025].

stowarzyszenia, instytucje, partie polityczne, firmy, korporacje i celebryci/osoby ogólnie znane. Należy przy tym podkreślić, że trudność w wykryciu i zdefiniowaniu, czy dane zdarzenie wystąpiło w obszarze działań hybrydowych, spowodowana jest często charakterem tych działań, tzn. działania hybrydowe mają zwykle charakter „pełzający”[10]. Poniżej na rysunku przedstawiono sposoby prowadzenia działań hybrydowych.



Rysunek 1. Sposoby prowadzenia działań hybrydowych

Źródło: wyniki kontroli NIK. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi. KPB.430.002.2023 Nr ewid. 16/2023/P/22/029/KPB.

Wojna hybrydowa, prowadzona poniżej progu działań zbrojnych lub bez bezpośredniej, jawnej agresji, przynosi liczne korzyści. Jest ona znacznie łatwiejsza, tańsza i mniej ryzykowna niż operacje kinetyczne. Taka forma walki wpisuje się również w starożytną filozofię wojny, według której najwyższą sztuką jest pokonanie przeciwnika bez konieczności walki – jak sugerował Sun Zi, jeden z największych strategów wojskowych. Drugą charakterystyczną cechą wojny hybrydowej jest jej niejednoznaczność i trudność w przypisaniu

[10] Wyniki kontroli NIK. Przygotowanie państwa na zagrożenia związane z działaniami hybrydowymi. KPB.430.002.2023 Nr ewid. 16/2023/P/22/029/KPB.

odpowiedzialności, czyli tzw. atrybucji. Ataki hybrydowe zwykle cechuje wysoki poziom niejasności. Ta niepewność jest celowo kreowana i pogłębiania przez podmioty prowadzące takie działania, aby utrudnić wykrycie ataku i ustalenie jego sprawcy. Wykorzystując progi wykrywalności i poziomy atrybucji, agresorzy hybrydowi skutecznie utrudniają państwu obronę i opracowanie odpowiednich strategii[11].

Służby specjalne w systemie bezpieczeństwa państwa

W dobie tak specyficznych i unikalnych zagrożeń hybrydowych zapewnianie szeroko pojętego bezpieczeństwa jest naczelnym zadaniem polityki państwa, a także konstytucyjnym zadaniem jego organów. Funkcjonowanie państwa oparte na systemie bezpieczeństwa narodowego jest nierozerwalnie związane z działalnością służb specjalnych. Są to instytucje, które poprzez działalność operacyjno-rozpoznawczą (głównie o charakterze niejawnym) pozyskują i chronią kluczowe dla bezpieczeństwa państwa informacje. Ich cechą charakterystyczną jest tajność działania, a fundamentalnym zadaniem służb specjalnych ochrona bezpieczeństwa zewnętrznego i wewnętrznego wraz z ochroną jego porządku konstytucyjnego.

Rozważając problematykę służb specjalnych w systemie bezpieczeństwa państwa warto odpowiedzieć na pytanie: czym są służby specjalne? Sławomir Zalewski definiuje je jako „zorganizowane zazwyczaj przez państwo struktury, ukierunkowane na niejawne pozyskiwanie informacji, istotnych z punktu widzenia bezpieczeństwa organizatora tej działalności (państwa) bądź przeciwdziałania ich zdobywaniu przez podobne struktury, identyfikowane jako obce”[12]. Jednocześnie wskazuje, że pojęcie nie jest jednoznaczne, mimo że tym mianem powszechnie określany jest wywiad i kontrwywiad. W polskim systemie prawnym nie występuje definicja służb specjalnych, która wskazywałaby na charakter ich działalności. A zatem Zalewski wskazuje, że termin – służby specjalne – nie odnosi się do wszystkich służb prowadzących niejawną działalność, polegającą na podejmowaniu na podstawie przepisów

[11] A. Bilal, *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie” jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html, [dostęp: 15.04.2025].

[12] S. Zalewski, *Służby specjalne w państwie demokratycznym*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 13.

prawa działań operacyjno-rozpoznawczych, a tylko do tych, które „tradycyjnie" wykonują zadania wywiadowcze i kontrwywiadowcze"[13]. Bogusław Pacek z kolei wskazuje, że wszystkie instytucje państwowe, które prowadzą działania operacyjno-rozpoznawcze o niejawnym charakterze to służby specjalne[14]. *Słownik terminów z zakresu bezpieczeństwa* wskazuje, że służby specjalne to „instytucje pozyskujące i chroniące informacje kluczowe dla bezpieczeństwa państwa poprzez działalność operacyjno-rozpoznawczą, głównie o charakterze niejawnym". Przeważnie są to służby wywiadowcze i kontrwywiadowcze[15]. Na tej podstawie przyjmuje się, że w Polsce instytucje zajmujące się wywiadem i kontrwywiadem noszą miano służb specjalnych. Przyjmuje się także, że służby wywiadowcze koncentrują się na zdobywaniu i opracowywaniu informacji ważnych dla bezpieczeństwa państwa[16], a kontrwywiadowcze na udaremnianiu wysiłków obcych wywiadów w penetrowaniu lub dekonspirowaniu własnych służb wywiadowczych i ich operacji[17].

W polskim systemie bezpieczeństwa państwa funkcjonują cztery służby specjalne zajmujące się wywiadem i kontrwywiadem – dwie cywilne i dwie wojskowe. Do cywilnych służb specjalnych zalicza się Agencję Bezpieczeństwa Wewnętrznego odpowiedzialną za ochronę bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego oraz Agencję Wywiadu odpowiedzialną za ochronę bezpieczeństwa zewnętrznego państwa. Do wojskowych służb specjalnych należy Służba Kontrwywiadu Wojskowego właściwa w sprawach z zakresu ochrony przed zagrożeniami wewnętrznymi dla obronności kraju, zdolności bojowej i bezpieczeństwa Sił Zbrojnych RP oraz Służba Wywiadu Wojskowego odpowiedzialna za ochronę przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej SZ RP.

Z uwagi na szeroki zakres zadań, wiodącą rolę w systemie bezpieczeństwa państwa odgrywa w Polsce ABW. Głównym zadaniem ABW jest ochrona bezpieczeństwa wewnętrznego państwa oraz porządku konstytucyjnego. ABW

---

[13] D. Laskowski, *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, Obronność. Zeszyty Naukowe, 2(10), 2014. s. 60-61.

[14] B. Pacek, *Osobowościowe uwarunkowania efektywności oficerów kontrwywiadu*, wyd. Akademia Obrony Narodowej Warszawa 2013, s. 10.

[15] J. Pawłowski, B. Zdrodowski, M. Kuliczkowski, *Słownik terminów z zakresu bezpieczeństwa*, Wydawnictwo Adam Marszałek, Toruń 2020 r., s. 206-207.

[16] S. Hoc, *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Akademia Spraw Wewnętrznych, Warszawa 1985, s. 36.

[17] R. Kessler, *CIA od środka*, Wydawnictwo Ryton, Warszawa 1994, s. 295

zajmuje się rozpoznawaniem, zapobieganiem i zwalczaniem zagrożeń, takich jak terroryzm, szpiegostwo, naruszenia informacji niejawnych, przestępstwa godzące w podstawy ekonomiczne państwa czy korupcja na najwyższych szczeblach władzy. Do jej obowiązków należy również ochrona systemów teleinformatycznych i infrastruktury krytycznej państwa. Obszary w jakich ABW działa to: informacyjny, ścigania karnego oraz profilaktyczno-kontrolny. Zadania z zakresu zwalczania szpiegostwa, terroryzmu, ujawnienia bądź wykorzystania informacji niejawnych obejmują m.in. „monitorowanie instytucjonalnej i cudzoziemskiej aktywności na terenie Rzeczpospolitej Polskiej pod kątem realizacji zadań na rzecz obcych służb specjalnych, ofensywne rozpracowanie obcych służb specjalnych, rozpoznanie osób oraz innych podmiotów współpracujących z obcymi służbami specjalnymi”[18]. Z punktu widzenia zagrożeń hybrydowych istotnym zadaniem wykonywanym przez ABW jest prowadzenie szkoleń prewencyjnych dla urzędników państwowych na temat niebezpieczeństw z jakimi mogą się zetknąć w trakcie wykonywanych obowiązków.

Natomiast Służba Kontrwywiadu Wojskowego (SKW) ma za zadanie ochronę przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej. Do podstawowych zadań SKW należy zwalczanie przestępstw tj. szpiegostwa przeciwko RP, zamachu lub sabotażu wobec SZ RP, nielegalnego obrotu z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa czy terroryzmu, ochrona informacji niejawnych, ochrona (kontrwywiadowcza) wojska poza granicami kraju, kontrwywiad radioelektroniczny oraz kryptografia i kryptoanaliza, kontrola umów międzynarodowych dotyczących rozbrojenia i ochrona badań naukowych. SKW zajmuje się również działaniami z zakresu cyberbezpieczeństwa np. dostarcza informacji o zagrożeniach związanych z wyborem oraz korzystaniem z technologii sprzętowych, informatycznych i szuka odpowiednich środków zaradczych”[19]. Jednocześnie prowadzi działania z zakresu „cyberkontrwywiadu w kontekście systemów teleinformatycznych i neutralizowania zagrożeń wewnętrznych o charakterze szpiegostwa, działania mające

[18] B. Opaliński, M. Rogalski, P. Szustakiewicz, Usta*wa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Wydawnictwo C.H. Beck, Warszawa 2017, s 21-22.

[19] *Służba Kontrwywiadu Wojskowego*, https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m--suzbakontrwywiadu-wojskowego/, [dostęp: 17.04.2025].

na celu wykrywanie przestępstw w kontekście systemów teleinformatycznych określonych w Rozdziale XXXIII Kodeksu karnego (przestępstwa przeciwko ochronie informacji)"[20]. Istotnym zadaniem jest także prowadzenie działań operacyjno-rozpoznawczych w cyberprzestrzeni, których celem jest badanie i neutralizowanie zagrożeń. W wyniku prowadzonych badań SKW gromadzi informacje nt. modus operandi oraz technik, taktyk i procedur grup hakerskich lub adwersarzy w cyberprzestrzeni celem umożliwienia realizacji działań wyprzedzających potencjalny atak cybernetyczny na systemy teleinformatyczne resortu.

Z kolei Agencja Wywiadu odpowiada za „uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego". Do jej zadań należy „rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej". W kontekście zagrożeń hybrydowych AW chroni zagraniczne przedstawicielstwa Polski oraz ich pracowników przed działaniami obcych służb specjalnych, a także zapewnia ochronę kryptograficzną łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej. Do zakresu zainteresowań AW należą także rejony napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo Polski. W tym zakresie funkcjonariusze AW rozpoznają i analizują zagrożenia tam występujące celem podjęcia działań mających je wyeliminować. Współczesne zagrożenia hybrydowe obejmują szerokie spektrum działań, takich jak operacje w cyberprzestrzeni, dezinformacja, ataki na infrastrukturę krytyczną, działania wywiadowcze, a także terroryzm i przestępczość zorganizowaną. W tym kontekście szczególnego znaczenia nabiera realizowany przez Agencję wywiad elektroniczny.

Służba Wywiadu Wojskowego otrzymała natomiast zadania z zakresu uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa potencjału obronnego Rzeczypospolitej Polskiej, bezpieczeństwa i zdolności bojowej SZ RP oraz warunków realizacji, przez SZ RP, zadań poza granicami państwa. Służba zajmuje się rozpoznawaniem i przeciwdziałaniem

[20] Ibidem.

militarnym zagrożeniom zewnętrznym godzącym w obronność Rzeczypospolitej Polskiej oraz zagrożeniom międzynarodowym terroryzmem. Analogicznie do AW funkcjonariusze SWW prowadzą rozpoznanie i analizę zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na obronność państwa oraz zdolność bojową SZ RP. SWW zostało również zobowiązane do eliminacji tych zagrożeń. SWW wykorzystuje zaawansowane technologie do zabezpieczania działań SZ RP (kryptografia) oraz łamania szyfrów stosowanych przez przeciwnika (kryptoanaliza), co ma szczególne znaczenie w walce z zagrożeniami hybrydowymi, gdzie granica między działaniami militarnymi, cybernetycznymi i informacyjnymi jest coraz bardziej płynna.

Służby specjalne wobec wybranych zagrożeń hybrydowych

Współczesny świat staje w obliczu coraz bardziej złożonych i różnorodnych zagrożeń, szczególnie tych o charakterze hybrydowym, które, choć znane od wieków, dopiero od lat 90. XX wieku są systematycznie badane i analizowane przez środowiska naukowe i wojskowe. Ich rosnące znaczenie wynika między innymi z działań Rosji wobec Ukrainy, które nasiliły się po Arabskiej Wiośnie, aneksji Krymu w 2014 r. i eskalacji konfliktu w 2022 r. W takich warunkach skuteczne zapewnienie bezpieczeństwa państwa wymaga sprawnie działających służb specjalnych, które odgrywają kluczową rolę w identyfikacji, analizie i przeciwdziałaniu współczesnym zagrożeniom hybrydowym.

Analizując rolę służb specjalnych w warunkach wojny hybrydowej, należy precyzyjnie powiązać ich działania z kluczowymi komponentami tego typu konfliktu. Wojna hybrydowa obejmuje bowiem równoległe operacje w przestrzeni dyplomatycznej, politycznej, ekonomicznej, informacyjnej oraz – choć w ograniczonym zakresie – militarnej. Celem tych działań jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. „Profesor Khalid Mohamed Alqahtani, w publikacji „Modern Counter-IntelligenceSocial", podkreśla kluczowe znaczenie kontrwywiadu dla zapewnienia bezpieczeństwa, stabilności psychicznej społeczeństwa oraz wczesnego wykrywania wrogich zamiarów, zanim zostaną one zrealizowane"[21].

[21] A. Jawor, *Zadania kontrwywiadu w dobie współczesnych zagrożeń*, https://infosecurity24.pl/za-granica/zadania-kontrwywiadu-w-dobie-wspolczesnych-zagrozen, [dostęp: 18.04.2025].

Kontrwywiad tradycyjnie koncentrował się na zwalczaniu szpiegostwa, sabotażu i dywersji prowadzonej przez inne państwa. Po zakończeniu zimnej wojny i atakach z 11 września 2001 r., służby kontrwywiadowcze państw zachodnich ukierunkowały swoje zadania na walkę z terroryzmem i ekstremizmem oraz aktorami niepaństwowymi. Operacje antyterrorystyczne i antyrebelianckie sprawiły, że „kontrwywiad zaczął pełnić funkcję służebną wobec strategii ukierunkowanych na zwalczanie zagrożeń asymetrycznych". Wraz ze wzrostem znaczenia nowych technologii, aneksją Krymu w 2014 r., eskalacją konfliktu w Ukrainie i wojną informacyjną Rosji wobec Zachodu, zagrożenia hybrydowe przybierają na sile. W związku z tym, jak twierdzi Philip H. J. Davies, współczesny kontrwywiad skupia się nie tylko na przeciwdziałaniu infiltracji struktur państwowych poprzez wykrywanie obcych agentów, ale również na neutralizowaniu kanałów przenikania wpływów i aktywności informacyjno-psychologicznej, a także na przeciwdziałaniu zaawansowanym technikom rozpoznania przeciwnika[22]. W dobie cyberataków i dezinformacji kontrwywiad odpowiada za ochronę systemu politycznego, militarnego i gospodarczego państwa.

Z kolei wywiad w działaniach hybrydowych staje się niezbędny w realizacji złożonych operacji informacyjnych, przygotowaniu społeczeństw wg wcześniej opracowanych schematów oraz w prowadzeniu defensywnych i ofensywnych operacji. Służby wywiadowcze prowadzą działania w sferze politycznej, ekonomicznej, informacyjnej, dyplomatycznej i militarnej (w ograniczonym zakresie). W sferze politycznej wywiad monitoruje działania i zamiary zarówno państw, jak i aktorów niepaństwowych, analizując procesy decyzyjne, nastroje społeczne oraz potencjalne punkty zapalne. Pozwala to na wczesne wykrywanie prób destabilizacji, ingerencji w procesy wyborcze czy inspirowania protestów społecznych. Działania te są szczególnie istotne w kontekście zagrożeń hybrydowych, gdzie granica między polityką wewnętrzną a zewnętrzną często się zaciera, a operacje wpływu mogą być prowadzone zdalnie, przy użyciu nowoczesnych technologii komunikacyjnych. W wymiarze ekonomicznym wywiad skupia się na identyfikacji zagrożeń dla gospodarki państwa, takich jak próby przejęcia strategicznych przedsiębiorstw przez podmioty powiązane z obcymi wywiadami, manipulacje rynkami finansowymi, czy działania mające na celu wywołanie kryzysów energetycznych.

[22] Ibidem.

Służby wywiadowcze analizują również przepływy kapitału, inwestycje zagraniczne oraz transakcje handlowe, które mogą stanowić narzędzie wywierania nacisku lub infiltracji gospodarczej. W obszarze informacyjnym wywiad odgrywa kluczową rolę w rozpoznawaniu i przeciwdziałaniu kampaniom dezinformacyjnym, które mają na celu wprowadzenie chaosu, podważenie zaufania do instytucji państwowych, czy polaryzację społeczeństwa. Służby te monitorują media tradycyjne i społecznościowe, identyfikując źródła i kanały rozpowszechniania fałszywych informacji, a także analizują ich wpływ na opinię publiczną.

W razie potrzeby prowadzą działania kontrpropagandowe, mające na celu neutralizację szkodliwych narracji. Na płaszczyźnie dyplomatycznej wywiad wspiera działania rządu poprzez dostarczanie informacji o zamierzeniach i strategiach innych państw, przewidywanie reakcji na inicjatywy polityczne oraz identyfikowanie potencjalnych sojuszników i przeciwników na arenie międzynarodowej. Pozwala to na podejmowanie bardziej świadomych i skutecznych decyzji w zakresie polityki zagranicznej oraz budowanie koalicji przeciwdziałających zagrożeniom hybrydowym. W ograniczonym zakresie, wywiad angażuje się również w działania militarne, wspierając planowanie i realizację operacji wojskowych poprzez dostarczanie informacji o rozmieszczeniu sił przeciwnika, jego zdolnościach bojowych czy planowanych ruchach. Współczesne konflikty hybrydowe często wymagają ścisłej współpracy wywiadu z siłami zbrojnymi, zwłaszcza w zakresie rozpoznania elektronicznego, cyberoperacji oraz działań specjalnych[23].

Przykładem działań hybrydowych skierowanych przeciwko Polsce jest kryzys migracyjny na granicy polsko-białoruskiej toczący się od 2022 r. Operacja prowadzona przez Rosję i Białoruś z wykorzystaniem szlaku nielegalnej migracji ma na celu destabilizację krajów wschodniej flanki NATO. Przebieg operacji obejmuje zarówno działania fizyczne na granicy – forsowanie ogrodzeń, niszczenie zapór, prowokacje wobec polskich służb – jak i szeroko zakrojoną kampanię dezinformacyjną, mającą na celu oczernianie

[23] K. Surdyk, *Rola służb wywiadowczych w wojnie hybrydowej*, Ante Portas – Studia nad Bezpieczeństwem, Nr 2(11), 2018, s. 70-71.

Polski, polaryzację społeczeństw państw Zachodu i osłabianie ich solidarności, a także testowanie zdolności reagowania kryzysowego[24, 25].

Polskie służby specjalne w 2024 r. odnotowały intensyfikację działań o charakterze dywersyjnym wymierzonych przeciwko Rzeczypospolitej Polskiej oraz państwom członkowskim Unii Europejskiej i NATO. Są one inicjowane i koordynowane przez rosyjskie służby specjalne. Celem stały się przede wszystkim obiekty cywilne, w tym magazyny i sklepy wielkopowierzchniowe, a metodą – podpalenia. Działania te przybierają coraz częściej formę działań terrorystycznych. Charakter tych operacji wskazuje, że celem Rosji jest przede wszystkim zastraszenie obywateli Polski i państw Zachodu oraz zniechęcenie ich do udzielania dalszego wsparcia Ukrainie. Jednocześnie stanowią one narzędzie służące Moskwie do testowania odporności RP i naszych sojuszników na zagrożenia hybrydowe[26].

Działania hybrydowe obejmują szeroki wachlarz środków, w tym propagandę, dezinformację, operacje psychologiczne oraz próby rekrutacji do formacji zbrojnych, które służą destabilizacji państwa i społeczeństwa. Przykładem takiej aktywności była operacja zatrzymania przez Agencję Bezpieczeństwa Wewnętrznego w sierpniu 2023 r. dwóch obywateli Rosji, którzy rozklejali w Krakowie i Warszawie materiały propagandowe zachęcające do zaciągu do Grupy Wagnera – nielegalnej formacji najemniczej powiązanej z rosyjskimi służbami specjalnymi. Jak ustaliły polskie organy ścigania, zatrzymani prowadzili działania na rzecz rosyjskiego wywiadu, realizując elementy wojny hybrydowej, w tym operacje propagandowe i rekrutacyjne, mające na celu destabilizację sytuacji politycznej w Polsce i Europie oraz budowanie zaplecza do dalszych działań wywiadowczych i terrorystycznych[27].

---

[24] R. Gönczi, *Dezinformacja jako oręż wojny hybrydowej na granicy z Białorusią*, https://warsawinstitute.org/pl/dezionformacja-jako-orez-wojny-hybrydowej-na-granicy-z-bialorusia/, [dostęp: 15.04.2025].

[25] F. Bryjka, A. Legucka, *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, https://pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego, [dostęp: 15.04.2025].

[26] *Komunikat dotyczący działalności dywersyjnej FR*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html, [dostęp: 15.04.2025].

[27] *ABW zatrzymała 2 obywateli Rosji*, https://www.abw.gov.pl/pl/informacje/2368,ABW-zatrzymala-2-obywateli-Rosji.html, [dostęp: 15.04.2025].

Podsumowanie

Zagrożenia hybrydowe, będące jednym z najpoważniejszych wyzwań dla współczesnych państw, charakteryzują się wielowymiarowością, tajnością oraz trudnością w jednoznacznym przypisaniu odpowiedzialności za ich realizację. Działania te łączą metody militarne i niemilitarne, konwencjonalne i niekonwencjonalne, a ich celem jest destabilizacja struktur państwowych, erozja zaufania społecznego oraz osłabienie przeciwnika na wielu płaszczyznach. Przykłady takich działań obejmują cyberataki na infrastrukturę krytyczną, kampanie dezinformacyjne, presję ekonomiczną, sabotaż, działania terrorystyczne oraz instrumentalizację migracji – jak miało to miejsce na granicy polsko-białoruskiej w ostatnich latach.

Kluczową rolę w przeciwdziałaniu zagrożeniom hybrydowym odgrywają służby specjalne, zarówno cywilne, jak i wojskowe. W polskim systemie bezpieczeństwa są to m.in. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego oraz Służba Wywiadu Wojskowego. Instytucje te realizują zadania z zakresu rozpoznawania, zapobiegania i neutralizowania zagrożeń hybrydowych, prowadząc działania operacyjno-rozpoznawcze, monitorując aktywność obcych służb specjalnych, chroniąc infrastrukturę krytyczną oraz przeciwdziałając szpiegostwu, sabotażowi i dezinformacji. Szczególne znaczenie mają działania w cyberprzestrzeni, gdzie ataki na systemy informatyczne i telekomunikacyjne stanowią coraz większe zagrożenie dla funkcjonowania państwa.

Do współczesnych zagrożeń hybrydowych zalicza się działania Rosji wobec Ukrainy, operacje dywersyjne wymierzone w Polskę i jej sojuszników. Działania te pokazują, że zagrożenia są realne i dynamicznie się rozwijają. Rosyjskie służby specjalne prowadzą szeroko zakrojone operacje informacyjne, cybernetyczne i propagandowe, mające na celu destabilizację państw Zachodu, testowanie ich odporności oraz zniechęcanie do wspierania Ukrainy. Przykładem takich działań są podpalenia obiektów cywilnych, kampanie dezinformacyjne oraz próby rekrutacji do formacji zbrojnych, jak Grupa Wagnera.

Literatura

1. Hoc S., *Zagadnienia odpowiedzialności karnej za szpiegostwo*, Warszawa 1985.
2. Kessler R., *CIA od środka*, Warszawa 1994.

3. Laskowski D., *Prawne podstawy funkcjonowania służb specjalnych z perspektywy potrzeb obronnych państwa*, Obronność. Zeszyty Naukowe 2(10), 2014.
4. Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017.
5. Pacek B., *Osobowościowe uwarunkowania efektywności oficerów kontrwywiadu*, Warszawa 2013.
6. Pawłowski J., Zdrodowski B., Kuliczkowski M., *Słownik terminów z zakresu bezpieczeństwa*, Toruń 2020.
7. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Netografia

1. *A Europe that Protects: Countering Hybrid Threats*, https://www.eeas.europa.eu/node/46393_en.
2. *ABW zatrzymała 2 obywateli Rosji*, https://www.abw.gov.pl/pl/informacje/2368,ABW-zatrzymala-2-obywateli-Rosji.html.
3. Bilal A., *Wojna hybrydowa - nowe zagrożenia, złożoność i „zaufanie" jako antidotum*, https://www.nato.int/docu/review/pl/articles/2021/11/30/wojna-hybrydowa-nowe-zagrozenia-zlozonosc-i-zaufanie-jako-antidotum/index.html.
4. Bryjka F., Legucka A., *Dezinformacja i propaganda Rosji oraz Białorusi w kontekście polsko-białoruskiego kryzysu granicznego*, https://pism.pl/publikacje/dezinformacja-i-propaganda-rosji-oraz-bialorusi-w-kontekscie-polsko-bialoruskiego-kryzysu-granicznego.
5. *Countering hybrid threats*, https://www.nato.int/cps/en/natohq/topics_156338.htm.
6. Dyner A. M., *Działania hybrydowe Rosji przeciw państwom NATO i UE, Działania hybrydowe Rosji przeciw państwom NATO i UE*, https://pism.pl/publikacje/dzialania-hybrydowe-rosji-przeciw-panstwom-nato-i-ue.
7. Gönczi R., *Dezinformacja jako oręż wojny hybrydowej na granicy z Białorusią*, https://warsawinstitute.org/pl/dezionformacja-jako-orez-wojny-hybrydowej-na-granicy-z-bialorusia/.
8. *Hybrid threats*, https://www.hybridcoe.fi/hybrid-threats/.
9. Jawor A., *Zadania kontrwywiadu w dobie współczesnych zagrożeń*, https://infosecurity24.pl/za-granica/zadania-kontrwywiadu-w-dobie-wspolczesnych-zagrozen.
10. *Komunikat dotyczący działalności dywersyjnej FR*, https://www.abw.gov.pl/pl/informacje/2569,Komunikat-dotyczacy-dzialalnosci-dywersyjnej-FR.html.
11. Krajowy Plan Zarządzania Kryzysowego, https://www.gov.pl/web/rcb/krajowy-plan-zarzadzania-kryzysowego.
12. Służba Kontrwywiadu Wojskowego, https://www.cyber.mil.pl/articles/o-nas-f/2018-11-20m-suzbakontrwywiadu-wojskowego/.