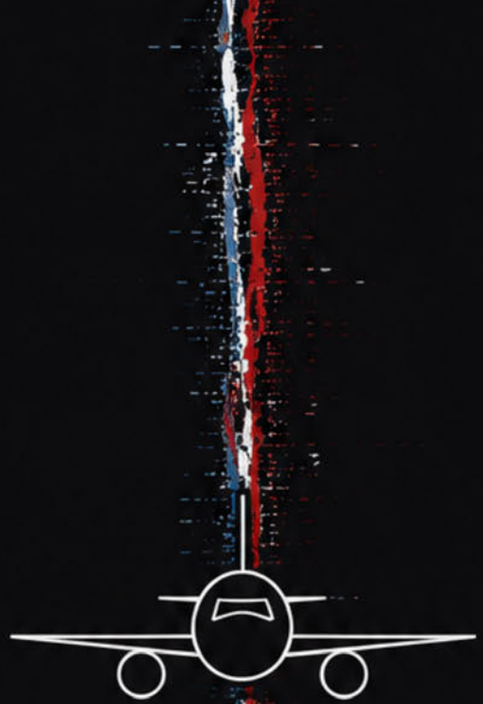
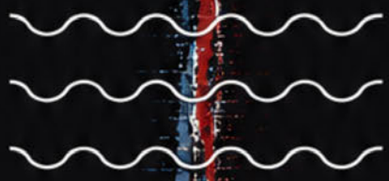
BIAŁA KSIĘGA



ROSYJSKICH AKTÓW SABOTAŻU
I DYWERSJI WOBEC CZŁONKÓW
RADY PAŃSTW MORZA BAŁTYCKIEGO

FILIP BRYJKA
ANNA MARIA DYNER
ALEKSANDRA KOZIOŁ



PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIAŁA KSIĘGA
rosyjskich aktów sabotażu i dywersji wobec członków Rady Państw Morza Bałtyckiego

Filip Bryjka, Anna Maria Dyner, Aleksandra Kozioł

Warszawa, maj 2026
Polski Instytut Spraw Międzynarodowych

Redakcja: **Marta Przyłuska-Brzostek**

Redakcja techniczna i projekt okładki: **Dorota Dołęgowska**

zdjęcie na okładce: **Aleksandra Kozioł**

ISBN 978-83-68555-31-8

E-ISBN 978-83-68555-32-5

Polski Instytut Spraw Międzynarodowych
Warecka 1a, 00-950 Warszawa
tel. (+48) 22 556 80 00
pism@pism.pl, www.pism.pl

Druk:
Mazowieckie Centrum Poligrafii
ul. Lisi Jar 29
05-270 Marki

Spis treści

Wstęp i główne wnioski

Od momentu rozpoczęcia pełnoskalowej inwazji na Ukrainę Rosja zintensyfikowała działania hybrydowe[1] przeciwko państwom NATO, szczególnie tym, które najbardziej aktywnie wspierały ukraiński opór. W tym gronie znaleźli się członkowie Rady Państw Morza Bałtyckiego (RPMB), wobec których Rosja zastosowała całe spektrum narzędzi, takich jak akty dywersji i sabotażu wymierzone w infrastrukturę krytyczną, incydenty związane z naruszaniem przestrzeni powietrznej i granic morskich czy zakłócenia sygnału GNSS (radiowe transmisje satelitarne), które tworzyły szereg problemów w funkcjonowaniu żeglugi morskiej i powietrznej. Celem rosyjskich operacji było nie tylko spowodowanie wymiernych szkód czy testowanie sposobów reakcji i odpowiedzi państw RPMB, ale także kognitywne oddziaływanie na ich społeczeństwa, aby funkcjonowały w poczuciu rosnącego zagrożenia. Działania wobec członków RPMB wyróżniały się przy tym skalą, a zdecydowana większość aktów dywersji i sabotażu odnotowana w państwach europejskich od lutego 2022 r. była podjęta przeciw nim.

Biorąc to pod uwagę, państwa RPMB powinny poszerzyć i wzmocnić współpracę mającą na celu zapobieganie i przeciwstawianie się tym zagrożeniom. Ofensywna natura rosyjskich działań dywersyjno-sabotażowych, które zostały zidentyfikowane od 2022 r., a zintensyfikowane w 2024 r., świadczy o gotowości Rosji do podejmowania coraz większego ryzyka (w tym związanego z ofiarami śmiertelnymi) w celu destabilizowania państw NATO i UE.

Skuteczne przeciwdziałanie kolejnym atakom wymaga zatem wysokiego poziomu świadomości sytuacyjnej, która może być zapewniona dzięki ścisłej współpracy (na poziomie krajowym i międzynarodowym) wojskowych i cywilnych służb wywiadowczych i kontrwywiadowczych, straży granicznych i policji. Członkowie RPMB mają w tym zakresie istotny potencjał wynikający z walki z podobnymi zagrożeniami i bliskości geograficznej. Mogą zatem rozważyć utworzenie specjalnego systemu wymiany informacji na temat zagrożeń hybrydowych. Istotne będzie także jednoznaczne wskazywanie sprawców działań sabotażowych i dywersyjnych. Brak atrybucji będzie utrudniał podejmowanie skoordynowanych działań zarówno prewencyjnych, jak i stanowiących odpowiedzi na zagrożenia.

[1] „Hybrid threats as a concept", European Centre of Excellence for Countering Hybrid Threats, www.hybridcoe.fi.

Biorąc pod uwagę, że schematy działania Rosji są znane i powtarzalne, należałoby na tej podstawie opracować katalog dobrych praktyk określający wspólne reguły monitorowania, raportowania i reagowania na operacje hybrydowe. Państwa regionu Morza Bałtyckiego powinny zobowiązać się do konsekwentnego stosowania się do zawartych w nim zasad, ponieważ tylko spójna reakcja wszystkich może skutecznie oddziaływać na Rosję. Dopiero całe spektrum działań podejmowanych przez państwa NATO i UE może zmniejszyć ryzyko kolejnych incydentów hybrydowych.

Metodologia

Celem niniejszego raportu jest zidentyfikowanie aktów dywersji i sabotażu, które wystąpiły na terenie krajów należących do RPMB od pełnoskalowej inwazji Rosji na Ukrainę 24 lutego 2022 r. do 13 kwietnia 2026 r. Intencją autorów jest nie tylko wskazanie incydentów, które można bezpośrednio lub pośrednio przypisać Rosji lub Białorusi, ale także analiza dynamiki prowadzonej kampanii dywersyjno-sabotażowej, jej celów i uwarunkowań strategicznych. Utylitarnym celem raportu jest sformułowanie wniosków i praktycznych rekomendacji, które będą mogły zostać wdrożone przez państwa RPMB (a także pozostałych sojuszników w ramach NATO i UE), by zwiększyć odporność i skuteczność reagowania na dywersję i sabotaż.

Autorzy raportu definiują działania dywersyjno-sabotażowe jako zorganizowane operacje mające na celu osłabienie państwa poprzez zakłócanie jego funkcjonowania w wymiarze politycznym, społecznym, gospodarczym i wojskowym. Rozróżniają przy tym – zgodnie z terminologią obowiązującą w Rosji – pojęcie dywersji i sabotażu. Sabotaż to działania mające na celu zakłócanie funkcjonowania systemu od wewnątrz, np. przez pracowników danej instytucji. Może to oznaczać umyślne zaniedbanie lub zaniechanie obowiązków służbowych, fałszowanie dokumentów, dyskredytowanie współpracowników czy świadome wyrządzenie szkód materialnych lub finansowych. Dywersja z kolei polega na fizycznym niszczeniu obiektów, np. magazynów, linii komunikacyjnych czy infrastruktury, m.in. z wykorzystaniem materiałów wybuchowych lub łatwopalnych, w celu odwrócenia uwagi przeciwnika od innych działań. Ma ona także istotny wymiar psychologiczny, polegający m.in. na zastraszeniu atakowanego społeczeństwa, wymaga więc strategicznego planowania i wykorzystania przez stronę atakowaną większych zasobów sił i środków[2].

Autorzy zdecydowali się też na zaprezentowanie roli i znaczenia narzędzi hybrydowych w rosyjskiej polityce zagranicznej i bezpieczeństwa. Koncepcja tzw. wojny nowej generacji, przedstawiona przez szefa Sztabu Sił Zbrojnych Rosji gen. Walerija Gierasimowa w wystąpieniach z 2013 i 2019 r., sięga co najmniej początków Związku Radzieckiego, a obecnie jest rozwijana m.in. dzięki coraz nowocześniejszym narzędziom i metodom wrogiego oddziaływania.

[2] E. Ferris, *Russian Sabotage of NATO Infrastructure: Identifying Alliance Vulnerabilities*, RUSI, 26 marca 2026 r., www.rusi.org.

Przyjęta metodologia opiera się na założeniu, że skuteczna analiza wymaga zarówno uporządkowanej klasyfikacji przypadków, jak i zastosowania zestawu zmiennych analitycznych pozwalających uchwycić ich ewolucję w czasie i przestrzeni. Podstawę analizy stanowi podział incydentów dywersyjno-sabotażowych na następujące domeny operacyjne:

- **morską** – obejmującą akty dywersji wobec podwodnej infrastruktury energetycznej (rurociągi i kable), nawodnej infrastruktury energetycznej, a także portów i baz marynarki wojennej;
- **lądową** – obejmującą m.in. akty dywersji i sabotażu skierowane przeciwko liniom kolejowym, tzw. celom miękkim (np. sklepom wielkopowierzchniowym, magazynom), bazom wojskowym, przemysłowi zbrojeniowemu i infrastrukturze krytycznej;
- **powietrzną** – związaną przede wszystkim z naruszeniami przestrzeni powietrznej, w tym z wykorzystywaniem dronów, a także zakłócaniem sygnału GNSS.

Autorzy celowo zrezygnowali z identyfikowania i analizowania incydentów w cyberprzestrzeni, ograniczając się do tych, które miały charakter fizyczny (kinetyczny). Kwestie dotyczące domeny kosmicznej (np. zagłuszanie sygnału GNSS) zostały uwzględnione w rozdziale dotyczącym wrogich aktywności w przestrzeni powietrznej. Z kolei rozdział poświęcony dywersji i sabotażowi na lądzie jest poszerzony o elementy analizy sfery informacyjnej (kognitywnej), coraz częściej wskazywanej przez NATO jako szósta domena operacyjna.

Taka struktura umożliwia uporządkowanie materiału empirycznego według spójnych kategorii i zastosowanie analizy porównawczej, a także identyfikację sektorów szczególnie podatnych na działania sabotażowe. Autorzy raportu poddali analizie także techniki, taktyki i procedury (TTPs) wykorzystywane przez Rosję w poszczególnych domenach operacyjnych, co pozwala uchwycić zarówno kontekst, jak i mechanizm działania, analizować powtarzalność i dostosowywanie metod przez sprawców, identyfikować wzorce operacyjne w obrębie domen i pomiędzy nimi.

W pracy nad raportem autorzy korzystali przede wszystkim z informacji znajdujących się w źródłach otwartych, m.in. z publicznych wersji raportów służb wywiadowczych państw RPMB i tekstów prasowych. Użyto także materiałów przekazanych analitykom PISM przez Agencję Bezpieczeństwa Wewnętrznego (ABW), Agencję Wywiadu (AW), Służbę Kontrwywiadu Wojskowego (SKW), Dowództwo Operacyjne Rodzajów Sił Zbrojnych (DO RSZ), Rządowe Centrum Bezpieczeństwa (RCB), Centralne Biuro Śledcze Policji (CBŚP), a także polskie placówki dyplomatyczne w państwach RPMB. Ze względu na wrażliwy charakter informacji, często objętych klauzulą niejawności, a także z powodu trudności z ustaleniem w części przypadków sprawców i atrybucji zleceniodawcy, niniejsza Biała Księga nie ma ambicji zbudowania jednej kompleksowej bazy danych zawierającej wszystkie dotąd zidentyfikowane akty sabotażu, które można jednoznacznie powiązać z Rosją. Jest to zadanie niewykonalne bez woli rządów, by ujawnić i udostępnić wszystkie posiadane w tym zakresie informacje.

Pogłębiona wiedza autorów na temat przedmiotu badań, szczególnie w zakresie metod analizy zagrożeń tego typu, pochodzi również z licznych zagranicznych wyjazdów studyjnych, udziału w konferencjach, warsztatach i grach symulacyjnych, a także z zamkniętych seminariów eksperckich i projektów badawczych. Spośród nich warto wspomnieć m.in. o seminarium zatytułowanym „Workshop on the Financing of Russian Sabotage", które odbyło się w listopadzie 2025 r. w Warszawie. Zostało ono zorganizowane przez PISM we współpracy z brytyjskim ośrodkiem analitycznym The Royal United Services Institute (RUSI) i było poświęcone przede wszystkim kwestiom sposobów finansowania przez Rosję działań sabotażowych w Europie[3]. Ważny wkład w przygotowanie tego raportu miał także udział jednego z autorów w projekcie badawczym „Deterrence and Defense in the Baltic Sea Region Against the Russian Threat", realizowanym przez The George C. Marshall Center for European Security Studies (GCMC) oraz Centrum Doktryn i Szkolenia Sił Zbrojnych RP (CDiS SZ)[4].

Autorzy dziękują także za wsparcie dwóm stażystom w programie Bezpieczeństwo Międzynarodowe PISM – panu Grzegorzowi Batorowi i panu Janowi Staroście za pomoc w wyszukiwaniu i agregacji części danych.

W pracach nad raportem autorzy korzystali również z dotychczasowych badań nad rosyjską dywersją i sabotażem, weryfikując znajdujące się tam dane i poszerzając je o badania własne. Na szczególne odnotowanie zasługuje kilka kompleksowych opracowań. Opublikowany we wrześniu 2024 r. raport Amerykańskiej Komisji Helsińskiej przedstawia 150 rosyjskich operacji hybrydowych przeprowadzonych na terytorium NATO od początku rosyjskiej inwazji na Ukrainę. Zostały one podzielone na cztery kategorie:

1) ataki na infrastrukturę krytyczną (33% przypadków),
2) kampanie przemocy (20%),
3) instrumentalizacja migracji (12%),
4) manipulacje informacyjne i ingerencje w wybory (35%)[5].

Chociaż raport Komisji jest dobrą ilustracją skali rosyjskich działań wywrotowych prowadzonych przeciwko państwom NATO, obejmuje jednak szerszy zakres zdarzeń niż te, które niniejsza Biała Księga klasyfikuje jako dywersję lub sabotaż.

Bardziej precyzyjne dane można znaleźć w raporcie Centrum Studiów Strategicznych i Międzynarodowych (CSIS), w którym zidentyfikowano 52 potwierdzone przypadki tego

[3] Szerzej zob. K. Redlowska, M. Popyk, T. Keatinge, *Responding to Russian Sabotage Financing*, RUSI, 14 stycznia 2026 r., www.rusi.org

[4] Niektóre ustalenia uwzględnione w tym raporcie pochodzą z publikacji podsumowującej ten projekt, zob. F. Bryjka, *Russian Sabotage Targeting NATO*, w: F. Rademacher, A. Lis (red.), *Deterrence and Defense in the Baltic Sea Region Against the Russian Threat*, Doctrine and Training Center of the Polish Armed Forces, Bydgoszcz 2026, s. 7–32.

[5] *Spotlight on the Shadow War: Inside Russia's Attacks on NATO Territory*, U.S. Helsinki Commission, 2024, www.csce.gov.

rodzaju działań podejmowanych na zlecenie Rosji od stycznia 2022 r. do marca 2025 r.[6] Podobne obliczenia przedstawiono w raporcie International Institute for Strategic Studies (IISS), w którym odnotowano dodatkowych 11 ataków hybrydowych w Europie od stycznia do maja 2025 r.[7] W raporcie CSIS wskazano, że rosyjskie działania dywersyjno-sabotażowe były skierowane głównie przeciwko infrastrukturze transportowej (27%), celom rządowym i wojskowym (27%), infrastrukturze energetycznej (21%) oraz przemysłowi obronnemu (21%). Autorzy opracowania przeanalizowali także taktyki ataków i wykazali, że rosyjscy agenci najczęściej (w 35% przypadków) korzystali z materiałów zapalających i wybuchowych, a w 27% przypadków użyto tępych lub ostrych narzędzi, takich jak kotwice służące do przecinania podmorskich kabli. W 15% były to ataki elektroniczne, a w 8% jako narzędzie wykorzystano nielegalnych migrantów[8].

Badacze holenderskiego Uniwersytetu w Leiden zidentyfikowali 63 rosyjskie operacje hybrydowe w latach 2022–2024, obejmujące sabotaż (36), wandalizm (10), operacje wpływu (8), zabójstwa (4), terroryzm (4) i instrumentalizację migracji (1)[9]. Ważny wkład w analizowanie rosyjskich działań dywersyjno-sabotażowych wniosły także badania przeprowadzone przez International Center for Countering Terrorism (ICCT) i GLOBSEC. Autorzy raportu zidentyfikowali 151 aktów sabotażu przeprowadzonych na terytorium UE na zlecenie Rosji w okresie od stycznia 2022 r. do końca lutego 2026 r. Ponad połowa z nich (83 incydenty) miała miejsce w państwach RPMB – najwięcej (31) w Polsce, po 15 w Niemczech i na Litwie, 11 w Estonii, 5 na Łotwie, po 2 w Szwecji i Finlandii, po 1 w Danii i Norwegii[10].

[6] W przypadku każdego ataku uwzględnionego w bazie danych CSIS zidentyfikowało co najmniej trzy wiarygodne źródła potwierdzające bezpośredni lub pośredni udział rządu rosyjskiego oraz przeprowadziło wywiady z ekspertami rządowymi i pozarządowymi. Poproszono również kilku ekspertów o przegląd danych i analizy oraz oceniono poziom pewności dla każdego incydentu.

[7] C. Edwards, N. Seidenstein, *The scale of Russian sabotage operations against Europe's critical infrastructure*, The International Institute for Strategic Studies (IISS), 19 sierpnia 2025 r., www.iiss.org.

[8] S.G. Jones, *Russia's shadow war against the West*, Center for Strategic & International Studies (CSIS), 18 marca 2025 r., www.csis.org.

[9] B. Schuurman, *Russian operations against Europe since the 2022 invasion of Ukraine*, University of Leiden, Haga 2025.

[10] Szerzej zob. J. Lanchès, K. Rękawek, *More of the Same: Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, International Centre for Counter-Terrorism, 23 lutego 2026 r., www.icct.nl. Tekst uzupełnia dane uwzględnione w raporcie D. Hajdu (red.), *Russia's Crime–Terror Nexus: Criminality as a Tool of Hybrid Warfare in Europe*, International Centre for Counter-Terrorism/Globsec, wrzesień 2025, s. 18–19, www. globsec.org.

Strategia Rosji

Rosja postrzega NATO i jego państwa członkowskie jako główne źródło zagrożenia. Sygnalizuje to od lat w najważniejszych dokumentach strategicznych w obszarze bezpieczeństwa, takich jak doktryna wojenna z 2014 r.[11], strategia bezpieczeństwa narodowego z 2021 r.[12], a pośrednio także w przyjętej w 2024 r. tzw. doktrynie jądrowej[13]. Deklaracje o tym, że Rosja – zwłaszcza od momentu rozpoczęcia pełnoskalowej inwazji na Ukrainę 24 lutego 2022 r. – znajduje się de facto w stanie wojny z NATO, wielokrotnie padały też ze strony najważniejszych rosyjskich polityków, w tym Dmitrija Miedwiediewa czy rzecznika Kremla Dmitrija Pieskowa[14].

Celem Rosji jest zatem jak największe osłabienie głównego adwersarza za pomocą wszystkich środków, które nie przekroczą progu wojny kinetycznej i nie narażą jej na systemowy odwet. Aktywności te Rosja stara się prowadzić we wszystkich obszarach, które uważa za szczególnie wrażliwe, a więc w sferze informacyjnej i cyberprzestrzeni, ale podejmuje je także wobec infrastruktury krytycznej. Wykorzystuje przy tym doświadczenia konfrontacji z państwami zachodnimi sięgające okresu międzywojennego i kształtowania się państwa radzieckiego, a później zimnej wojny, oraz poszerza zakres działań o możliwości generowane przez nowoczesne technologie.

Zarys koncepcji wojny nowej generacji, która w państwach zachodnich najczęściej jest określana mianem wojny hybrydowej, został przedstawiony w 2013 r. przez generała armii Walerija Gierasimowa, szefa Sztabu Generalnego Sił Zbrojnych FR[15]. Zakłada ona, że wrogie aktywności wobec adwersarzy mają mieć charakter polityczny, ekonomiczny, informacyjny i społeczny, a do ich prowadzenia można wykorzystać „potencjał protestu" lub wysoki stopnień polaryzacji w społeczeństwach państw stanowiących cel

[11] *Военная доктрина Российской Федерации*, Совет Безопасности Российской Федерации, www.scrf.gov.ru/security/military/document129/.

[12] *Указ Президента Российской Федерации от 02.07.2021 г. № 400 о Стратегии национальной безопасности Российской Федерации,* Президент России, www.kremlin.ru/acts/bank/47046.

[13] *Указ Президента Российской Федерации от 19.11.2024 г. № 991 об утверждении Основ государственной политики Российской Федерации в области ядерного сдерживания*, Президент России, www.kremlin.ru/acts/bank/51312.

[14] *Медведев заявил, что Россия в одиночку сражается с Западом*, ТАСС, https://tass.ru/politika/16307167.

[15] В. Герасимов, *Ценность науки в предвидении*, „Военно-промышленный курьер", ВПК.name, https://vpk.name.

agresji. Gierasimow wskazał też, że pierwsza faza działań militarnych powinna koncentrować się na wyeliminowaniu infrastruktury krytycznej, co uniemożliwi działania struktur państwowych i będzie negatywnie wpływało na morale zaatakowanego społeczeństwa[16].

Zaprezentowana przez gen. Gierasimowa koncepcja była efektem dokonanej przez Rosję analizy tzw. kolorowych rewolucji, które miały miejsce na obszarze byłego ZSRR na początku XXI w., oraz wydarzeń arabskiej wiosny w Afryce i na Bliskim Wschodzie. Rosja zaczęła wdrażać plan Gierasimowa już w 2013 r., m.in. poprzez działania gospodarcze, polityczne i informacyjne wymierzone w Ukrainę, których celem było wymuszenie na jej władzach zmiany prozachodniej polityki i rezygnacji z podpisania umowy stowarzyszeniowej z Unią Europejską. Cel ten udało się osiągnąć. Wykorzystując środki wojskowe, informacyjne oraz potencjał protestacyjny ludności, Rosja zdołała też opanować Krym i wbrew prawu przyłączyć go do swojego terytorium. Skuteczność narzędzi oddziaływania strona rosyjska sprawdziła też w okresie 2014–2022, podczas nieregularnych działań zbrojnych w Donbasie.

W 2019 r. gen. Gierasimow uzupełnił swoje wcześniejsze tezy[17] i podkreślił, że w celu zwiększenia skuteczności narzędzi niewojskowych należy aktywnie wykorzystywać nie tylko środki nacisku gospodarczego, politycznego, dyplomatycznego i informacyjnego, ale także demonstrację siły militarnej. Dodał, że rosyjskie siły zbrojne muszą być gotowe do prowadzenia wojen i konfliktów zbrojnych nowego typu, z wykorzystaniem metod asymetrycznych. Tym samym jasno wskazał priorytety państwa rosyjskiego, a szczególnie jego struktur siłowych. W koncepcjach prezentowanych przez gen. Gierasimowa pojawia się nawet stwierdzenie, że aby oddziaływanie było skuteczne, środki niewojskowe i wojskowe powinny być wykorzystywane w stosunku 4:1[18].

Warto jednak podkreślić, że w rozumieniu Rosji wojna nowoczesna jest kontynuacją i rozwinięciem radzieckiej koncepcji „działań aktywnych", która zakładała aktywności o charakterze dezinformacyjnym, destabilizującym i agenturalnym, wynikające z aktualnych priorytetów ZSRR i nastawione na wpływanie na politykę innych państw. Środki i metody przetestowane w Ukrainie w latach 2013–2022 Rosja zaczęła na szeroką skalę stosować wobec państw NATO, by wpływać na ich politykę, dzięki czemu udoskonala swoje sposoby działania. Rosja koncentruje się przy tym na specjalnych operacjach dywersyjnych oraz wywiadowczych. Do tych pierwszych coraz częściej rekrutuje niezwracające uwagi służb osoby, które – głównie pod wpływem motywacji finansowej – godzą się na prowadzenie różnych działań rozpoznawczych czy dokonywanie aktów dywersji. Część osób zatrzymywanych z tego powodu przez kontrwywiady państw

[16] Więcej: M. Wojnowski, *Koncepcja „wojny nowej generacji" w ujęciu strategów Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 13/2025, www.abw.gov.pl.

[17] *Выступление генерала армии Валерия Герасимова на конференции по развитию военной стратегии*, LIVEJOURNAL, https://bmpd.livejournal.com/3557155.html.

[18] К.Е. Кожухова, *Концепция политической войны: подходы Запада и Китая*, „Вестник Московского государственного лингвистического университета. Общественные науки" 2024, nr 3 (856), s. 17–22.

NATO zeznaje, że nie wiedziały, że działają na rzecz Rosji. Zostali oni zwerbowani za pośrednictwem różnego rodzaju serwisów społecznościowych (takich jak Telegram), a wynagrodzenie otrzymywali głównie w formie kryptowalut[19]. Rosyjskie służby starają się do swoich celów wykorzystywać skrajne środowiska, ale werbunek prowadzą też wśród uchodźców i migrantów, co dodatkowo ma wzniecać spory wewnątrzpolityczne w atakowanych państwach.

Do osiągnięcia swoich celów Rosja wykorzystuje także innych aktorów, w tym państwowych. Dlatego z perspektywy członków RPMB, zwłaszcza Polski, Litwy i Łotwy, bardzo istotne są wrogie działania podejmowane przez Białoruś. Białoruskie służby nie tylko wspierają rosyjskie aktywności, ale także przeprowadzają niezależne operacje, których celem jest przeciążenie służb kontrwywiadowczych państw sąsiednich, co ma zwiększyć szanse na skuteczność części ataków dywersyjnych i sabotażowych.

Zgodnie z koncepcją gen. Gierasimowa wśród używanych przez Rosję narzędzi oddziaływania istotne miejsce zajmuje demonstracja militarna. Rosyjskie władze stosują ją, m.in. organizując ćwiczenia wojskowe na Morzu Bałtyckim[20] i u granic państw NATO[21] (również we współpracy z Białorusią i Organizacją Układu o Bezpieczeństwie Zbiorowym[22]). Służby wywiadowcze Finlandii regularnie raportują też o zwiększaniu rosyjskiej obecności wojskowej w pobliżu jej granic i o wzmacnianiu odtworzonego w 2024 r. Leningradzkiego Okręgu Wojskowego[23].

Wrogie działania przeciwko członkom RPMB (a szczerzej także państwom NATO) wskazują, że Rosja dąży do wywołania kryzysu, który umożliwi jej osiągnięcie celów polityczno-wojskowych, m.in. uznania jej stref wpływów i znaczącego osłabienia państw wschodniej flanki Sojuszu. Oznacza to też, że Rosja jest gotowa do podejmowania długotrwałego wysiłku i stosowania szerokiej palety narzędzi mających na celu osłabienie państw NATO, w tym członków RPMB. Tym samym rosyjskie zagrożenie należy traktować jako trwałe i poważne, co wymaga planowania długofalowych działań prewencyjnych. Analiza polityki zagranicznej Rosji jasno wskazuje, że jej władze postrzegają państwa NATO jako wrogie, a zatem działania hybrydowe przeciwko nim mają charakter długoterminowy i nie należy oczekiwać ich zaprzestania.

[19] M. Miłosz, *Jarosław Stróżyk: Zachowań prorosyjskich jest w Polsce coraz więcej*, „Rzeczpospolita", 16 marca 2026 r., www.rp.pl.

[20] A.M. Dyner, *Ćwiczenia „Ocean 2024" – rosyjska sygnalizacja strategiczna*, „Biuletyn PISM" nr 138 (2948), 26 września 2024 r., www.pism.pl.

[21] A.M. Dyner, *„Zapad 2025" – sygnalizacja Rosji i Białorusi mimo wojny*, „Biuletyn PISM" nr 101 (3104), 23 września 2025 r., www.pism.pl.

[22] A.M. Dyner, *Znaczenie ćwiczeń OUBZ na Białorusi*, „Komentarz PISM" nr 63/2025, 8 września 2025 r., www.pism.pl.

[23] *Finnish Military Inteligence Review 2026*, The Finnish Defence Forces, https://puolustusvoimat.fi.

Rosyjskie działania wymierzone w członków RPMB

Rosyjskie wrogie działania dywersyjno-sabotażowe koncentrowały się na domenach morskiej, lądowej i powietrznej. Prowadzone w ich ramach aktywności niejednokrotnie były ze sobą powiązane (np. zagłuszanie sygnału GNSS, które miało negatywne konsekwencje zarówno dla żeglugi powietrznej, jak i morskiej) oraz podejmowane w tym samym czasie wobec kilku państw, co miało wywołać dodatkowe efekty, m.in. psychologiczne, tworząc wrażenie państwa omnipotentnego, będącego w stanie skutecznie oddziaływać wielodomenowo w całym regionie Morza Bałtyckiego.

Domena morska

Morze Bałtyckie w 2022 r. stało się centralnym obszarem, na którym Rosja coraz aktywniej prowadzi operacje mające znamiona wojny hybrydowej[24]. Chociaż ich intensywność jest niższa niż w przypadku domeny powietrznej i lądowej, mogą one wywoływać daleko idące konsekwencje dla środowiska, żeglugi oraz gospodarki. Ma to szczególne znaczenie wobec charakteru Morza Bałtyckiego – stosunkowo niewielkiego i półzamkniętego akwenu, gdzie nawet incydent o niewielkich rozmiarach wpływa na wiele państw regionu.

Rosja prowadzi operacje mające znamiona wojny hybrydowej przy użyciu narzędzi i środków, które utrudniają lub uniemożliwiają bezpośrednie powiązanie wydarzeń ze strukturami siłowymi lub wywiadowczymi państwa rosyjskiego. W tym celu wypracowała szerokie instrumentarium, w skład którego wchodzą różnorodne formy działania i środki operacyjne. Operacje są rozłożone w czasie i prowadzone na masową skalę. Często mają też charakter wielodomenowy, co dodatkowo komplikuje ich wykrywanie.

Operacje hybrydowe w domenie morskiej przybierają dwie główne formy i są realizowane przy pomocy dwóch odmiennych strategii.

[24] G. Giannopoulos, H. Smith, M. Theocharidou, *The Landscape of Hybrid Threats*, European Commission & the European Centre of Excellence for Countering Hybrid Threats, Publications of the European Union, 2021, https://op.europa.eu.

Operacje rozpoznawcze:

- umożliwiają zebranie informacji na temat sił i słabych punktów przeciwnika;
- służą przygotowaniu działań kinetycznych (hybrydowych lub wojennych);
- prowadzone są przez jednostki powiązane z państwem rosyjskim.

Działania dywersyjne i sabotażowe:

- umożliwiają uszkodzenie lub zaburzenie działania konkretnego obiektu lub systemu;
- służą wdrażaniu zaplanowanych działań kinetycznych;
- prowadzone są przez pośredników.

Operacje te uzupełnia szeroki wachlarz działań wpisujących się w cele wojny hybrydowej, ale niebędących bezpośrednią formą ataku. Polegają one na doprowadzeniu do powstania takich warunków na morzu, w których utrudnione jest funkcjonowanie wszystkich jednostek pływających – zarówno wojskowych, jak i cywilnych. W skład takich działań wchodzą zakłócenia żeglugi polegające na notorycznym wyłączaniu transponderów AIS[25], niebezpiecznych manewrach wokół innych jednostek lub obiektów, a także kreowanie tzw. botów, czyli fikcyjnych statków widocznych w widmie radarowym[26]. Często działania te mają za zadanie rozproszyć uwagę służb państw regionu Morza Bałtyckiego lub zmylić je, podczas gdy realizowane są inne zadania operacyjne.

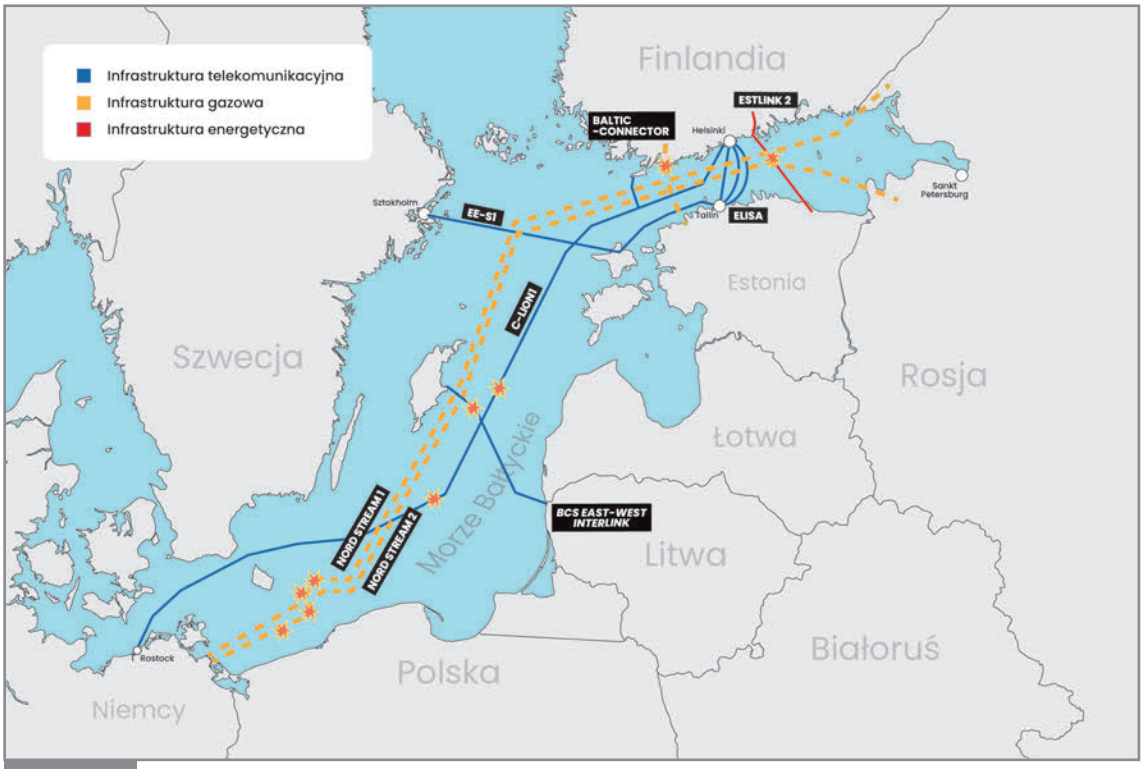
Dotychczasowe operacje hybrydowe Rosji w regionie Morza Bałtyckiego charakteryzują się wysoką powtarzalnością schematu działania. Stosunkowo najrzadziej wykorzystywane – ale mające największe skutki – są działania sabotażowe. Od 2022 r. doszło do trzech aktów sabotażu, których celem była podmorska infrastruktura energetyczna, oraz do sześciu ataków na podmorską infrastrukturę komunikacyjną (zob. załącznik). Tylko w przypadku dwóch z nich pojawiły się informacje o przynależności statku dokonującego sabotażu do rosyjskiej „floty cieni"[27], w pozostałych sytuacjach albo nie udało się ustalić sprawcy, albo pływał on pod banderą państwa trzeciego. Aż czterokrotnie były to statki chińskie, co sugeruje bezpośrednie zaangażowanie władz ChRL we wspieranie rosyjskiej wojny hybrydowej.

[25] System automatycznej identyfikacji (Automatic Identification System, AIS) jest międzynarodowo uznanym systemem służącym zarządzaniu ruchem morskim. Pozwala wymieniać dane między statkami i instytucjami nadbrzeżnymi o pozycji, kursie i prędkości jednostek pływających, w czasie rzeczywistym. Zgodnie ze standardami Międzynarodowej Organizacji Morskiej obejmuje wszystkie jednostki pływające.

[26] W Polsce jest to Zautomatyzowany System Radarowego Nadzoru Obszarów Morskich (ZSRN), wykorzystywany głównie przez Straż Graniczną.

[27] „Rosyjska «flota cieni» – starzejące się tankowce używane przez Rosję do obchodzenia zachodnich sankcji (głównie pułapu cenowego) przy eksporcie ropy i produktów naftowych. Jej statki nie korzystają z usług świadczonych branży morskiej przez podmioty z państw koalicji sankcyjnej, unikają inspekcji państwa bandery/portu i audytów komercyjnych, nie posiadają pełnego ubezpieczenia P&I (morskiego od odpowiedzialności cywilnej) lub mają minimalne pokrycie, często są przestarzałe lub w złym stanie technicznym, mają nietransparentną strukturę własności (często zmieniają bandery), ukrywają tożsamość i pozycje (poprzez manipulacje systemem automatycznej identyfikacji (AIS), zmiany nazw) oraz wykonują ryzykowne i nielegalne przeładunki *ship-to-ship* (STS)". Cyt. za: T. Pastucha, *Wyzwania ekologiczne*, w: A. Dziubińska, A. Kozioł (red.), *(Nie)bezpieczne wody. Region Morza Bałtyckiego wobec redefinicji bezpieczeństwa w Europie*, Raport PISM, kwiecień 2024, www.pism.pl.

Działania sabotażowe na Morzu Bałtyckim (2022–2026)



Źródło: opracowanie własne.

Uruchomienie operacji „Baltic Sentry" w ramach NATO[28] było bezpośrednią odpowiedzią na atak przeprowadzony w grudniu 2024 r. na kabel energetyczny łączący Estonię i Finlandię (zob. tabela), gdy – po raz pierwszy – udało się wskazać, że odpowiedzialny za spowodowanie uszkodzeń był statek rosyjskiej „floty cieni". Schemat działania Rosji był w tym przypadku szczególnie dobrze widoczny, gdyż do zniszczenia doszło niedługo przed odłączeniem państw bałtyckich od rosyjskiego systemu elektroenergetycznego. Wzmocnione dzięki „Baltic Sentry" patrole usprawniły monitorowanie i reagowanie na operacje hybrydowe. W 2025 r. doszło co prawda do dwóch aktów sabotażu, ale w obu przypadkach jednostki odpowiedzialne za nie były monitorowane, zostały zatrzymane i przeprowadzono ich inspekcje.

Zdecydowanie trudniejsze jest prześledzenie operacji rozpoznawczych, w tym związanych z naruszeniem wyłącznych stref ekonomicznych państw regionu Morza Bałtyckiego. Służby stosują różne podejście do tego rodzaju incydentów, jednak w większości przypadków nie informują o nich publicznie. Tylko w wyłącznej strefie ekonomicznej Polski wykryto od 2022 r. kilkanaście zdarzeń mających znamiona działań hybrydowych. Cywilne jednostki prowadziły operacje rozpoznawcze środowiska morskiego,

[28] *Baltic Sentry to enhance NATO's presence in the Baltic Sea*, SHAPE Public Affairs Office, 14 stycznia 2025 r., https://shape.nato.int/.

miejsc położenia i miejsc planowanych instalacji podwodnych i nawodnych, ćwiczeń morskich oraz morskich operacji transportu sprzętu wojskowego.

Tabela 1

Charakterystyka rosyjskich operacji rozpoznawczych na morzu

RODZAJ JEDNOSTKI	SPRZYJAJĄCE CZYNNIKI
Wojskowe jednostki rozpoznawcze	- sprzęt rozpoznawczy klasy wojskowej przystosowany do szerokiego zakresu pasm (elektromagnetyczne, hydroakustyczne, podczerwień) - możliwość długiego czasu operowania - wyspecjalizowana załoga
Wojskowe jednostki bojowe	- możliwość szybkiej zmiany miejsca - integracja danych rozpoznawczych z systemami walki
Statki rybackie i statki-przetwórnie	- duże obszary połowów - łatwość zmiany miejsca połowów - czas przebywania w miejscach połowów
Statki badawcze	- swoboda doboru obszaru badań - długi czas przebywania w miejscu badań - wyspecjalizowany sprzęt badawczy
Statki żaglowe	- swoboda przepływu i obserwacji ruchów okrętów, ćwiczeń, innych wybranych działań
Drobnicowce	- możliwość koordynacji z innymi jednostkami - łatwość uwalniania statków bezzałogowych

Źródło: opracowanie własne częściowo na podst. danych Agencji Wywiadu.

Od marca 2025 do marca 2026 r. Polska wykryła i zareagowała na przynajmniej cztery incydenty związane z rosyjskimi jednostkami, które prowadziły działania rozpoznawcze, testowały sposób reagowania służb lub miały na celu sabotaż (w żadnym przypadku nie doszło do uszkodzeń). Zaobserwowany schemat działania w wyłącznej strefie ekonomicznej Polski pokrywał się z wykorzystywanym podczas incydentów na innych obszarach morskich, w tym poza regionem Morza Bałtyckiego.

Tabela 2

Incydenty w wyłącznej strefie ekonomicznej Polski

DATA	RODZAJ JEDNOSTKI	PRAWDOPODOBNY CEL	REAKCJA
maj 2025	statek rosyjskiej „floty cieni”	kabel energetyczny łączący Polskę ze Szwecją	interwencja polskiej Marynarki Wojennej
październik 2025	rosyjski statek rybacki	gazociąg	interwencja polskiej Straży Granicznej
listopad 2025	rosyjski statek naukowy Akademik B. Pietrow	naruszenie wyłącznej strefy ekonomicznej Polski	monitoring
luty 2026	rosyjski statek badawczy Akademik Joffe	przepłynięcie wzdłuż wybrzeża Polski	monitoring (wcześniej monitoring prowadziły okręty niemieckie i duńskie)

Źródło: opracowanie własne na podst. danych Agencji Bezpieczeństwa Wewnętrznego.

Rosyjskie władze wspierają kinetyczne operacje hybrydowe na poziomie politycznym, o czym świadczy propozycja, którą Ministerstwo Obrony Federacji Rosyjskiej przedstawiło 21 maja 2024 r.[29] Kwestionowało w niej przebieg granic morskich Rosji z Finlandią i Litwą z 1985 r. we wschodniej części Zatoki Fińskiej, a także okolicach Bałtyjska i Zielenogradska w obwodzie królewieckim. Reakcja państw na tę propozycję nie była skoordynowana – minister spraw zagranicznych Finlandii Elina Valtonen określiła ją mianem „rutynowej”, podczas gdy jej litewski odpowiednik Gabrielius Landsbergis nazwał propozycję „eskalacją”. Fakt, że sprawa była dla rosyjskich władz sposobem na testowanie reakcji państw regionu Morza Bałtyckiego, potwierdziły komentarze rzecznika Kremla Dmitrija Pieskowa. Zwrócił on uwagę na konfrontacyjną postawę tych krajów wobec Rosji, która musi zapewnić sobie bezpieczeństwo[30]. Był to też klasyczny przykład rosyjskiej strategii dezinformacyjnej, w której oskarżenia wobec przeciwnika opisują faktyczne intencje strony rosyjskiej i mają za zadanie przygotować opinię publiczną do działań o charakterze hybrydowym lub wojskowym, następujących po takiej wypowiedzi lub kampanii.

[29] Informacja pojawiła się na stronie internetowej Ministerstwa Obrony Federacji Rosyjskiej, ale następnego dnia została usunięta.

[30] C. Szumski, *Russia's push to change Baltic Sea border sparks concern in the region*, „Euractiv”, 22 maja 2024 r., www.euractiv.com.

Domena lądowa

Rosyjskie działania dywersyjno-sabotażowe prowadzone w domenie lądowej mają różny stopień zaawansowania i szkodliwości – od działalności rozpoznawczo-wywiadowczej, poprzez akty wandalizmu i przemocy politycznej, po ataki dywersyjne, sabotażowe i terrorystyczne. Działania kinetyczne są przy tym koordynowane z operacjami dezinformacyjnymi, których celem jest psychologiczne oddziaływanie na społeczeństwa i decydentów poprzez wywoływanie strachu i poczucia niebezpieczeństwa. Fizyczne ataki w połączeniu z fałszywymi narracjami rozpowszechnianymi za pośrednictwem rosyjskich kanałów dezinformacji (w tym trolli, botów i agentów wpływu) narzucają odbiorcom zmanipulowaną interpretację wydarzeń, odsuwają odpowiedzialność Rosji i przypisują ją Ukrainie lub władzom zaatakowanego państwa.

Podczas gdy w domenie morskiej głównym instrumentem Rosji jest „flota cieni", tak w domenie lądowej – by zminimalizować koszty i ryzyko działań dywersyjno-sabotażowych – rosyjskie służby wywiadowcze wykorzystują tzw. jednorazowych agentów (*disposable agents* lub *single use agents*) – niewyszkolonych amatorów rekrutowanych za pomocą mediów społecznościowych. Do pewnego stopnia daje to Rosji możliwość wiarygodnego zaprzeczenia (*plausible deniability*) i utrudnia zachodnim służbom atrybucję odpowiedzialności. Model ten został wypracowany przez Rosję, gdy po rozpoczęciu pełnoskalowej inwazji na Ukrainę państwa NATO i UE zdecydowały się wydalić ponad 600 rosyjskich dyplomatów, w tym ok. 400 funkcjonariuszy wywiadu działających w Europie pod przykryciem dyplomatycznym[31]. Chociaż rosyjskie zdolności do prowadzenia operacji wywiadowczych w Europie zostały osłabione, Rosjanie umiejętnie dostosowali się do tych uwarunkowań i kontynuowali działalność w oparciu o zasoby wywiadu „nielegalnego", a przede wszystkim na dużą skalę rekrutowali lokalnych pośredników (***proxies***) w charakterze „agentów jednorazowego użytku".

Badania ICCT i Globsec wskazują jednak, że wbrew nazewnictwu w większości przypadków (62%) takie osoby biorą udział w co najmniej dwóch atakach[32]. Ich „jednorazowość" polega na tym, że rosyjskie służby nie podejmują zaawansowanych działań na rzecz zapewnienia im bezpieczeństwa operacyjnego, a w przypadku ich wykrycia i neutralizacji przez kontrwywiad są po prostu zastępowani kolejnymi „jednorazowymi agentami".

Werbunek przebiega głównie za pośrednictwem komunikatora Telegram (w 88% przypadków przenalizowanych przez ICCT i Globsec)[33], a także Viber, Zengi czy Facebook. W tym celu tworzone i wykorzystywane są kanały powiązane z Grupą Wagnera i „batalionami ochotniczymi" (np. Española), chatboty rosyjskiego wywiadu wojskowego GU (d. GRU) –

[31] S. Jones, J.P. Rathbone, R. Milne, *Russia plotting sabotage across Europe, intelligence agencies warn*, „Financial Times", 5 maja 2024 r., www.ft.com.

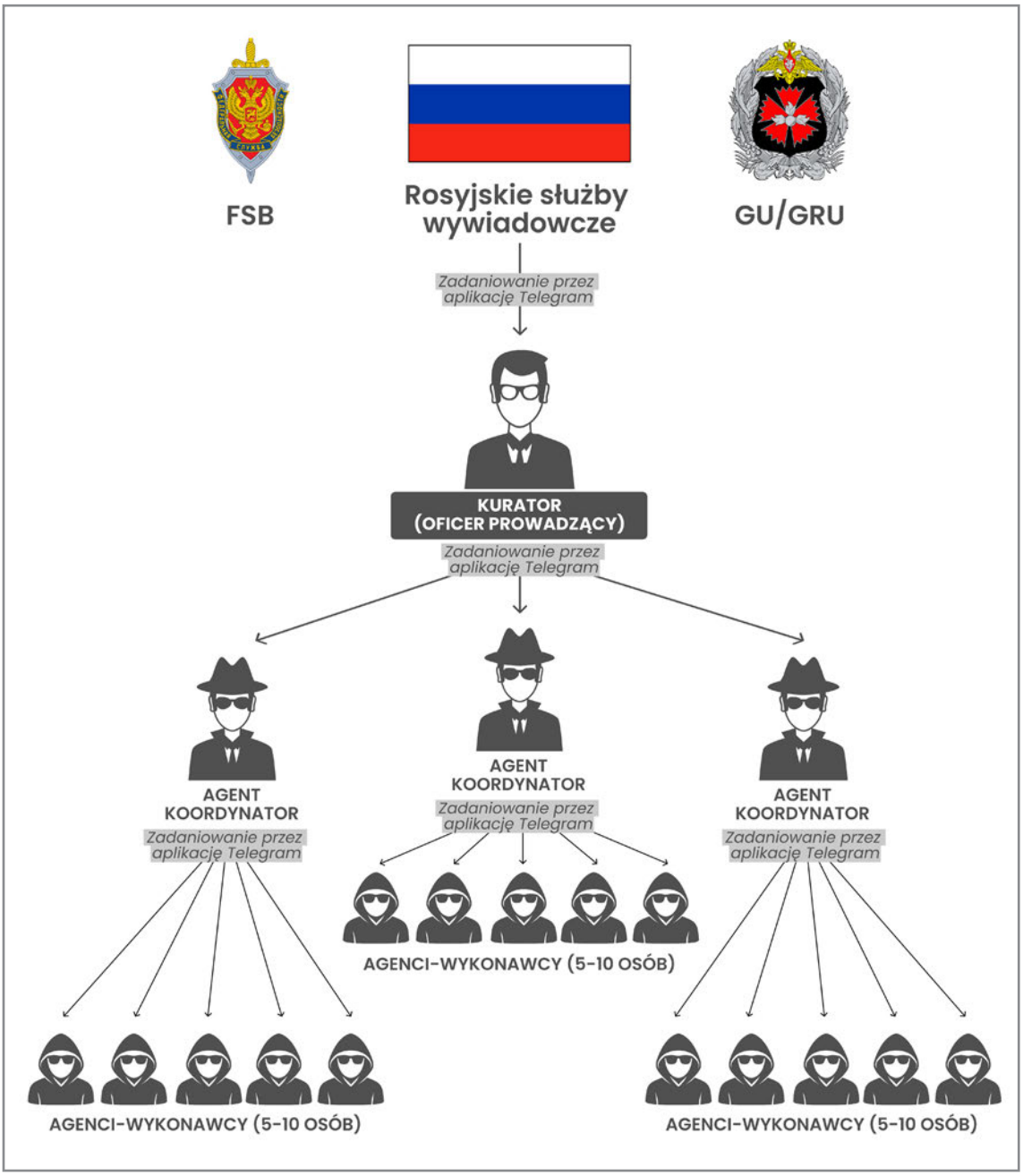
[32] D. Hajdu (red.), *op. cit.*, s. 22.

[33] *Ibidem*, s. 28.

np. Oko Saurona, kanały tzw. Z-bloggerów militarnych (np. Aleksander Kots, Jewgienij Poddubny, Aleksandr Malkiewicz, Jewgienij „TopaZ" Rasskazow, Russkaja wiesna, Dwa majora) czy grupy z ofertami pracy (np. Rabota Polsza, Warszawa objawlenija, Bomba Poland Media)[34]. Zwerbowane osoby działają w hierarchicznych grupach (ok. 90%), na czele których stoi koordynator poszukujący kolejnych współpracowników również poprzez kontakt bezpośredni (44%), m.in. wśród agentów pozyskanych do wcześniejszych zadań (13%)[35].

Schemat 1

Rosyjskie służby wywiadowcze



[34] Д. Беловодьев, *"Ваше сообщение отправлено в ГРУ". Как военная разведка совместно с неонацистом "Топазом" создает телеграм-ботов для вербовки диверсантов*, „Настоящее Время", 25 września 2025 r., www.currenttime.tv.

[35] D. Hajdu (red.), *op. cit.*, s. 28–29.

Według zeznań zatrzymanych osób dominującą motywacją nawiązania współpracy z rosyjskim wywiadem są korzyści finansowe (ok. 96% przypadków), czasami wspierane motywami ideologicznymi (ok. 15% spraw)[36]. Warto przy tym zaznaczyć, że osoby werbowane nie zawsze są świadome współpracy z obcym wywiadem (dotyczy to 58% spraw)[37], co może wynikać m.in. z zawoalowanej formy werbunku stosowanej przez rosyjskie służby specjalne w pierwszych dwóch latach kampanii sabotażowej. Początkowo agenci byli wykorzystywani do wykonywania prostych zadań, takich jak rozdawanie ulotek propagandowych czy malowanie graffiti. Popełniając drobne przestępstwa, demonstrowali gotowość do łamania prawa w zamian za atrakcyjne korzyści finansowe wypłacane przede wszystkim w kryptowalutach. Następnie powierzane były im poważniejsze zadania, takie jak zakup sprzętu do prowadzenia obserwacji lub instalowanie go w pobliżu linii kolejowych, jednostek wojskowych, portów morskich i innych obiektów infrastruktury krytycznej, a także dokonywanie podpaleń i innych aktów sabotażu, za co otrzymywali wynagrodzenia w wysokości ok. 10 tys. euro. Mechanizm ten pozwalał osobie dokonującej werbunku na uwikłanie agenta w mniej lub bardziej świadomą współpracę z rosyjskimi wywiadem, co miało przeciwdziałać ewentualnej gotowości do dekonspiracji i podjęcia współpracy z organami ścigania. Przyjmowane korzyści majątkowe mogły też stanowić podstawę szantażu. Śledztwa dziennikarskie wskazują jednak, że sposób działania rosyjskich rekruterów w 2025 r. zmienił się i jest o wiele bardziej bezpośredni. Poszukują oni przede wszystkim osób mających dostęp do obiektów infrastruktury krytycznej, gotowych do podejmowania się takich zadań jak wywoływanie pożarów lub podkładanie materiałów wybuchowych[38]. Po wykonaniu zadania sprawcy często nie otrzymują jednak obiecanego wynagrodzenia i zostają porzuceni przez oficerów prowadzących, którzy zrywają z nimi łączność[39].

Rosyjską bazę werbunkową stanowią środowiska przestępcze (26% przypadków)[40], kluby sztuk walki, kibice piłkarscy, ochotnicy walczący po stronie Rosji przeciwko Ukrainie, a także prawicowi radykałowie. Władze Litwy odnotowały przy tym zwiększoną liczbę prób werbunku wśród nastolatków[41]. Obiektem werbunku (pod przymusem) są także obywatele państw bałtyckich podróżujący do Rosji i na Białoruś w celach prywatnych (np. rodzinnych, turystycznych)[42]. Według Łotewskiej Służby Bezpieczeństwa

[36] J. Lanchès, K. Rękawek, *op. cit.*

[37] D. Hajdu (red.), *op. cit.*, s. 23–24.

[38] Na podstawie rozmów z dziennikarzami śledczymi z państw bałtyckich.

[39] *Apdraudējuma novērtējums un 2025. gada darbības pārskats*, Militārās izlūkošanas un drošības dienests, saīsināti (MIDD), s. 19–21, www.midd.gov.lv.

[40] J. Lanchès, K. Rękawek, *op. cit.* Szerzej zob. M. Galeotti, *Gangsters at War: Russia's use of organized crime as an instrument of statecraft*, Global Initiative Against Transnational Organized Crime, listopad 2024, https://globalinitiative.net.

[41] *Граждане третьих стран должны будут сообщать о цели визита в Латвию, решила комиссия Сейма*, „Delfi", 23 marca 2025 r., www.delfi.lt.

[42] Por. *National Threat Assessment 2026*, Defence Intelligence and Security Service (AOTD) / State Security Department of the Republic of Lithuania (VSD), Vilnius 2026, s. 27–28, www.kam.lt; *Apdraudējuma…*, *op. cit.*, s. 24–25.

Państwowego (VDD) typowym agentem-sabotażystą jest osoba młoda, z przeszłością kryminalną, borykająca się z problemami finansowymi, o złym statusie społeczno-ekonomicznym, pozbawiona stałego dochodu, o niskim poziomie wykształcenia, niewielkich wartościach moralnych, nadużywająca alkoholu, narkotyków lub środków psychotropowych[43]. W większości przypadków osobami werbowanymi są mężczyźni (93%) w wieku 16–59 lat (średnia 30 lat), pochodzący z państw byłego Związku Radzieckiego (głównie Ukrainy, Białorusi, Rosji i Mołdawii) i mieszkający na terytorium UE, dzięki czemu mają możliwość swobodnego przemieszczania się w strefie Schengen. Nadaje to ich aktywnościom wymiar transgraniczny i umożliwia prowadzenie działań w kilku państwach. Przykładem tego są ataki przeprowadzone przez tych samych sprawców na sklepy IKEA w Wilnie[44] i Rydze (udaremniony), a także sklep OBI i centrum handlowe przy ulicy Marywilskiej 44 w Warszawie[45]. Dzięki międzynarodowej współpracy służb i organów śledczych udało się zatrzymać pięć osób należących do tej grupy, kierowanej przez rosyjski wywiad. Dwie osoby wciąż są poszukiwane na podstawie europejskich nakazów aresztowania oraz listów gończych.

Podobny mechanizm wystąpił w przypadku obywatela Kolumbii, który najpierw podpalił skład budowlany w Radomiu (Polska), a następnie podłożył ogień w zajezdni autobusowej w Pradze, gdzie planował również atak na centrum handlowe. Został zatrzymany w Czechach i skazany na osiem lat pozbawienia wolności. Był on częścią większej grupy dywersyjno-rozpoznawczej pochodzenia latynoamerykańskiego, wykorzystywanej przez rosyjski wywiad, która była zaangażowana także w dwie próby podpalenia obiektów producenta sprzętu wojskowego dla Ukrainy. Władze Litwy rozbiły tę grupę, do której należeli również m.in. obywatel Hiszpanii, osoba mająca podwójne obywatelstwo hiszpańsko-kolumbijskie, Rosjanin i Białorusin, którzy przybyli na Litwę z Hiszpanii, a także obywatel Kuby i pośrednik z Kolumbii mieszkający w Hiszpanii[46].

W latach 2022–2023 działania prowadzone przez rosyjskich „jednorazowych agentów" koncentrowały się przede wszystkim na obserwacji linii kolejowych, portów morskich i lotniczych, baz wojskowych i zakładów przemysłu zbrojeniowego. Ich celem było m.in. rozpoznanie szlaków wykorzystywanych do dostarczania pomocy humanitarnej i wojskowej dla Ukrainy. Aktywność ta była prowadzona przede wszystkim na terytorium Polski, ze względu na jej rolę centrum logistycznego, przez które transportowane jest ok. 80–90% zachodniego wsparcia militarnego dla Ukrainy. W marcu 2023 r. Agencja Bezpieczeństwa Wewnętrznego zidentyfikowała grupę dywersyjno-rozpoznawczą liczącą 30 osób, której działalność była finansowana i koordynowana przez Federalną Służbę Bezpieczeństwa (FSB) Federacji Rosyjskiej. Koordynatorem grupy był Michaił Mirogrodski zwerbowany w tym celu na terytorium Rosji. W wyniku działań operacyjno-śledczych

[43] *Annual Report for 2024*, Latvian State Security Service (VDD), 2025, www.vdd.gov.lv

[44] L. Peter, *Lithuania accuses Russia over Ikea store fire in Vilnius*, „BBC", 17 marca 2025 r., www.bbc.com.

[45] E. Matysiak, *Nie tylko Marywilska i OBI płonęły na rozkaz Kremla. Śledczy ujawniają plan ataku na kolejny sklep*, „Biznes Info, 4 kwietnia 2026 r., www.biznesinfo.pl.

[46] *Baudžiamoji byla dėl teroro išpuolių Šiauliuose perduota teismui*, Lietuvos Respublikos Prokuratura, 16 stycznia 2026 r., www.prokuraturos.lt.

16 członków tej grupy zostało zatrzymanych (w tym 13 Ukraińców, 2 Białorusinów i 1 Rosjanin), a następnie skazanych na karę pozbawienia wolności od 13 miesięcy do 6 lat. Grupa ta planowała także przeprowadzenie ataków na linie kolejowe, czemu udało się zapobiec. Pozostali członkowie i koordynator są poszukiwani listami gończymi.

Rosyjskie działania dywersyjno-sabotażowe obejmują także liczne akty wandalizmu (np. malowanie napisów propagandowych i dezinformacyjnych, niszczenie pomników i obiektów kultury), których głównym celem jest pogłębianie polaryzacji społecznej, formowanie fałszywych oskarżeń, np. wobec władz państw bałtyckich o rzekomą rusofobię i nazyfikację polityki. Pod koniec 2023 r. estońskie służby bezpieczeństwa (KAPO) zatrzymały 13 osób za zbezczeszczenie kilku narodowych miejsc pamięci (zwłaszcza związanych z II wojną światową), natomiast na Łotwie dwóch mężczyzn próbowało podpalić Muzeum Okupacji[47]. W Polsce akty wandalizmu są skierowane przede wszystkim przeciwko miejscom odnoszącym się do trudnej historii relacji polsko-ukraińskich. W 2025 r. zdewastowano pomnik upamiętniający zbrodnię wołyńską w Domostawie, a także pomnik i mogiłę UPA w Monasterzu. Działania te były realizowane przez 17-letniego obywatela Ukrainy na zlecenie rosyjskiego wywiadu, a ich celem było podsycanie napięć etnicznych w Polsce.

Od 2024 r. operacje dywersyjno-sabotażowe inspirowane przez rosyjskie służby specjalne przybierają coraz bardziej ofensywny charakter. Obejmowały one dotychczas m.in. stosowanie przemocy politycznej – pobicia i próby zabójstw. Ich celem było wymuszenie zmiany stanowiska polityków, dziennikarzy śledczych, przedstawicieli opozycji i przemysłu obronnego w sprawie wojny w Ukrainie. W Estonii uszkodzono samochód należący do ministra spraw wewnętrznych Lauriego Läänemetsa, a także auto redaktora naczelnego portalu „Delfi" Andrija Szumakowa. Na Litwie brutalnie pobito Leonida Wołkowa, byłego bliskiego współpracownika Aleksieja Nawalnego. Atak został zorganizowany przez rosyjskiego prawnika Anatolija Blinowa i białoruskiego biznesmena Wiktora Pawełkę – pełnomocnika rosyjsko-izraelskiego miliardera Leonida Niewzlina[48]. Rzeczywistym zleceniodawcą były jednak najprawdopodobniej rosyjskie lub białoruskie służby specjalne. W Polsce Rosja planowała przeprowadzić zamach na prezydenta Ukrainy Wołodymyra Zełenskiego na lotnisku w Rzeszowie-Jasionce, z którego korzysta on podczas większości swoich podróży zagranicznych[49]. W Niemczech przygotowywano zamach na Armina Pappergera – dyrektora generalnego Rheinmetall, największego europejskiego producenta amunicji, który dostarcza pociski artyleryjskie i pojazdy wojskowe do Ukrainy. Działania te zostały jednak wykryte i udaremnione przez amerykańskie i niemieckie agencje wywiadowcze[50].

[47] H. Praks, *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*, „Hybrid CoE Working Paper", nr 32, maj 2024, www.hybridcoe.fi.

[48] *Polish prosecutors say attack on Navalny ally Leonid Volkov was carried out at the behest of exiled billionaire Leonid Nevzlin*, „The Insider", 14 lipca 2025 r., www.theins.press.

[49] I. Vock, *Man arrested in Poland over alleged Russia plot to kill Zelensky*, BBC News, 18 kwietnia 2024 r., www.bbc.com.

[50] K.B. Lillis, N. Bertrand, F. Pleitgen, *US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine*, CNN Politics, 11 lipca 2024 r., www.edition.cnn.com.

Kolejnym etapem eskalacji rosyjskiej kampanii dywersyjno-sabotażowej była fala pożarów. Dywersanci atakowali przede wszystkim tzw. miękkie cele (m.in. sklepy wielkopowierzchniowe, magazyny budowlane, samochody z ukraińskimi tablicami rejestracyjnymi czy restauracje solidaryzujące się z Ukrainą). Zdarzenia te były wykorzystywane przez rosyjskie kanały dezinformacji i propagandy. Prezentowano nagrania płonących sklepów budowlanych, które opisywano jako zachodnie zakłady zbrojeniowe, w których zniszczone zostało uzbrojenie i sprzęt wojskowy przeznaczone dla Ukrainy.

W październiku 2025 r. łotewska VDD zatrzymała cztery osoby, które prowadziły akcje sabotażowe wymierzone w infrastrukturę obronną i krytyczną Łotwy. Jesienią 2025 r. osoby te podpaliły obiekt należący do prywatnej firmy realizującej projekty związane z obronnością, a w 2024 r. usiłowały podpalić ciężarówkę z ukraińskimi tablicami rejestracyjnymi, znajdującą się w jednym z obiektów infrastruktury krytycznej. Łotewskie władze znalazły dowody na to, że grupa dokładnie zbadała lokalizację i protokoły bezpieczeństwa, sporządziła mapy wejść i wyjść. Podejrzani fotografowali i filmowali również inne wrażliwe obiekty, a następnie przekazywali te informacje rosyjskim służbom wywiadowczym, prawdopodobnie w celu przygotowania przyszłych ataków[51].

Oprócz strat materialnych, takich jak spowodowane przez pożary wywołane na zlecenie rosyjskiego wywiadu (np. w wyniku pożaru centrum handlowego przy ul. Marywilskiej 44 w Warszawie zniszczonych zostało ok. 1400 sklepów i punktów usługowych, zob. załącznik), niektóre z planowanych przez Rosję ataków mogły mieć poważne konsekwencje dla życia i zdrowia ludności. W styczniu 2024 r. ABW zatrzymała obywatela Ukrainy, który na zlecenie rosyjskiego wywiadu przygotowywał atak na fabrykę farb należącą amerykańskiego przedsiębiorstwa PPG Industries. Cel był zlokalizowany w pobliżu infrastruktury strategicznej (bazy paliw) oraz rzeki Odry, co mogło doprowadzić do poważnego skażenia środowiska. Za wykonanie zlecenia Serhij S. (51 lat) miał otrzymać 4 tys. dol. Ustalenia w tej sprawie umożliwiły nie tylko udaremnienie tego ataku, ale także wykrycie kolejnej zorganizowanej grupy przestępczej zajmującej się działalnością dywersyjną (podpalenia magazynów, fabryk i restauracji) na rzecz rosyjskiego wywiadu.

W kwietniu 2024 r. w Niemczech zatrzymano dwie osoby pochodzenia rosyjskiego, którym postawiono zarzuty działania na zlecenie rosyjskiego wywiadu i zamiar przeprowadzenia ataków na obiekty wojskowe, fabryki broni, obiekty przemysłowe oraz infrastrukturę transportową wykorzystywaną do zaopatrzenia Ukrainy. Działania te miały przybrać formę podpaleń i detonacji materiałów wybuchowych, a jednym z planowanych celów były instalacje sił zbrojnych USA w Grafenwöhr w Bawarii, gdzie ukraińscy żołnierze byli szkoleni w zakresie obsługi czołgów M1 Abrams[52]. W konsekwencji w amerykańskich bazach wojskowych w Europie podniesiono wówczas poziom alarmowy do

[51] *Annual Report for 2025*, Latvian State Security Service (VDD), 2026, s. 8, www.vdd.gov.lv.

[52] N. Bertrand, *Intelligence on Russian sabotage threat prompted increase in security at US military bases in Europe*, CNN Politics, 9 lipca 2024 r., https://edition.cnn.com.

poziomu CHARLIE[53], co oznaczało, że doszło do incydentu lub pojawiły się dane wywiadowcze wskazujące na prawdopodobieństwo ataków na obiekty i personel.

W 2024 r. w Niemczech miało miejsce również kilka aktów sabotażu wymierzonych w okręty wojenne. Uszkodzono trałowiec w stoczni w Wilhelmshaven, a w Hamburgu do silnika nowo budowanej korwety Emden wrzucono ok. 30 kg metalowych opiłków. Wykrycie tej ingerencji zapobiegło potencjalnemu unieruchomieniu statku i znacznemu opóźnieniu w przekazaniu go niemieckiej marynarce wojennej. W związku z tą sprawą aresztowano obywateli Rumunii i Grecji, ale dotychczas niemieckiej prokuraturze nie udało się wykazać ich związków z rosyjskim wywiadem. W 2025 r. w Erfurcie, w środkowych Niemczech, podpalono sześć pojazdów wojskowych marki Rheinmetall MAN z oznaczeniami Bundeswehry i NATO, które znajdowały się na terenie warsztatu samochodowego[54].

Od 2024 r. rosyjskie służby specjalnie nasiliły działania, których celem było tworzenie międzynarodowych kanałów przerzutu materiałów wykorzystywanych do działalności dywersyjno-sabotażowej (m.in. materiałów wybuchowych, części do dronów wykorzystywanych do rozpoznawania infrastruktury krytycznej czy kart SIM). W lipcu 2024 r. w Katowicach zatrzymano dwoje rosyjskich opozycjonistów zaangażowanych w obrót materiałami wybuchowymi na zlecenie FSB. W październiku ABW zatrzymała cztery osoby biorące udział w operacji rozpoznania kanałów przerzutu materiałów wybuchowych drogą lotniczą do USA i Kanady. W ramach testowej fazy operacji w paczkach z masażerami erotycznymi, która miała zostać nadana z Warszawy, umieszczono łatwopalną substancję. Operację zdekonspirowały przedwczesne zapłony, które miały miejsce w centrum logistycznym DHL w Lipsku w Niemczech i Birmingham w Wielkiej Brytanii[55].

Punktem początkowym przerzutu materiałów łatwopalnych i wybuchowych, a także części do dronów oraz kart SIM, była Litwa, skąd grupa dywersyjna działająca na zlecenie GU transportowała je w puszkach po kukurydzy, a następnie chowała w tzw. martwych skrzynkach kontaktowych (m.in. na cmentarzach)[56]. W związku z tą sprawą zatrzymano 15 osób (pochodzących m.in. z Rosji, Litwy, Łotwy, Estonii i Ukrainy) i zabezpieczono 6 kg trotylu, który miał zostać wykorzystany do kolejnych ataków. Nadzór nad operacją sprawował Aleksandr Bezrukawyj – 44-letni obywateli Rosji, który został za-

[53] CHARLIE to trzeci poziom alarmowy w czterostopniowej skali, który wskazuje na wysokie ryzyko ataków terrorystycznych. Status ten wiąże się z wprowadzeniem rygorystycznych środków bezpieczeństwa, w tym wzmożonych kontroli bezpieczeństwa przy wejściach do baz, zwiększonej obecności personelu ochrony, ograniczeń dostępu i przemieszczania się w obrębie obiektów wojskowych, wzmożonego nadzoru i patroli na obrzeżach.

[54] M. Bewarder, J. Diehl, F. Flade, *BKA zählt mehr als 320 Sabotage-Verdachtsfälle*, „Tagesschau", 5 lutego 2026 r., www.tagesschau.de.

[55] W. Wallis, J.P., Rathbone, O. Telling, *UK counterterror police probe whether Russia planted parcel bomb*, „Financial Times", 15 października 2024 r., www.ft.com.

[56] Szerzej zob. M. Weiss, K. Kopaleishvili, ***Revealed: How Russia's GRU Plotted Europe's Parcel Explosions***, „VSquare", 17 września 2025 r., www.vsquare.org.

trzymany przez służby bezpieczeństwa Bośni i Hercegowiny (SIPA), a następnie deportowany do Polski. Do zatrzymania na Bałkanach doszło w związku z jego rolą w organizowaniu szkoleń paramilitarnych dla mołdawskich grup dywersyjnych, które miały destabilizować sytuację w trakcie wyborów w Mołdawii w 2024 r.

W październiku 2025 r. dzięki współpracy ABW z rumuńską służbą bezpieczeństwa (SRI) udało się zapobiec kolejnemu transportowi materiałów wybuchowych, które miały zostać wykorzystane do działań dywersyjno-sabotażowych. Plan obejmował wysłanie dwóch paczek z materiałami zapalającymi za pośrednictwem ukraińskiej firmy kurierskiej Nova Post, która obsługuje połączenia między państwami UE a Ukrainą. Urządzenia miały służyć do podpalenia i zniszczenia budynku tej firmy w centrum Bukaresztu[57].

W sierpniu 2024 r. Niemcy padły ofiarą ataków na infrastrukturę wojskową i transportową, w tym sabotażu sieci wodociągowej w pobliżu niemieckiej bazy wojskowej niedaleko lotniska w Kolonii. W marcu 2025 r. szwedzka policja wszczęła dochodzenie w sprawie podejrzenia sabotażu, gdy uszkodzono kable energetyczne podłączone do systemu pomp na wyspie Gotlandia. W lipcu 2025 r. w Polsce aresztowano obywatela Ukrainy Ihora H. (36 lat) za przygotowywanie ataku na system zaopatrzenia w wodę, który miał na celu sparaliżowanie dystrybucji wody w Sopocie. Incydenty te wskazują, że celem potencjalnej eskalacji działań inicjowanych przez rosyjski wywiad mogą być usługi istotne dla ludności, takie jak dostawy wody czy energii elektrycznej.

W 2025 r. niemiecki Federalny Urząd Policji Kryminalnej odnotował aż 321 incydentów o charakterze sabotażu, które były skierowane głównie wobec sektora energetycznego, linii kolejowych i obiektów wojskowych, a także 1289 zgłoszeń dotyczących nieautoryzowanych przelotów dronów nad obiektami infrastruktury o znaczeniu strategicznym[58].

O gotowości Rosji do eskalacji działań ofensywnych świadczy zamach terrorystyczny na linie kolejowe w Polsce. W dniach 15–17 listopada 2025 r. doszło do dwóch poważnych incydentów na odcinku Warszawa–Lublin, których celem było wykolejenie pociągów. Trasa ta ma duże znaczenie dla transportu pasażerskiego, towarowego i wojskowego. W miejscowości Mika zdetonowano na torach materiał wybuchowy C4. Ze względu na to, że jeden z podłożonych ładunków nie eksplodował, sprawcom nie udało się wystarczająco uszkodzić szyny i wykoleić pociągu towarowego. W pobliżu miejscowości Gołąb uszkodzono natomiast sieć trakcyjną i umieszczono na szynie dwa specjalnie skonstruowane metalowe elementy, które miały doprowadzić do wykolejenia pociągu. Elementy te zostały wykryte i zneutralizowane. Oba incydenty, będące przejawem działalności dywersyjno-terrorystycznej realizowanej na zlecenie Rosji, groziły poważną katastrofą w ruchu lądowym. Zidentyfikowano sprawców – obywateli Ukrainy Jewhenija Iwanowa i Ołeksandra Kononowa, którzy wjechali do Polski, posługując się fałszywymi dokumentami, a po zdarzeniu uciekli na Białoruś. Pierwszy z nich w maju

[57] J. Lanchès, K. Rękawek, *op. cit*.

[58] M. Bewarder, J. Diehl, F. Flade, *op. cit.*

2024 r. został w Ukrainie skazany zaocznie na 15 lat więzienia za zorganizowanie dywersji na fabrykę produkującą drony we Lwowie.

Zamach dywersyjno-terrorystyczny na kolei został skoordynowany z akcją dezinformacyjną, która miała udowodnić, że była to operacja pod fałszywą flagą przeprowadzona przez Ukrainę i polskie władze. Taką narrację rosyjska Służba Wywiadu Zagranicznego (SWR) wprowadziła już pod koniec września 2025 r. w komunikacie prasowym. Sugerowano w nim, że ukraińskie i polskie służby specjalne zamierzają wykorzystać rosyjskich i białoruskich ochotników walczących po stronie Ukrainy do przeprowadzenia ataku, a następnie obarczyć winą Rosję i Białoruś, by wciągnąć NATO do wojny. Według danych Res Futura Data House[59] aż 42% z 14 tys. przeanalizowanych komentarzy dotyczących tego incydentu wskazywało na winę Ukrainy, a 19% – polskiego rządu. Badanie to oczywiście nie odzwierciedla rzeczywistej percepcji zdarzenia w polskim społeczeństwie, a jedynie pokazuje poziom intoksykacji infosfery w wyniku działań rosyjskiego aparatu dezinformacji i propagandy (w tym farm trolli i botów).

W odpowiedzi na zamach na linie kolejowe w Polsce uruchomiono operację „Horyzont", do której zaangażowano 10 tys. żołnierzy z zadaniem monitorowania infrastruktury kolejowej. Wcześniej w Polsce miały miejsce zakłócenia funkcjonowania pociągów sygnałami radiowymi. Dochodziło również (m.in. w Polsce i Niemczech) do incydentów polegających na odłączeniu pojedynczych wagonów towarowych i wymuszonym zatrzymaniu pociągów przewożących materiały niebezpieczne. We wrześniu 2025 r. miały miejsce zakłócenia funkcjonowania dwóch kluczowych linii kolejowych w Niemczech – między Hamburgiem a Berlinem oraz między Kolonią a Düsseldorfem. W pierwszym przypadku zdetonowano ładunek wybuchowy w tunelu, w drugim przecięto przewody elektryczne. W styczniu 2026 r. w Essen doszło do wykolejenia pociągu towarowego załadowanego chlorem, formaldehydem i nitrobenzenem. Do torów przymocowano metalowe zaciski podobne do tych, które zostały użyte w Polsce. W dniu zdarzenia trasę tę miał pokonać pociąg transportujący amunicję i sprzęt dla stacjonujących w Europie wojsk amerykańskich. Również władze Szwecji prowadzą dochodzenie w sprawie dwóch wypadków (z grudnia 2023 i lutego 2024 r.) związanych z wykolejeniem pociągów na linii Malmbanan oraz serią uszkodzeń kabli kolejowych i podziemnych, które miały miejsce w zachodniej części kraju od początku 2025 r.

[59] Res Futura zrzesza ekspertów zajmujących się analizą przestrzeni informacyjnej oraz zagadnieniami związanymi z bezpieczeństwem państwowym, zob. https://resfutura.pl/res-futura-o-nas/.

Rosyjskie ataki dywersyjno-sabotażowe w państwach RPMB
24 lutego 2022 – 30 kwietnia 2026

Źródło: opracowanie własne.

Domena powietrzna

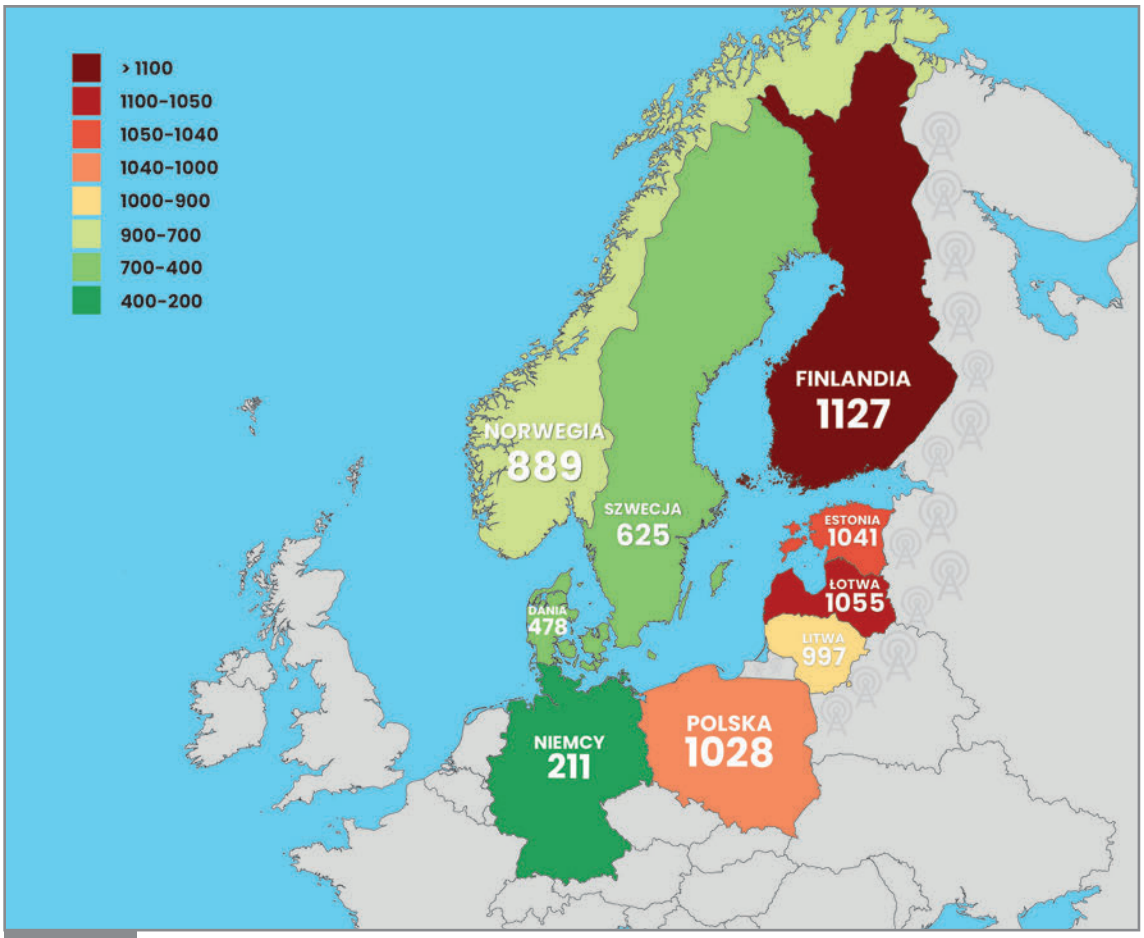
Do najważniejszych działań hybrydowych prowadzonych przez Rosję przeciwko członkom RPMB w tej domenie należą zakłócenia sygnału GNSS oraz naruszenia przestrzeni powietrznej przez rosyjskie i białoruskie samoloty, myśliwce i systemy bezzałogowe, co powoduje konieczność poderwania myśliwców dyżurnych. Zakłócenia sygnału GNSS trwają nieprzerwanie od rozpoczęcia przez Rosję pełnoskalowej agresji na Ukrainę, a znacząco nasiliły się w drugiej połowie 2024 r., co koresponduje z przeprowadzaniem przez rosyjskie służby coraz bardziej ofensywnych operacji w domenie lądowej. Natomiast do naruszeń przestrzeni powietrznej przez samoloty i śmigłowce dochodziło incydentalnie, choć od drugiej połowy 2025 r. można obserwować nasilenie działań związanych z wykorzystaniem w tym celu systemów bezzałogowych oraz balonów meteorologicznych i przemytniczych.

Zakłócenia sygnału GNSS

Od początku pełnoskalowej rosyjskiej agresji na Ukrainę można zaobserwować codzienne zakłócenia sygnału GNSS. W latach 2022–2024 koncentrowały się one głównie w państwach wschodniego Bałtyku, Finlandii, Estonii (zwłaszcza w Zatoce Fińskiej), Łotwie, Litwie i Polsce. Zakłócenia często występowały także na północy Norwegii. Od drugiej połowy 2024 r. przyjęły one szerszy wymiar i objęły także Szwecję, Danię, a okresowo również Niemcy. Dane serwisu gpsjam.org, który monitorował zakłócenia sygnału GNSS od lutego 2022 r., wskazują, że od 1 marca 2022 r. do 31 marca 2026 r. dni z problemami (od niewielkich po obejmujące znaczne terytorium poszczególnych państw) było: w Polsce – 1028, na Litwie – 997, Łotwie – 1055, w Estonii – 1041, Finlandii – 1127, Szwecji – 625, Norwegii – 889, Danii – 478, a w Niemczech – 211. Udowadnia to, że dla Rosji naruszanie bezpieczeństwa żeglugi powietrznej oraz morskiej było ważnym elementem oddziaływania na państwa regionu Morza Bałtyckiego.

W 2022 r. zakłócenia sygnału GNSS pojawiały się falami, często obejmując Polskę, Litwę, Łotwę, Estonię, Finlandię i Norwegię. Ich zasięg był zmienny – od pojedynczych państw po 6–7 lokalizacji jednocześnie. Stale występowały one w Zatoce Fińskiej, a w 2023 r. zakłócenia sygnału GNSS w państwach nadbałtyckich i Norwegii stały się codziennością. Coraz częściej obejmowały wszystkie państwa nadbałtyckie jednocześnie. Pod koniec 2023 oraz w całym 2024 r. niemal codziennie występowały zakłócenia we wszystkich państwach regionu. Przez wiele dni miały one miejsce jednocześnie, zarówno na terenie tych państw, jak i na rozległych obszarach Bałtyku. Zjawiska te nasiliły się w 2025 r. i coraz częściej obejmowały znaczne obszary regionu Morza Bałtyckiego. Podobnie było w pierwszym kwartale 2026 r., kiedy zakłócenia obejmowały Polskę, państwa bałtyckie, Finlandię, Norwegię, Szwecję, Danię, Niemcy i Morze Bałtyckie.

Liczba dni z zakłóceniami sygnału GNSS



Źródło: opracowanie własne na podst. danych serwisu gpsjam.org.

Źródła zakłóceń sygnału GNSS zlokalizowane były głównie w obwodach królewieckim oraz leningradzkim. Negatywnie oddziaływały one nie tylko na ruch lotniczy, ale także na bezpieczeństwo cywilnej żeglugi morskiej. Stale odnotowywano przypadki zakłóceń sygnału GPS na polskich jednostkach pływających, jak również przekłamań wskazań w systemie AIS[60], co stanowiło zagrożenie dla bezpieczeństwa żeglugi morskiej. Od lutego 2022 r. takich incydentów odnotowano blisko 100, niemniej prawdziwa ich liczba jest trudna do określenia, ponieważ nie wszystkie jednostki zgłaszają problemy z odbiornikami GPS, tylko od razu przechodzą na nawigację analogową (korzystają z map). Po zidentyfikowaniu zagrożenia Fińska Agencja Transportu i Łączności (Traficom) zaapelowała do marynarzy o ograniczenie polegania na systemach satelitarnych i wykorzystywanie podczas pracy tradycyjnych metod nawigacyjnych[61].

[60] System AIS obejmuje m.in. takie dane jak pozycja statku, jego kurs i prędkość, co ma celu np. uniknięcie kolizji w żegludze morskiej.

[61] *Finland and Estonia warn vessels in the Gulf of Finland of an increase in GNSS disruptions*, Transport and Communications Agency, 13 czerwca 2025 r., www.traficom.fi.

Do najważniejszych incydentów związanych z zakłóceniami sygnału GNSS doszło m.in. w Norwegii. W czerwcu 2025 r. w regionie wschodniego Finnmarku zidentyfikowano manipulacje sygnałami GPS na wysokościach do 150 m nad ziemią. Pomiar wykazał, że źródło zakłóceń znajdowało się po stronie rosyjskiej. We wrześniu 2025 r. samolot należący do linii Widerøe musiał przerwać lądowanie w Vardø z powodu utraty sygnału GPS[62]. Norweski urząd komunikacji (Nkom) przyznał, że w północnych regionach jest bardzo wiele zakłóceń, i powołał lokalne biuro w Tromsø, aby szybciej reagować na tego typu incydenty. Norweskie władze przyznają, że zakłócenia są codziennym problemem i zalecają korzystanie z mapy i kompasu jako zabezpieczenia.

Na początku 2025 r. zakłócenia sygnału GPS dotknęły m.in. szwedzkie wyspy Gotlandię i Olandię. Minister obrony Szwecji Pål Jonson zapewnił, że rząd uważnie monitoruje sytuację i utrzymuje ścisły dialog zarówno z Finlandią, jak i państwami bałtyckimi, a także w ramach NATO i UE. Jonson poinformował również, że Szwedzkie Siły Zbrojne (Försvarsmakten) rozważają podjęcie środków w celu wzmocnienia odporności i solidności oraz zmniejszenia podatności na zakłócenia nawigacji satelitarnej GNSS. Jako główne źródło zakłóceń Szwecja również wskazuje obwód królewiecki[63]. W lipcu 2025 r. Szwedzki Urząd Morski (Sjöfartsverket) wydał pilne ostrzeżenie w związku ze znacznym nasileniem zakłóceń w działaniu GPS i systemu AIS na Morzu Bałtyckim, w tym u zachodnich wybrzeży Szwecji[64]. Urząd Morski zalecił marynarzom zachowanie czujności i stosowanie alternatywnych metod nawigacji, takich jak tradycyjne mapy i namiar wizualny w celu ograniczenia ryzyka związanego z niewiarygodnymi danymi GPS i AIS.

W odpowiedzi na zakłócenia sygnału GNSS Finlandia wraz z 13 innymi państwami europejskimi, w tym krajami bałtyckimi i Niemcami[65], poinformowała Międzynarodową Organizację Morską (IMO) o zakłóceniach w działaniu systemu GNSS oraz manipulacjach w morskim systemie AIS. Finlandia uznała je za zagrożenie dla bezpieczeństwa, a wspólnie z Estonią wydała także ostrzeżenia nawigacyjne dotyczące Zatoki Fińskiej oraz zaktualizowała komunikaty dla żeglarzy. Poinformowała statki o zakłóceniach w działaniu systemu GNSS i zaleciła im stosowanie alternatywnych metod pozycjonowania[66].

W związku z zagrożeniem związanym z zakłóceniami litewska Oro Navigacija (podmiot świadczący usługi żeglugi powietrznej) oraz armia wprowadziły dodatkowe zalecenia dla pilotów i operatorów dronów. Nakazały im korzystanie z tradycyjnych metod

[62] *GPS jamming prevented plane from landing*, „Newsinenglish.no", 16 września 2025 r., www.newsinenglish.no.

[63] A. Walsh, *Sweden accuses Russia of GPS jamming over Baltic Sea*, BBC, 4 września 2025 r., www.bbc.com.

[64] *Warning of GPS interference in the Baltic Sea*, Emergency information from Swedish authorities, 20 czerwca 2025 r., www.krisinformation.se.

[65] *Coastal States of the Baltic Sea and the North Sea: Safety risks in navigation increased by GNSS interference*, Ministry of Transport and Communications, Finnish Government, 26 stycznia 2026 r., https://valtioneuvosto.fi.

[66] *A report recently published by the Finnish Geospatial Research Institute recommends new measures to protect against interference*, „Space Finland", 18 lutego 2026 r., https://spacefinland.fi.

nawigacji (radary, mapy papierowe, radionawigacja naziemna) w przypadku utraty sygnału GPS. Łotewski Urząd ds. Łączności Elektronicznej podjął natomiast współpracę z partnerami zagranicznymi w celu zwiększenia możliwości wykrywania i analizowania zakłóceń w systemach GNSS.

W 2024 r. Polska ogłosiła, że Państwowy Instytut Badawczy oraz Główny Urząd Geodezji i Kartografii rozpoczęły projekt „System Monitorowania Sygnałów GNSS w Polsce w Czasie Rzeczywistym (RTGMS)", finansowany przez Europejską Agencję Kosmiczną. System RTGMS ma wykrywać zakłócenia sygnałów GNSS, takie jak problemy z dostępem lub błędy w działaniu nawigacji satelitarnej[67]. System będzie też wysyłać ostrzeżenia i pokazywać wyniki pomiarów na stronie internetowej dostępnej dla wszystkich użytkowników.

W 2025 r. Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) oraz Międzynarodowe Stowarzyszenie Transportu Lotniczego (IATA) opublikowały ponadto kompleksowy plan, którego celem było ograniczenie ryzyka wynikającego z zakłóceń w globalnym systemie nawigacji satelitarnej[68]. Plan obejmuje m.in. uzgadnianie standardowych komunikatów radiowych dotyczących zgłaszania zakłóceń GNSS oraz ujednolicone kodowanie komunikatów, zapewnienie szybkiego i niezawodnego przywracania działania sprzętu GPS po utracie sygnału lub zakłóceniu, utrzymanie zapasowego systemu GNSS, lepsze wykorzystanie wojskowych zdolności zarządzania ruchem lotniczym, poprawę koordynacji cywilno-wojskowej, udoskonalenia procedur planowania awaryjnego i rezerwowego w przestrzeni powietrznej, tak aby statki powietrzne mogły bezpiecznie nawigować nawet w przypadku wystąpienia zakłóceń.

Naruszenia przestrzeni powietrznej

Od początku pełnoskalowej agresji na Ukrainę Rosja sprowokowała szereg incydentów związanych z naruszeniem przestrzeni powietrznej członków RPMB. W regionie dochodziło też do innych zdarzeń, takich jak przeloty w pobliżu granic, wymuszające na państwach RPMB reakcję w postaci podrywania myśliwców dyżurnych. Odnotowano także liczne przypadki wykorzystywania przez Rosję i Białoruś bezzałogowych statków powietrznych, które naruszały granice państw RPMB, co zmuszało atakowane państwa do podejmowania działań mających na celu ich zwalczanie.

W przypadku Polski wśród wszystkich zidentyfikowanych naruszeń należy wyróżnić incydenty z udziałem samolotów i śmigłowców, bezzałogowych systemów powietrznych, aerostatów oraz środków rażenia. Jako intencjonalne zostało jednak zakwalifikowane tylko jedno zdarzenie – z 25 kwietnia 2025 r., polegające na trzykrotnym naruszeniu granicy przez rosyjski śmigłowiec Ka-27. W Polsce charakterystyczne były

[67] *W Polsce powstanie system monitorowania sygnałów GNSS*, Ministerstwo Cyfryzacji, 13 listopada 2024 r., www.gov.pl/web/cyfryzacja.

[68] *EASA and IATA outline comprehensive plan to mitigate GNSS interference risks*, European Union Aviation Safety Agency, 18 czerwca 2025 r., www.easa.europa.eu.

natomiast incydenty związane z upadkiem na jej terytorium środków rażenia, do czego doszło 15 listopada oraz 16 grudnia 2022 r. W obszarze Bałtyku Południowego i Południowo-Wschodniego miały też miejsce prowokacje w postaci ryzykownych manewrów rosyjskich pilotów w pobliżu polskich jednostek pływających oraz morskiej infrastruktury krytycznej, np. przeloty rosyjskich myśliwców w rejonie polskich platform wiertniczych. Manewry te były ukierunkowane głównie na zaakcentowanie obecności i demonstrację siły.

Za największą liczbę naruszeń przestrzeni powietrznej Polski odpowiadają jednak głównie bezzałogowe systemy powietrzne, spośród których zdecydowana większość to tzw. cywilne drony przemytnicze. Za najbardziej niebezpieczne zdarzenie w domenie powietrznej można natomiast uznać użycie przez Rosję przeciw Polsce bezzałogowych systemów powietrznych w nocy z 9 na 10 września 2025 r. Warto podkreślić, że zdarzeniu towarzyszyła zmasowana operacja informacyjna[69], której celem było udowodnienie, że były to drony ukraińskie. W reakcji na incydent Polska zwołała spotkania Rady Północnoatlantyckiej zgodnie z art. 4 Traktatu północnoatlantyckiego. W wyniku tego incydentu NATO 12 września 2025 r. zdecydowało o uruchomieniu operacji „Wschodnia straż" („Eastern Sentry").

Od 2025 r. obserwowano także czasowe masowe wloty z terytorium Białorusi balonów przemytniczych zawierających papierosy. Choć nie stanowiły zagrożenia dla bezpieczeństwa państwa, według Dowództwa Operacyjnego Rodzajów Sił Zbrojnych miały także na celu testowanie polskiego sytemu obrony powietrznej. W nocy z 24 na 25 grudnia 2025 r. oraz w nocy z 16 na 17 stycznia 2026 r. z terenu Białorusi na terytorium Polski wleciało po kilkadziesiąt balonów meteorologicznych przenoszących przemycane wyroby tytoniowe[70]. Taka ilość towaru i takie nakłady finansowe wskazują jednoznacznie, że były to działania pozoracyjne, odwracające uwagę od rzeczywistego celu sprawców, którym jest paraliż ruchu powietrznego i polskich lotnisk. W związku z tymi zagrożeniami Wojsko Polskie podjęło szereg działań mających na celu lepsze skalibrowanie systemów obrony powietrznej chroniących polską granicę oraz rozmieściło w jej pobliżu systemy walki radioelektronicznej.

[69] F. Bryjka, A. Wójtowicz, *Rosyjska dezinformacja w sprawie ataku dronów na Polskę*, „Biuletyn PISM", nr 99 (3102), 19 września 2025 r., www.pism.pl.

[70] A.M. Dyner, *Białoruś coraz częściej wykorzystuje balony przeciw Polsce*, „Depesza PISM", 6 lutego 2026 r., www.pism.pl.

Tabela 3

Zidentyfikowane naruszenia polskiej przestrzeni powietrznej w latach 2022–2026

ROK	NARUSZENIA POLSKIEJ PRZESTRZENI POWIETRZNEJ	ZAŁOGOWE STATKI POWIETRZNE	DRONY	BALONY	ŚRODKI RAŻENIA	NIEZIDENTYFIKOWANE OBIEKTY POWIETRZNE
2022	477	0	471	0	2	4
2023	252	1	223	2	1	24
2024	290	2	279	2	1	6
2025	392	5	292	64	0	31
2026 (do marca)	308	0	32	274	0	2

Źródło: dane Dowództwa Operacyjnego Rodzajów Sił Zbrojnych.

Jednym z najczęściej atakowanych państw była też Litwa, gdzie jednak nasilenie incydentów naruszeń przestrzeni powietrznej i aktów sabotażu miało miejsce głównie w 2025 r. Wcześniej balony przemytnicze z paczkami papierosów pojawiały się incydentalnie. Ich masowy i systematyczny napływ od października 2025 r. został uznany przez władze Litwy za poważne zagrożenie dla lotnictwa cywilnego i bezpieczeństwa. Jednocześnie w grudniu 2025 r. litewskie władze zaklasyfikowały ataki z użyciem balonów nie jako hybrydowe, ale terrorystyczne, stanowiące nie tylko naruszenie granicy, ale stwarzające też zagrożenie dla lotnictwa cywilnego i życia pasażerów samolotów. W związku z szeregiem takich incydentów rząd Litwy wprowadził stan zagrożenia w pasie przy granicy z Białorusią i na lotnisku w Wilnie[71]. W 2025 r. doszło też do innych incydentów związanych z naruszeniem litewskiej przestrzeni powietrznej. 23 października dwa rosyjskie samoloty wojskowe z terenu obwodu królewieckiego na krótko naruszyły litewską przestrzeń powietrzną w pobliżu miasta Kibarty. Za incydent był odpowiedzialny myśliwiec Su-30, który prawdopodobnie przeprowadzał ćwiczenia tankowania w powietrzu, i latająca cysterna Ił-78, które wleciały ok. 700 m w głąb terytorium Litwy (znajdowały się w jej przestrzeni powietrznej ok. 18 sekund). W odpowiedzi poderwano dwa hiszpańskie myśliwce realizujące misję Baltic Air Policing NATO. Według Ministerstwa Obrony Rosji myśliwce Su-30 przeprowadziły „lot szkoleniowy" nad obwodem królewieckim i nie naruszyły granic żadnego państwa[72].

[71] A.M. Dyner, *Litwa wprowadza stan nadzwyczajny ze względu na działania Białorusi*, „Komentarz PISM", nr 83/2025, 10 grudnia 2025 r., www.pism.pl.

[72] A. Sytas, *NATO member Lithuania says two Russian jets briefly entered its airspace*, Reuters, 23 października 2025 r., www.reuters.com.

Najmniej incydentów związanych z naruszeniem przestrzeni powietrznej w latach 2022–2026 odnotowano na Łotwie, a do najpoważniejszego doszło we wrześniu 2024 r., kiedy rozbił się rosyjski dron typu Szahed[73].

Do poważnego naruszenia przestrzeni powietrznej Estonii doszło natomiast 19 września 2025 r. Państwo to zdecydowało się na zwołanie spotkania Rady Północnoatlantyckiej zgodnie z art. 4 Traktatu północnoatlantyckiego[74]. Naczelny dowódca sojuszniczy w Europie (SACEUR) poinformował, że incydent, w którym trzy uzbrojone rosyjskie samoloty typu MiG-31 naruszyły estońską przestrzeń powietrzną, trwał ponad dziesięć minut.

W Finlandii natomiast sporadycznie obserwowano działania niezidentyfikowanych dronów. 27 września 2025 r. zauważono dron przelatujący nad elektrownią Valajaskoski w Rovaniemi, mimo że obszar ten od sierpnia był objęty strefą zakazu lotów dronów. Przypadkowy świadek powiadomił o zdarzeniu policję, jednak operator drona nie został uchwycony przez monitoring elektrowni i opuścił teren przed przybyciem funkcjonariuszy. Firma Kemijoki Oy, która zarządza elektrownią, potwierdziła incydent i poinformowała, że doniesienia o dronach pojawiają się sporadycznie. Na przełomie marca i kwietnia 2026 r. w Finlandii, na Litwie, Łotwie i w Estonii odnotowano także upadki ukraińskich dronów, które były skierowane na nadbałtyckie porty rosyjskie. Zmiana trajektorii ich lotu była spowodowana zakłóceniami sygnału GNSS, których źródło było w Federacji Rosyjskiej[75].

W okresie 2022–2026 doszło również do naruszeń przestrzeni powietrznej Szwecji. W marcu 2022 r., krótko po rozpoczęciu inwazji na Ukrainę, cztery rosyjskie samoloty bojowe – dwa Su-27 i dwa Su-24 – naruszyły szwedzką przestrzeń powietrzną w pobliżu Gotlandii. W marcu 2022 r. miało miejsce naruszenie szwedzkiej przestrzeni powietrznej przez w sumie cztery rosyjskie samoloty Su-24 i Su-27. Doszło do tego nad Morzem Bałtyckim na wschód od Gotlandii[76]. Z kolei w kwietniu 2022 r. doszło do naruszenia szwedzkiej przestrzeni powietrznej na południe od Blekinge przez rosyjski samolot An-30. W czerwcu 2024 r. rosyjski bombowiec Su-24 naruszył szwedzką przestrzeń powietrzną na wschód od Gotlandii. Natomiast w październiku 2024 r. na prośbę NATO szwedzkie myśliwce poderwano w celu przeprowadzenia identyfikacji samolotu, który pojawił się w przestrzeni powietrznej nad Bałtykiem. Okazało się, że był to rosyjski wojskowy samolot rozpoznania radioelektronicznego typu Ił-20. W styczniu 2025 r. rosyjski samolot został zlokalizowany nad szwedzkim regionem Skania. Nielegalny przelot nad międzynarodowymi wodami terytorialnymi potwierdziły Szwedzkie Siły Zbrojne, które jednak nie podały czasu zdarzenia ani dokładnej trasy lotu. Samolot wykonywał lot bez

[73] T. Nedwick, *Russian Shahed Kamikaze Drone Crashes In Latvia*, TWZ, 9 września 2024 r., www.twz.com.

[74] A. Sytas, G. Slattery, *Russian jets enter Estonia's airspace in latest test for NATO*, Reuters, 20 września 2025 r., www.reuters.com.

[75] F. Bryjka, *Ukraińskie uderzenia na rosyjskie cele nad Bałtykiem*, „Depesza PISM", 27 marca 2026 r., www.pism.pl.

[76] *Swedish defence minister calls Russian violation of airspace 'unacceptable'*, Reuters, 2 marca 2022 r., www.reuters.com.

transpondera, co sprawiło, że nie był widoczny dla cywilnego ruchu lotniczego. W kwietniu 2025 r. szwedzkie myśliwce przechwyciły natomiast rosyjski samolot nad Bałtykiem. W czerwcu 2025 r. Szwecja poderwała dwa myśliwce nad regionem Skania po wykryciu dwóch rosyjskich myśliwców Su-30 w pobliżu swojej przestrzeni powietrznej[77].

W nocy z 8 na 9 września 2024 r. nad sztokholmskim lotniskiem Arlanda zaobserwowano cztery drony różnej wielkości, co wymusiło natychmiastowe zamknięcie ruchu lotniczego na kilka godzin. Zdaniem policji mogło to być działanie celowe. Wszczęto śledztwo w związku z podejrzeniem aktu sabotażu oraz naruszenia bezpieczeństwa obiektu chronionego. Podczas kolejnych nocy takie incydenty powtarzały się. Jak dotąd nie wiadomo, jaki typ dronów był zaangażowany ani kto stał za incydentem. Lotnisko Arlanda, podobnie jak wszystkie inne szwedzkie lotniska zarządzane przez firmę Swedavia, nie posiada systemów do wykrywania lub odpierania ataków dronów.

Władze Norwegii potwierdziły z kolei trzy przypadki naruszenia przestrzeni powietrznej tego państwa przez rosyjskie statki powietrzne w 2025 r.: 25 kwietnia – myśliwiec Su-24 naruszył na cztery minuty przestrzeń powietrzną koło Vardø, 24 lipca – rosyjski samolot L-410 Turbolet wleciał w przestrzeń powietrzną w regionie Finnmark, pozostając nad niezamieszkałym obszarem przez ok. trzy minuty, a 18 sierpnia – myśliwiec Su-33 na krótko (jedną minutę) wleciał w norweską przestrzeń nad Morzem Barentsa (na północny wschód od Vardø). Władze Norwegii zażądały od Rosji wyjaśnień i podkreśliły, że niezależnie od intencji – czy były to błędy nawigacyjne, czy działania celowe – każde z tych zdarzeń stanowiło zagrożenie dla bezpieczeństwa w regionie północnym[78].

W 2025 r. w Norwegii doszło także do incydentów z dronami. W dniach 22–23 września na lotnisku w Oslo (Gardermoen) zgłoszono obecność dronów w pobliżu pasa startowego, co doprowadziło do czasowego zamknięcia przestrzeni powietrznej i przekierowania części lotów. Natomiast 30 września na lotnisku Brønnøysund policja stwierdziła działanie niezidentyfikowanego drona, jednak operator bezzałogowca nie został zlokalizowany. Podobne obserwacje odnotowano również nad platformą Sleipner (na Morzu Północnym). Służby bezpieczeństwa podkreślają, że brak jest jednoznacznych dowodów na powiązanie zaobserwowanych dronów z konkretnymi podmiotami państwowymi, jednak zjawisko to traktowane jest jako realne ryzyko hybrydowe poniżej progu konfliktu zbrojnego.

Wystąpienie podobnych incydentów w Danii w tym samym okresie wzmocniło przypuszczenia o możliwej koordynacji tego typu rosyjskich działań wobec różnych krajów. W reakcji na operowanie niezidentyfikowanych dronów m.in. nad lotniskami (kopenhaskie Kastrup, porty lotnicze w Aalborgu i południowej Jutlandii) i bazami wojskowymi

[77] F. Lemieux, *Russia tested NATO's airspace 18 times in 2025 alone – a 200% surge that signals a dangerous shift*, „The Conversation", 19 lutego 2026 r., https://theconversation.com.

[78] *Norway says Russia violated its airspace three times in 2025*, Reuters, 23 września 2025 r., www.reuters.com.

(Karup), co miało miejsce we wrześniu 20205 r.[79], duńskie władze zamknęły przestrzeń powietrzną dla prywatnych dronów w dniach 28 września – 3 października 2025 r.

Ponadto tylko w 2024 r. duńskie myśliwce F-16 były podrywane 81 razy w celu zbadania i monitorowania statków powietrznych wlatujących w pobliże przestrzeni powietrznej Danii[80]. Jednym z celów takich działań Rosji jest stałe testowanie duńskiego systemu obrony powietrznej.

Loty niezidentyfikowanych dronów w 2025 r. stały się coraz poważniejszym problemem także dla Niemiec. Według prezesa Federalnego Urzędu Policji Kryminalnej (BKA) w ciągu ostatniego roku w Niemczech odnotowano ponad 1000 podejrzanych lotów dronów – w większości nad obiektami wojskowymi, przedsiębiorstwami z sektora obronnego oraz infrastrukturą krytyczną[81].

W 2025 r. doszło zatem sumarycznie do największej liczby naruszeń przestrzeni powietrznej państw RPMB (patrz załącznik), co korespondowało ze zwiększającą się liczbą aktów dywersji i sabotażu i świadczyło o zaostrzeniu polityki Rosji wobec regionu.

[79] I. Aikman, *Drones seen over Danish military bases in latest air disruption*, BBC, 27 września 2025 r., www.bbc.com.

[80] *F-16 deployed many times in 2024*, Danish Defence, 4 lutego 2025 r., www.forsvaret.dk.

[81] K. Neubert, *Germany records more than 1,000 suspicious drone sightings this year*, „Euractiv", 22 grudnia 2025 r., www.euractiv.com.

Potencjał eskalacyjny Rosji

Nasilenie wrogich aktywności hybrydowych obserwowanych od 2022 r. wskazuje, że Rosja dysponuje potencjałem dalszych eskalacji, który może wykorzystywać w zależności od sytuacji politycznej w regionie. Rosjanie najpewniej będą czasowo zwiększać presję z użyciem działań hybrydowych, zwłaszcza w okresach okołowyborczych w państwach RPMB. Będzie to jednym ze sposobów oddziaływania na procesy polityczne, przede wszystkim w celu ciągłego wielowymiarowego osłabiania bezpieczeństwa państw regionu. Polityka Rosji będzie jednak w istotnym stopniu zależała od zdolności do odpowiedzi i podjęcia działań odwetowych przez atakowane państwa.

Domena morska

Rosyjskie operacje hybrydowe w regionie Morza Bałtyckiego opierają się na gotowości sektora cywilnego – statków i załóg, a także obiektów związanych z działalnością morską – do wzmocnienia potencjału Sił Zbrojnych Federacji Rosyjskiej. Takie założenie przyjęto w Doktrynie morskiej Federacji Rosyjskiej z lipca 2022 r.[82] Należy zatem przypuszczać, że statki cywilne są i będą w przyszłości włączane w działania operacyjne i będą realizować wyznaczone zadania o charakterze rozpoznawczym lub sabotażowym nie w sposób incydentalny, a systemowy.

Takie podejście pozwala jednocześnie na odciążenie Floty Bałtyckiej od zadań związanych z prowadzeniem operacji hybrydowych. Jest to tym istotniejsze, że jej zasoby nie zostały uszczuplone w wyniku wojny z Ukrainą, co pokazały zakrojone na szeroką skalę ćwiczenia „Ocean 2024"[83]. Rosja ma zatem zdolności zarówno do kontynuowania bieżącego schematu operacji hybrydowych na Morzu Bałtyckim, jak i do podejmowania dalej idących działań pozostających poniżej progu wojny. Na eskalację w domenie morskiej Rosja mogłaby się zdecydować przede wszystkim w sytuacji skutecznego ograniczenia działania „floty cieni", która wspiera finansowanie machiny wojennej Władimira Putina. Do tej pory do takiej eskalacji doszło w maju 2025 r., gdy

[82] *Морская Доктрина Российской Федерации, утверждена Указом Президента Российской Федерации от 31 июля 2022 г. № 512*, Министерство иностранных дел Российской Федерации, 31 lipca 2022 r., www.mid.ru.

[83] Ćwiczenia pokazały, że choć rosyjski system A2/AD w regionie Morza Bałtyckiego został osłabiony przez wojnę z Ukrainą, to pozostaje w pełni operacyjny.

rosyjski myśliwiec (z naruszeniem przestrzeni powietrznej NATO) utrudnił zatrzymanie przez estońskie służby statku „floty cieni". Dalsza eskalacja mogłaby zatem polegać na systematycznym eskortowaniu statków „floty cieni" przez okręty rosyjskiej marynarki wojennej, co przełamywałoby schemat operowania takich jednostek, czyli unikanie bezpośrednich powiązań z państwem. Potwierdzeniem wzmożonej aktywności Rosji jest objęcie w kwietniu 2026 r. ochroną przez rosyjskie okręty ok. 40 statków „floty cieni", które w związku z zawieszeniem eksportu z portów w Primorsku i Ust-Ługde po ukraińskim ostrzale znajdują się na wodach Zatoki Fińskiej. Obawy przed eskalacją związaną z zatrzymywaniem takich jednostek przez Estonię wyraził dowódca estońskiej marynarki wojennej komandor Ivo Värk, choć groźby inspekcji i zatrzymań były dotąd jednym z niewielu narzędzi używanych przez państwa RPMB do ograniczania działalności „floty cieni"[84].

Domena lądowa

Analiza ewolucji metod stosowanych przez rosyjskie służby wywiadowcze w ramach prowadzonej od 2022 r. kampanii dywersyjno-sabotażowej wskazuje na gotowość Rosji do eskalacji w postaci przeprowadzenia operacji kinetycznych, w wyniku których może ostatecznie dojść do ofiar śmiertelnych. W domenie lądowej najpoważniejszymi incydentami były próby wykolejenia pociągów i ataki na infrastrukturę zawierającą substancje chemiczne. Kolejnym etapem eskalacji mogą być próby wykorzystania materiałów wybuchowych lub łatwopalnych przeciwko infrastrukturze energetycznej (dotychczas atakowanej głównie w cyberprzestrzeni) i teleinformatycznej (np. od czerwca 2025 r. szwedzkie władze prowadzą dochodzenie w sprawie ok. 30 aktów sabotażu wymierzonych w maszty telekomunikacyjne) czy systemom zaopatrywania ludności w wodę.

Do tej pory Rosja nie wykorzystuje również całego swojego potencjału do organizowania szeroko zakrojonych działań dywersyjno-sabotażowych. Kampania taka jest obecnie prowadzona przez niewyszkolonych amatorów, ale w przyszłości do realizacji takich zadań Rosja może wysyłać kadrowych oficerów wywiadu i żołnierzy sił specjalnych (Specnaz). W strukturze wywiadu wojskowego GU taką funkcję pełni m.in. Służba Działań Specjalnych (JW 29155 alias 161 Centrum), kierowana przez generała majora Andrieja Awerjanowa. W 2014 r. oficerowie tej jednostki byli zamieszani w wybuch magazynów amunicji we Vrběticach w Czechach. W wyniku tego zdarzenia zginęły dwie osoby, a 150 ton amunicji, która miała trafić na Ukrainę, uległo zniszczeniu. Działalność dywersyjno-sabotażową w Europie mogą prowadzić również oficerowie i żołnierze z jednostki GU „Sieneż" (JW 92154 alias 322 Centrum Szkolenia), która powstała w 1999 r. na potrzeby II wojny czeczeńskiej. To właśnie z tej jednostki pochodził Jurij Sizow – oficer prowadzący Jewhenija Iwanowa, który organizował zamach na fabrykę dronów we

[84] A. Sytas, *Estonia says detaining Russia's tankers in Baltic Sea is too risky*, Reuters, 10 kwietnia 2026 r., www.reuters.com.

Lwowie, a następnie uczestniczył w zamachu na linie kolejowe w Polsce. Wszystkie te jednostki, mimo zaangażowania Rosji w działania w Ukrainie, mają istotny potencjał eskalacyjny.

Domena powietrzna

W domenie powietrznej Rosja ma potencjał dalszego eskalowania napięcia nie tylko poprzez zwiększanie intensywności przelotów samolotów wojskowych w pobliżu przestrzeni powietrznej państw regionu lub wręcz naruszając ich granice, ale przede wszystkim poprzez wykorzystywanie na szerszą skalę różnego rodzaju dronów. Należy też oczekiwać utrzymania, a okresami nasilenia zakłóceń sygnału GNSS, co będzie narażało bezpieczeństwo przede wszystkim cywilnej żeglugi powietrznej i morskiej. W skrajnym wypadku, podobnie jak ma to miejsce w domenie lądowej, działania takie mogą doprowadzić do katastrofy lotniczej ze znaczną liczbą ofiar.

Nie można też wykluczyć, że będą się powtarzać incydenty z masowym wlotem dronów bojowych w przestrzeń powietrzną państw regionu Morza Bałtyckiego, co będzie zwiększać siłę oddziaływania kognitywnego prowadzonego głównie w domenie lądowej. Akty dywersji i sabotażu mogą być także prowadzone przy użyciu dronów FPV wykorzystywanych nie tylko w regionach przygranicznych, ale też przez tzw. jednorazowych agentów.

Działania te Rosja może prowadzić w zasadzie bezkosztowo, np. w ramach rutynowych ćwiczeń wojskowych czy poprzez zwiększenie liczby źródeł zakłóceń sygnału GNSS. Liczy przy tym, że reakcja zaatakowanych członków RPMB będzie o wiele bardziej kosztowna i wymagająca nie tylko stałego podrywania myśliwców dyżurnych, ale też inwestycji w odporne na zagłuszenia systemy geolokalizacji. Działania w domenie powietrznej będą też służyły Rosji do stałego testowania systemów obrony powietrznej państw NATO.

Dobre praktyki

Schematy działań wykorzystywane przez Rosję są coraz lepiej znane i coraz bardziej powtarzalne, zatem na ich podstawie należałoby opracować katalog dobrych praktyk, określający wspólne reguły monitorowania, raportowania i reagowania na operacje hybrydowe. Państwa regionu Morza Bałtyckiego powinny zobowiązać się do konsekwentnego ich stosowania, ponieważ tylko spójna reakcja wszystkich krajów może skutecznie oddziaływać na Rosję.

Dlatego, aby efektywnie zapobiegać i odpowiadać na zagrożenia generowane przez Rosję, warto, by państwa członkowskie RPMB wypracowały wspólny katalog dobrych praktyk obejmujący domeny morską, powietrzną i lądową, który umożliwiałby bardziej skuteczne reagowanie na prowadzone przez Rosję operacje hybrydowe.

Domena morska

W dotychczasowych przypadkach wrogich działań w domenie morskiej służby każdego z członków RPMB interweniowały głównie samodzielnie – monitorowały, zapobiegały, zatrzymywały i eskortowały podejrzane jednostki zgodnie z krajowymi przepisami i metodami operacyjnymi. Jednocześnie ze względu na obowiązujące prawo, przede wszystkim na ograniczoną jurysdykcję w wyłącznej strefie ekonomicznej i na wodach międzynarodowych, rzadko udaje się nakładać, a następnie egzekwować kary za naruszenia.

Najjaskrawszym przykładem jest umorzenie przez sąd w Finlandii postępowania wobec statku rosyjskiej „floty cieni" Eagle S, który uszkodził podmorski kabel energetyczny między Finlandią a Estonią w grudniu 2024 r. Była to jedna z najbardziej zdecydowanych i daleko idących reakcji na rosyjskie operacje hybrydowe, której niepowodzenie – związane z orzeczeniem przez sąd braku jurysdykcji – będzie zniechęcało inne państwa do podejmowania podobnego wysiłku.

Skuteczniejsze okazują się działania zapobiegawcze, takie jak zablokowanie 10 stycznia 2026 r. wejścia na niemieckie wody terytorialne statku Tavian, należącego do rosyjskiej „floty cieni". Niemieckie służby wysłały śmigłowiec, zażądały przedstawienia dokumentów i zagroziły konfiskatą, co zmusiło załogę do zawrócenia z kursu i skierowania się na Morze Barentsa.

Państwa RPMB nie podjęły dotychczas skoordynowanych działań, dlatego też dobre praktyki opierają się na pojedynczych interwencjach państw. Jest ich jednak niewiele, choć modele operowania służb i systemy krajowego prawodawstwa są powoli dostosowywane do nowych warunków.

Jedynym dotychczasowym działaniem na szerszą skalę jest misja „Baltic Sentry", zainicjowana dzięki zacieśnianiu współpracy państw NATO na Morzu Bałtyckim i dowodzona przez Combined Task Force BALTIC (CTF B) w Rostocku podległe Dowództwu Sojuszniczych Sił Morskich (MARCOM) oraz Dowództwu Połączonych Sił Sojuszniczych w Brunssum (JFC BS). Jej działania wzmacniają odstraszanie przez samą obecność (*deterrence by presence*), co ma obniżać możliwości eskalacji po stronie rosyjskiej.

Domena lądowa

W odpowiedzi na rosyjskie działania dywersyjno-sabotażowe i terrorystyczne Polska stopniowo podejmowała dyplomatyczne działania odwetowe. W pierwszej kolejności ograniczono swobodę przemieszczania się rosyjskiego personelu dyplomatycznego do województw, w których mieści się placówka dyplomatyczna. Następnie, po wykazaniu przez prokuraturę roli rosyjskiego wywiadu w przygotowaniach zamachu na fabrykę we Wrocławiu, zdecydowano o zamknięciu konsulatu Federacji Rosyjskiej w Poznaniu. Takie same represalia podjęto po ustaleniach dotyczących spalenia centrum handlowego przy ul. Marywilskiej 44 (zamknięto konsulat w Krakowie), a także po zamachu terrorystycznym na linii kolejowej (zamknięto konsulat w Gdańsku).

Aby utrudnić Rosji prowadzenie działań wywiadowczych, Łotwa wprowadziła dodatkowe wymogi dla cudzoziemców pragnących wjechać do tego kraju bez wizy lub pozwolenia na pobyt. Na 48 godzin przed przekroczeniem granicy trzeba podać miejsce docelowe, planowany czas i miejsce pobytu, trasę podróży oraz dane kontaktowe. Władze łotewskie od września 2025 r. wymagają także informacji o zawodzie cudzoziemca oraz o tym, czy jest on posłem do parlamentu, dyplomatą, urzędnikiem państwowym lub funkcjonariuszem służb mundurowych. Odmowa podania informacji lub udzielenie informacji fałszywych mają być karane grzywną w wysokości do 2 tys. euro. Aby przeciwdziałać rekrutacji obywateli łotewskich przez rosyjskie służby wywiadowcze, wprowadzono zakaz podróży do Rosji i na Białoruś dla pracowników sektora publicznego, którzy mają dostęp do tajemnic państwowych, są odpowiedzialni za bezpieczeństwo infrastruktury krytycznej, są pracownikami ministerstw obrony, spraw wewnętrznych i sprawiedliwości, funkcjonariuszami służb podległych tym ministerstwom, dyplomatami oraz pracownikami misji dyplomatycznych i konsularnych, pracownikami sądów i prokuratur.

Łotewska VDD prowadzi też regularne dogłębne weryfikacje osób zatrudnionych w obiektach infrastruktury krytycznej, a także dostawców różnych usług. Celem jest identyfikacja osób stanowiących zagrożenie wywiadowcze. W czerwcu 2025 r. na Łotwie weszły w życie zmiany w ustawie o bezpieczeństwie narodowym, ograniczające

dostęp do obiektów infrastruktury krytycznej Łotwy dla obywateli Rosji i Białorusi, a także innych państw wspierających agresję Rosji. VDD uczestniczyło w opracowywaniu tych zmian, a ich celem było wzmocnienie ochrony infrastruktury krytycznej ważnej dla bezpieczeństwa państwa i społeczeństwa poprzez prewencyjne eliminowanie potencjalnych zagrożeń. W konsekwencji w 2025 r. kilkudziesięciu obywatelom Rosji i Białorusi zakazano pracy lub świadczenia usług w obiektach infrastruktury krytycznej w związku z pozbawieniem ich dostępu do informacji i sprzętu technicznego niezbędnych do funkcjonowania obiektu[85].

Czynnikiem zniechęcającym „agentów jednorazowego użytku" do współpracy z rosyjskim wywiadem może być zaostrzenie kar za działania dywersyjno-sabotażowe, które traktowane są na równi z terroryzmem. W odpowiedzi na rosnącą liczbę aktów sabotażu polskie władze rozszerzyły wykaz przestępstw popełnianych na rzecz zagranicznych służb wywiadowczych, określonych w art. 130 kodeksu karnego (szpiegostwo), o udział w działaniach dywersyjnych, sabotażowych i terrorystycznych, co podlega karze pozbawienia wolności na czas nie krótszy niż 10 lat lub dożywotniego pozbawienia wolności. Od początku 2023 r. do stycznia 2026 r. polskie organy ścigania postawiły zarzuty na podstawie tego artykułu 82 osobom. Dla porównania, w ciągu poprzednich siedmiu lat (2016–2023) odnotowano jedynie 46 aresztowań związanych z obcą działalnością wywiadowczą. Rosnąca liczba aresztowań świadczy zarówno o intensyfikacji działań rosyjskiego wywiadu, jak i o skuteczności polskiego kontrwywiadu.

W lutym 2025 r. sąd w Krakowie ustanowił nowy precedens prawny w zakresie ścigania rosyjskich operacji hybrydowych w Europie. Dwóch obywateli Rosji – Aleksiej Titow i Andriej Gontarew – otrzymało wyroki pięciu i pół roku pozbawienia wolności za szpiegostwo i przestępstwa związane z terroryzmem i współpracę z Grupą Wagnera (w tym członkostwo i przynależność do wyznaczonej organizacji terrorystycznej oraz szerzenie propagandy w imieniu zagranicznej agencji wywiadowczej). Władze polskie aresztowały ich w sierpniu 2023 r. za rozpowszechnianie materiałów rekrutacyjnych i propagandowych, a także prowadzenie operacji rozpoznawczych na terenie całego kraju. Ich przełożeni zainwestowali co najmniej 24 tys. dol. w liczne operacje wywiadowcze i operacje wpływu w Polsce, Francji i Niemczech[86].

Warto, aby wskazane środki były stosowane przez szersze grono państw, co utrudni działania służbom specjalnym Federacji Rosyjskiej. Członkowie RPMB mogą zatem rozważyć wprowadzenie podobnych obostrzeń, które będą miały na celu m.in. zwiększenie bezpieczeństwa infrastruktury krytycznej. Jednocześnie istotne będzie zaostrzanie kar w innych państwach UE i NATO, co jasno pokaże ich podejście do osób współpracujących z rosyjskimi służbami specjalnymi.

[85] *Annual Report for 2025*, Latvian State Security Service (VDD), 2026, s. 14, www.vdd.gov.lv.

[86] C. Rondeaux, *The legal counteroffensive to Russia's hybrid war*, „Lawfare", 6 kwietnia 2025 r., www.lawfaremedia.org.

Domena powietrzna

Jednym z najważniejszych działań państw NATO po masowym wlocie rosyjskich dronów bojowych na terytorium Polski we wrześniu 2025 r. było uruchomienie operacji „Wschodnia straż", dzięki której od tego czasu udało się uniknąć wydarzenia o takiej skali. Warto, aby Sojusz nadal prowadził takie działania, a jego państwa członkowskie wspólnie odbywały misje w regionach najbardziej narażonych na rosyjskie ataki, takich jak m.in. obszar Morza Bałtyckiego.

Istotną rolę w prewencji zagrożeń w domenie powietrznej odgrywa też współpraca państw NATO w misji Air Policing koordynowanej przez Dowództwo Sojuszniczych Sił Powietrznych (Allied Air Command, AIRCOM) w Ramstein, które było aktywnie zaangażowane w działania zabezpieczające polską przestrzeń powietrzną w czasie wlotu rosyjskich dronów w nocy z 8 na 9 września 2025 r.

Warto też odnotować współpracę członków RPMB na rzecz walki z zakłóceniami sygnału GNSS. Działania w ramach międzynarodowych agencji oraz wspólne projekty na rzecz budowy systemów odpornych na zagłuszanie będą ważnymi inicjatywami zwiększającymi bezpieczeństwo żeglugi powietrznej i morskiej.

Przytoczone przykłady skutecznych działań poszczególnych członków RPMB mogą składać się na katalog dobrych praktyk, którymi państwa Rady mogą się dzielić, a także współpracować w zakresie ich wdrażania.

Wnioski i rekomendacje

Obserwowana od 2022 r. w państwach Regionu Morza Bałtyckiego rosnąca liczba aktów dywersji i sabotażu wskazuje, że Rosja prowadzi kompleksową kampanię, której celem jest podwyższenie kosztów zachodniej pomocy dla Ukrainy, osłabienie społecznego i politycznego poparcia dla kontynuowania tej polityki, a także wywołanie na tym tle rozbieżności w strukturach europejskich i transatlantyckich. Choć mimo tych wysiłków Rosja do tej pory nie osiągnęła swoich celów, to skala zagrożeń pozostaje duża, a Rosja zachowuje zdolność do eskalacji konfliktu.

Dotychczas Rosja decydowała się na eskalację przede wszystkim w okresach, kiedy przedmiotem dyskusji w UE i NATO były kolejne transze pomocy wojskowej dla Ukrainy, a także gdy negocjowano nałożenie na Rosję kolejnych pakietów sankcji. Należy założyć, że w przyszłości może ona dążyć do zaostrzenia, by wywrzeć presję na europejskich decydentów w podobnych uwarunkowaniach politycznych. Co więcej, wypracowane przez Rosjan metody będą dalej rozwijane, by systemowo osłabiać atakowane państwa. Rosnąca liczba aktów dywersji i sabotażu wskazuje także, że Rosja prowadzi wobec państw NATO i UE kompleksową kampanię, której celem jest podwyższenie kosztów zachodniej pomocy dla Ukrainy, osłabienie społecznego i politycznego poparcia dla kontynuowania tej polityki, a także wywołanie na tym tle rozbieżności w ramach struktur europejskich i transatlantyckich.

Za skuteczność rosyjskich operacji hybrydowych na morzu odpowiadały opracowane wcześniej schematy, które były konsekwentnie i nieprzerwanie wdrażane. Pozwalają one Rosji destabilizować sytuację w regionie Morza Bałtyckiego poprzez wywoływanie strat bieżących (zaburzenia dostaw energii i łączności) oraz systemowych – rozproszenie sił i środków wojskowych na zwalczanie zagrożeń hybrydowych i odciąganie od podstawowych zadań obrony i odstraszania. Ułatwiają ponadto zarządzanie ryzykiem eskalacji, ponieważ atrybucja działań sabotażowych jest utrudniona, a działania rozpoznawcze co do zasady nie wyrządzają szkody obiektom lub systemom, więc reakcje na nie zawsze będą ograniczone.

W domenie lądowej Rosji udało się doprowadzić do szeregu incydentów wymierzonych w bezpieczeństwo infrastruktury krytycznej, a nasilanie się tych działań od 2024 r. wskazuje na coraz większą determinację do spowodowania wymiernych szkód mających również znaczenie kognitywne.

W domenie powietrznej Rosja również pozostawała aktywna i nie ograniczała się do incydentów wykorzystujących wojskowe samoloty i śmigłowce, ale wielokrotnie stosowała bezzałogowe statki powietrzne. Ważnym elementem oddziaływania były także zakłócenia sygnału GNSS, co wywoływało problemy w żegludze powietrznej i morskiej. W konsekwencji działań Rosji region Morza Bałtyckiego stał się tym obszarem GNSS w Europie, gdzie zakłóceń było najwięcej.

W domenie morskiej na poziomie operacyjnym kluczowe będzie zatem wspieranie przez UE rozwoju sieci wymiany informacji CISE i MARSUR, które poprawią świadomość sytuacyjną w regionie Morza Bałtyckiego. Niezbędne będzie także wdrożenie opracowanego w ramach NATO systemu Mainsail[87]. Dzięki zastosowaniu sztucznej inteligencji analiza danych z różnych źródeł pozwoli łatwiej wykrywać podejrzane jednostki lub operacje w domenie morskiej i podejmować działania zapobiegawcze.

Na poziomie regulacyjnym najważniejsza będzie natomiast implementacja przez państwa członkowskie unijnej dyrektywy z 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych. Newralgiczne będzie też wprowadzenie uregulowań prawnych dotyczących zbierania i wymiany informacji między sektorem prywatnym i publicznym w zakresie ochrony morskiej infrastruktury krytycznej. Istotne będzie też przyjęcie uregulowań prawnych dotyczących zasad wykorzystywania nawodnych i podwodnych bezzałogowych platform oraz ich ewentualnej neutralizacji.

Jednocześnie wdrożona niedawno praktyka odstraszania przez obecność (*deterrence by presence*) powinna być traktowana przez państwa NATO i UE jako rozwiązanie tymczasowe. Nie eliminuje ono podstawowego problemu, którym jest niemożność pociągnięcia Rosji do odpowiedzialności lub nałożenia na nią adekwatnych kosztów za operacje hybrydowe.

Na poziomie politycznym dla skutecznego przeciwdziałania rosyjskim akcjom dywersyjno-sabotażowym kluczowe jest natomiast zapewnienie wysokiego poziomu świadomości sytuacyjnej dzięki ścisłej współpracy – na poziomie krajowym i międzynarodowym – wojskowych i cywilnych służb wywiadowczych i kontrwywiadowczych, straży granicznej i policji. Jest to szczególnie istotne, jeśli weźmie się pod uwagę swobodę przemieszczania się w ramach strefy Schengen i możliwość prowadzenia przez dywersantów działalności na obszarze kilku państw. Współdziałanie czeskiej, litewskiej, polskiej i rumuńskiej prokuratury w ramach Agencji UE ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (EUROJUST) umożliwiło zatrzymanie i skazanie siatki dywersyjno-terrorystycznej odpowiedzialnej za podpalenia obiektów w tych państwach[88].

Rolę platformy międzynarodowej wymiany doświadczeń i szkoleń w zakresie zwalczania rosyjskiego sabotażu pełni Centrum Doskonalenia NATO ds. Kontrwywiadu (NATO

[87] *NATO advances maritime innovation and readiness through Exercise Dynamic Messenger 2025*, Public Affairs Office at MARCOM, 29 września 2025 r., https://mc.nato.int.

[88] *Terrorist group responsible for arson attacks across Europe taken to court*, European Union Agency for Criminal Justice Cooperation, 27 stycznia 2026 r., www.eurojust.europa.eu.

CI CoE) z siedzibą w Krakowie, a także Europejskie Centrum Doskonalenia ds. Przeciwdziałania Zagrożeniom Hybrydowym (Hybrid CoE) w Helsinkach. Instytucje te nie zostały jednak powołane w celu wymiany informacji wywiadowczych między państwami. Dlatego warto, aby na poziomie krajowym państwa RPMB rozważyły utworzenie Centrów Zwalczania Zagrożeń Hybrydowych, których zadaniem byłaby koordynacja wymiany informacji między poszczególnymi instytucjami. Zbudowanie takiej struktury w ramach Federalnego Urzędu Ochrony Konstytucji (BfV) zapowiedziały Niemcy. W przypadku Polski i działań operacyjnych możliwe byłoby rozszerzenie zakresu kompetencji istniejącego już Centrum Antyterrorystycznego ABW (która już pełni rolę krajowego koordynatora w inicjatywach KE związanych z budowaniem odporności infrastruktury krytycznej). Z kolei w wymiarze strategicznym i systemowym konieczna będzie rozbudowa zdolności RCB, które powinno być instytucją spajającą całość polskiego systemu ochrony infrastruktury krytycznej. Na poziomie UE funkcję koordynatora wymiany informacji pełni Komórka ds. Syntezy Informacji o Zagrożeniach Hybrydowych (Hybrid Fusion Cell), utworzona w 2016 r. przy Centrum Wywiadowczym i Sytuacyjnym UE (EU INTCENT). Wyzwaniem pozostaje jednak gotowość i chęć poszczególnych służb kontrwywiadowczych i wywiadowczych do dzielenia się wrażliwymi informacjami w gronie 27 państw. Mając na uwadze te ograniczenia, państwa preferują współpracę w wymiarze bilateralnym. Członkowie RPMB mogą przezwyciężyć te ograniczenia i we własnym gronie stworzyć system wymiany informacji wywiadowczych na temat zagrożeń hybrydowych.

Ze względu na to, że operatorami obiektów infrastruktury krytycznej są często podmioty prywatne, na poziomie operacyjnym i regulacyjnym kluczowe jest także wzmacnianie wymiany informacji między sektorem publicznym a prywatnym. Kwestie podziału kompetencji i obowiązków w tym zakresie reguluje Dyrektywa CER (Critical Entities Resilience Directive), której sprawna implementacja do krajowych systemów zarządzania kryzysowego ma zasadnicze znaczenie dla możliwości budowania zdolności do monitorowania i reagowania na zagrożenia dywersyjno-sabotażowe (zwłaszcza w zakresie zwalczania dronów powietrznych i morskich). Zainwestowanie prywatnych operatorów infrastruktury krytycznej w sensory umożliwiające wczesne wykrycie zagrożenia poprawi świadomość sytuacyjną i skróci czas reakcji struktur siłowych (policji, straży granicznej lub wojska). Kluczowe znaczenie ma również zapewnienie najwyższych standardów bezpieczeństwa oraz podnoszenie świadomości kadry kierowniczej i pracowników obiektów infrastruktury krytycznej na temat zagrożenia dywersją i sabotażem, m.in. poprzez szkolenia.

By zmniejszyć podatność linii kolejowych na działalność dywersyjno-sabotażową, niezbędne będzie zwiększenie nakładów finansowych na ich modernizację i dostosowanie do norm wojskowych (ze względu na podwójne zastosowanie tej infrastruktury). Konieczne będzie także wzmocnienie systemów monitoringu i ostrzegania o uszkodzeniach infrastruktury kolejowej. W unijnym planie działania na rzecz gotowości obronnej do 2030 r. przewidziano na ten cel pakiet o wartości 1,7 mld euro. Zaplanowano w jego ramach inwestycje w regionie bałtyckim i skandynawskim, mające na celu dostosowanie tamtejszej infrastruktury kolejowej do europejskich systemów szerokości torów.

Prywatne przedsiębiorstwa wskazują jednak, że zaplanowany budżet jest niewystarczający (potrzeba co najmniej 100 mld euro), dlatego zwróciły się do UE z wnioskiem o przydzielenie dodatkowych środków w ramach instrumentu „Łącząc Europę" (CEF)[89].

By zniechęcić potencjalnych „jednorazowych agentów" do współpracy z rosyjskim wywiadem, państwa RPMB powinny na poziomie regulacyjnym dążyć do zaostrzenia kar za działalność dywersyjną, sabotażową i terrorystyczną. Jednocześnie warto, aby prowadziły przy tym szeroko zakrojone działania komunikacyjne, uświadamiające społeczeństwo o charakterze zagrożenia i możliwych konsekwencjach. Kampania społeczna powinna być przy tym ukierunkowana na grupy najbardziej podatne na werbunek (w tym imigrantów z państw Europy Wschodniej). Podwyższenie społecznej świadomości na temat sytuacji, które powinny zwracać uwagę, oraz sposobów informowania organów państwowych (np. ABW utworzyła specjalnego chatbota w serwisie Telegram do raportowania prób werbunku za pomocą tej aplikacji) stworzy dodatkowe źródło ważnych informacji. Rosjanie, którzy prowadzili w Polsce działania ukierunkowane m.in. na rekrutację do Grupy Wagnera, zostali złapani, gdy przypadkowa osoba poinformowała policję o dystrybucji materiałów rekrutacyjnych.

By skutecznie reagować na rosyjską dywersję i sabotaż, a także wpływać na kalkulacje Rosji i odstraszać ją przed kontynuowaniem lub eskalowaniem prowadzonej kampanii, państwa NATO i UE muszą w większym stopniu obciążać kosztami agresora. Może to obejmować działania dyplomatyczne, m.in. dalsze wydalenia rosyjskich szpiegów działających pod przykrywką dyplomatyczną, sankcje, obniżenie rangi stosunków dwustronnych, zamknięcie rosyjskich misji dyplomatycznych lub innych instytucji wykorzystywanych jako przykrywka dla wywiadu (np. Domów Rosyjskich).

W domenie powietrznej na poziomie operacyjnym niezbędne może okazać się natomiast wprowadzenie systemów pozwalających na korzystanie z alternatywnych technologii pozycjonowania (np. sieci 5G), co będzie miało znaczenie wspomagające w realizacji procedur lotniczych (zwłaszcza najbardziej newralgicznych, czyli startu i lądowania, w trakcie których niezbędne jest precyzyjne ustalenie pozycji). Dla poprawy bezpieczeństwa żeglugi powietrznej kluczowe będzie rozwijanie zdolności umożliwiających lokalizację emiterów zakłóceń, co powinno pozwolić na odfiltrowywanie zakłóconych sygnałów. Systemy te mogą znaleźć zastosowanie również w żegludze morskiej. Warto też rozważyć poszerzenie współpracy cywilno-wojskowej w zakresie korzystania z urządzeń neutralizujących zakłócenia, które są używane przez samoloty wojskowe. Niezbędny może się okazać ponadto rozwój sieci naziemnych radarów wspomagających samoloty i statki.

Biorąc pod uwagę, że coraz więcej zagrożeń jest powodowanych przez bezzałogowe statki powietrzne, konieczne będzie poszerzenie ochrony radioelektronicznej obiektów kluczowych dla funkcjonowania państwa, ze szczególnym uwzględnieniem infrastruk-

[89] E. Ferris, *Russian Sabotage of NATO Infrastructure: Identifying Alliance Vulnerabilities*, RUSI, 26 marca 2026 r., www.rusi.org.

tury transportowej, energetycznej, telekomunikacyjnej i granicznej. Członkowie RPMB mogą w tym zakresie korzystać też z doświadczeń Ukrainy, która stale rozwija takie zdolności. Dla Finlandii, państw bałtyckich i Polski wskazane może okazać się także opracowanie wspólnych systemów zwalczania balonów meteorologicznych i wypracowanie procedur wspólnej reakcji (w tym dyplomatycznej) na takie zdarzenia.

W przypadku nasilających się incydentów z udziałem rosyjskich samolotów wojskowych na poziomie regulacyjnym niezbędna może okazać się zmiana zasad podejmowania działań przy użyciu siły (*rules of engagement*, ROE) i przekazanie większych kompetencji pilotom państw NATO, którzy prowadzą misje Air Policing, oraz operatorom naziemnych systemów przeciwlotniczych, aby mogli bardziej aktywnie bronić przestrzeni powietrznej państw NATO.

Odrębną kwestią pozostaje konieczność budowania odporności społecznej, m.in. poprzez szeroko zakrojone kampanie edukacyjne i odpowiednią zmianę programów nauczania, np. na wzór państw nordyckich. Warto, aby państwa RPMB wykorzystywały wzajemnie swoje doświadczenia w tym zakresie i dzieliły się najlepszymi praktykami. W kwestii walki z dezinformacją towarzyszącą aktom sabotażu i dywersji niezbędna będzie także współpraca między instytucjami państw RPMB odpowiedzialnymi za komunikowanie strategiczne. Wspólne organizowanie kampanii społecznych pozwoli dotrzeć do znacznie szerszego kręgu odbiorców.

Zagrożenie ze strony Rosji pozostanie najważniejszym wyzwaniem bezpieczeństwa, z jakim w najbliższych latach będą mierzyć się członkowie RPMB. Wynika to z systemowego podejścia Rosji do państw regionu Morza Bałtyckiego, które są postrzegane jako wrogie. Oznacza to, że w najbliższych miesiącach i latach należy oczekiwać nasilenia działań dywersyjnych i sabotażowych prowadzonych przez Rosję. Tym samym jedynie szeroko zakrojona współpraca międzynarodowa w ramach RPMB, a szerzej także UE i NATO, pozwoli zwiększyć odporność na rosyjskie działania hybrydowe.

Załączniki

Domena morska

Tabela 1

Kinetyczne zdarzenia hybrydowe w domenie morskiej (2022–2026)

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
26.09.2022	Wody międzynarodowe, wyłączne strefy ekonomiczne Danii i Szwecji	Uszkodzenie trzech z czterech nitek gazociągów Nord Stream 1 i Nord Stream 2	Sprawa w toku w Niemczech, zamknięta w Danii i Szwecji w 2024 r.	Podmorska infrastruktura energetyczna	Podejrzana grupa siedmiorga Ukraińców (jacht Andromeda)	Brak	Śledztwo	Eksplozje
7.10.2023	Wody terytorialne Estonii	Uszkodzenie podwodnego kabla komunikacyjnego między Szwecją a Estonią (EE-S1)	Sprawa zakończona	Podmorska infrastruktura komunikacyjna	Podejrzewane statki: New-new Polar Bear (Chiny), Siewmorput' (Rosja)	Brak	Śledztwo	Do publicznej wiadomości podano 17.10. Sprawa łączona z Balticconector i Elisa

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
8.10.2023	Zatoka Fińska, wyłączna strefa ekonomiczna Finlandii	Uszkodzenie gazociągu Balticconnector między Finlandią a Estonią	Sprawa w toku	Podmorska infrastruktura energetyczna	Newnew Polar Bear (bandera Hongkongu)	Chiny	Współpraca z Chinami w toku dochodzenia. Chiny twierdzą, że wypadek był spowodowany trudnymi warunkami pogodowymi	Statek ciągnął kotwicę, odnalezioną na miejscu zdarzenia. Podejrzewano również znajdujący się w pobliżu rosyjski barkowiec o napędzie nuklearnym Siewmorput'. Sprawa łączona z EE-S1 i Elisa
10.2023	Strefa ekonomiczna Estonii, poza wodami terytorialnymi	Uszkodzenie podwodnego kabla komunikacyjnego między Estonią a Finlandią (operator Elisa)	Sprawa zakończona	Podmorska infrastruktura komunikacyjna	Podejrzewane statki: Newnew Polar Bear (Chiny), Siewmorput' (Rosja)	Brak	Śledztwo	Sprawa łączona z Balticconector i EE-S1
17.11.2024	Wyłączna strefa ekonomiczna Szwecji	Uszkodzenie podmorskiego kabla telekomunikacyjnego łączącego Litwę ze Szwecją (BCS East-West Interlink)	Sprawa w toku	Podmorska infrastruktura komunikacyjna	Yi Peng 3 (bandera Chin)	Chiny	Żądanie straży granicznej Danii, by zakotwiczono statek w Cieśninach Duńskich	Sprawa rozpatrywana wspólnie z C-Lion1. W pobliżu zakotwiczenia Yi Peng 3 przebywał rosyjski okręt Jewgienij Czurow

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
18.11.2024	Wyłączna strefa ekonomiczna Szwecji	Uszkodzenie podmorskiego kabla telekomunikacyjnego łączącego Finlandię z Niemcami (C-Lion1)	Sprawa w toku	Podmorska infrastruktura komunikacyjna	Yi Peng 3 (bandera Chin)	Chiny	Żądanie straży granicznej Danii, by zakotwiczono statek w Cieśninach Duńskich	Sprawa rozpatrywana wspólnie z BCS East-West Interlink. W pobliżu zakotwiczenia Yi Peng 3 przebywał rosyjski okręt Jewgienij Czurow
25.12.2024	Zatoka Fińska	Uszkodzenie podmorskiego kabla elektrycznego między Finlandią a Estonią (Estlink2)	Sprawa umorzona (brak sądowej jurysdykcji nad wodami międzynarodowymi)	Podmorska infrastruktura energetyczna	Eagle S (bandera Wysp Cooka)	Statek rosyjskiej „floty cieni”	Zatrzymanie statku i załogi przez straż graniczną Finlandii	Statek ciągnął kotwicę. Wydarzenie dwa miesiące przed odłączeniem państw bałtyckich od rosyjskiego systemu elektroenergetycznego
01.02.2025	Wyłączna strefa ekonomiczna Szwecji	Ponowne uszkodzenie podmorskiego kabla telekomunikacyjnego łączącego Finlandię z Niemcami (C-Lion1)	Sprawa w toku	Podmorska infrastruktura komunikacyjna	Arne (bandera Antigui i Barbudy)	Brak	Monitorowanie statku przez jednostki Niemiec i Danii, następnie inspekcja	
31.12.2025	Zatoka Fińska, wyłączna strefa ekonomiczna Estonii	Uszkodzenie podmorskiego kabla telekomunikacyjnego między Estonią a Finlandią (operator Elisa)	Sprawa w toku	Podmorska infrastruktura komunikacyjna	Fitburg (bandera St. Vincent i Grenadyny)	Statek rosyjskiej „floty cieni”, transportował stal objętą sankcjami (nie zarekwirowano)	Zatrzymanie statku i załogi przez straż graniczną Finlandii	Statek ciągnął kotwicę

Źródło: badania własne.

Domena lądowa

Tabela 2

Kinetyczne ataki dywersyjno-sabotażowe w domenie lądowej (2022–2026)

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
2023	Gdynia, Bydgoszcz, Warszawa, Rzeszów (Polska)	Przygotowania do dywersji	Udaremniony	Monitorowanie szlaków transportu uzbrojenia dla Ukrainy, rozpoznawanie infrastruktury krytycznej i baz wojskowych	Siatka szpiegowska licząca 30 osób, 16 z nich zostało zatrzymanych (13 Ukraińców, 2 Białorusinów i 1 Rosjanin)	Wywiad FR	Wyroki od 13 miesięcy do 6 lat pozbawienia wolności	
05-12.2023 r.	Sinimäed Hills, Tallin x2, Mustla i Viljandi (Estonia)	Wandalizm	Zrealizowany	Miejsca pamięci historycznej, samochód MSW i redaktora naczelnego Delfi	13 osób – siatka Allana Hantsoma	Wywiad FR	Kierujący grupą Allen Hantsom został skazany na 6,5 roku więzienia	
03.2023-07.2024	Gdańsk x2, Marki, Radom, Warszawa x2, Łódź (Polska)	Podpalenie	Udaremnione próby w Gdańsku i Łodzi, zrealizowane w Markach, Radomiu i Warszawie	Centra budowlane	9 osób zatrzymanych (Polacy, Ukraińcy i Białorusini); podpalenie w Radomiu zrealizował Kolumbijczyk		Śledztwo	

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
01.2024	Wrocław (Polska)	Podpalenie	Udaremniony	Fabryka chemikaliów znajdująca się w pobliżu infrastruktury strategicznej (bazy paliw) i rzeki Odry	Obywatel Ukrainy	Wywiad FR	Zamknięcie konsulatu FR w Poznaniu	Celem operacji mogło być doprowadzenie do poważnego skażenia środowiska
02.2024	Ryga (Łotwa)	Podpalenie	Udaremniony	Muzeum Okupacji	3 obywateli Łotwy			
03.2024	Wilno (Litwa)	Pobicie polityczne	Zrealizowany	Leonid Wołkow – rosyjski dysydent	2 obywateli Polski	Anatolij Blinow – rosyjski prawnik	Śledztwo	Jest wysoce prawdopodobne, że to rosyjskie służby wywiadowcze były faktycznym inicjatorem tych wydarzeń, jednak prokuratura w Polsce nie uzyskała rozstrzygających dowodów
04.2024	Rzeszów-Jasionka (Polska)	Zabójstwo polityczne	Udaremniony	Prezydent Ukrainy	Paweł K. – obywatel Polski, były żołnierz 2. Hrubieszowskiego Pułku Rozpoznawczego	Wywiad FR	Śledztwo	Sprawca zgłosił gotowość do współpracy z rosyjskim wywiadem i chęć dołączenia do Grupy Wagnera

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
04.2024	Niemcy	Dywersja	Udaremniony	Bazy USA w Bawarii, infrastruktura kolejowa	3 obywateli Niemiec rosyjskiego pochodzenia	Wywiad FR	Śledztwo, podwyższenie stanu alarmowego do poziomu CHARLIE	
05.2024	Wilno (Litwa), Ryga (Łotwa), Warszawa (Polska)	Podpalenie	Zrealizowane w Wilnie, udaremnione w Rydze i Warszawie	Sklepy budowlane	5 osób (w tym obywatele Ukrainy)	Wywiad FR	Śledztwo	Podpalenie sklepu IKEA w Wilnie uznano za zamach terrorystyczny
05.2024	Frankfurt (Niemcy)	Zabójstwo polityczne	Udaremniony	Ukraiński żołnierz	3 osoby zatrzymane (Ormianin, Ukrainiec, Rosjanin)	Wywiad FR	Śledztwo	
05.2024	Warszawa (Polska)	Podpalenie	Zrealizowany	Centrum Handlowe przy ul. Marywilskiej 44	5 osób (w tym obywatele Ukrainy)	Wywiad FR	Zamknięcie konsulatu FR w Krakowie	
07.2024	Düsseldorf (Niemcy)	Zabójstwo polityczne	Udaremniony	Dyrektor wykonawczy firmy Rheinmetall Armin Papperger		Wywiad FR		Udaremniony dzięki współpracy amerykańskich i niemieckich służb wywiadowczych
07.2024	Wola Bykowska (Polska)	Dywersja	Udaremniony	Transport materiałów niebezpiecznych	3 osoby zatrzymane	Wywiad FR	Śledztwo	

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
09.2024	Szawle (Litwa)	Podpalenie	Pierwsza próba udaremniona, druga zrealizowana	Dostawca sprzętu wojskowego TVC Solutions, produkujący mobilne stacje analizy spektrum radiowego	2 obywateli Hiszpanii (w tym 1 z podwójnym obywatelstwem) mieli dokonać pierwszej (nieudanej) próby zamachu. Druga próba (zakończona pożarem) miała być dokonana przez 2 obywateli Rosji i obywatela Białorusi	Wywiad FR	Śledztwo	
10.2024	Wilno (Litwa), Warszawa (Polska), Lipsk (Niemcy), Birmingham (Wielka Brytania)	Zamach terrorystyczny	Przedwczesna detonacja ładunków w centrach logistycznych firm spedycyjnych zdekonspirowała operację	Samoloty cargo obsługujące loty transatlantyckie z Europy do USA i Kanady	15 osób zatrzymanych (obywatele Rosji, Litwy, Łotwy, Estonii i Ukrainy)	Wywiad FR	Śledztwo	Celem operacji było m.in. rozpoznanie szlaków przerzutu materiałów wybuchowych. Nie można wykluczyć zamiaru zamachu na samoloty z użyciem materiałów łatwopalnych

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
10.2024	Ryga (Łotwa)	Podpalenie	Zrealizowany	Przedsiębiorstwo zbrojeniowe, samochody z ukraińskimi tablicami rejestracyjnymi, obiekty IK	4 osoby, co najmniej 2 to obywatele Łotwy	Wywiad FR		
01.2025	Osula i Tallinn (Estonia)	Podpalenie	Zrealizowany	Supermarket i restauracja	2 obywateli Mołdawii	Wywiad FR		
02.2025	Hamburg (Niemcy)	Sabotaż	Zrealizowany	Korweta Emden (F266), budowana w stoczni NVL Blohm + Voss	Obywatel Rumunii i obywatel Grecji	Brak	Śledztwo	W układzie napędowym znaleziono blisko 30 kg metalowych opiłków, które mogły doprowadzić do poważnej awarii silnika. Wykrycie tej ingerencji zapobiegło unieruchomieniu okrętu i znaczącemu opóźnieniu jego przekazania niemieckiej marynarce wojennej
02.2025	Wilhelmshaven (Niemcy)	Sabotaż	Zrealizowany	Fregata Hessen należąca do marynarki wojennej Niemiec	Brak	Brak	Śledztwo	

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
03.2025	Gotlandia (Szwecja)	Dywersja	Zrealizowany	Wodociągi	Brak	Brak	Śledztwo	Uszkodzenie kabli zasilających system pomp
08.2025	Sopot (Polska)	Dywersja	Udaremniony	Wodociągi	Obywatel Ukrainy	Brak	Śledztwo	
04-08.2025	Monasterz i Domostawa (Polska)	Wandalizm	Zrealizowany	Miejsca pamięci dotyczące relacji polsko-ukraińskich	Obywatel Ukrainy	Wywiad FR	Zatrzymanie sprawcy	Podsycanie napięć w relacjach polsko-ukraińskich
06.2025	Erfurt (Niemcy)	Podpalenie	Zrealizowany	6 pojazdów należących do Bundeswehry	Brak	Brak	Śledztwo	
08.2025	Łotwa	Dywersja	Zrealizowany	Infrastruktura kolejowa				Sprawcy podpalili pociąg i stacje kontroli ruchu pociągów. Nagranie ze zdarzenia wykorzystano w celach dezinformacyjnych.
09.2025	Linia kolejowa między Hamburgiem a Berlinem oraz między Kolonią a Düsseldorfem (Niemcy)	Dywersja	Zrealizowany	Infrastruktura kolejowa	Brak	Brak	Śledztwo	
10.2025	Polska i Rumunia	Dywersja	Udaremniony	Siedziba firmy Nova Post w Bukareszcie				Przechwycenie materiałów wybuchowych

DATA	MIEJSCE	ATAK	STATUS	SPECYFIKACJA CELU	SPRAWCY	ATRYBUCJA	ODPOWIEDŹ	DODATKOWE INFORMACJE
11.2025	Mika i Gołąb (Polska)	Dywersja	Zrealizowany	Linia kolejowa nr 7 między Warszawą a Dorohuskiem o strategicznym znaczeniu dla transportów pomocy humanitarnej i wojskowej dla Ukrainy	2 obywateli Ukrainy	Wywiad FR	Zamknięcie konsulatu FR w Gdańsku	
01.2026	Essen (Niemcy)	Dywersja	Zrealizowany	Pociąg towarowy przewożący substancje niebezpieczne	Brak	Brak	Śledztwo	Wykolejenie pociągu wymusiło zmianę trasy pociągu transportującego amunicję dla sił USA w Europie

Źródło: badania własne.

Domena powietrzna

Tabela 3

Zidentyfikowane przekroczenia granicy powietrznej

DATA	PAŃSTWO	MIEJSCE	TYP OBIEKTU
02.03.2022	Szwecja	Gotlandia	2x Su-24, 2x Su-27
29.04.2022	Szwecja	Blekinge	An-30
17.06.2022	Dania	Bornholm	KA-31/KA-27
18.08.2022	Finlandia	Porvoo	2x MiG-31
16.12.2022	Polska	Bydgoszcz	pocisk Ch-55
12.05.2023	Estonia	Vaindloo	myśliwiec
01.08.2023	Polska	Białowieża	2x śmigłowce (Mi-24/8)
24.03.2024	Polska	Osera	pocisk manewrujący
14.06.2024	Szwecja	Gotlandia	Su-24
07.09.2024	Łotwa	Rzeżyca	dron Shahed
11.02.2025	Polska	Rejon Ustki (Bałtyk)	Su-24
25.04.2025	Polska	Mierzeja Wiślana	śmigłowiec Ka-27
22.06.2025	Estonia	Vaindloo	Il-76
20.08.2025	Polska	Mazury (rejon jeziora Mamry)	dron Orlan-10
09.09.2025	Polska	granica wschodnia	19x UAV
19.09.2025	Estonia	Tallinn / Zatoka Fińska	3x MiG-31
23.10.2025	Litwa	Korytarz Suwalski / Granica	Il-76MD (Eskorta Su-30SM)
24.11.2025	Estonia	Vaindloo / Zatoka Fińska	Tu-134 & 2x Su-30SM
01.01.2026	Estonia	Vaindloo / Tallinn	3x MiG-31BM
18.03.2026	Estonia	Wyspa Vaindloo	Su-30
25.03.2026	Estonia	Auvere (koło Narwy)	dron (UAV)

Źródło: opracowanie własne.

Tabela 4

Przechwycenia w międzynarodowej przestrzeni powietrznej

PAŃSTWO (BAZA)	DATA	REJON	TYP OBIEKTU	PRZECHWY-CENIE
Litwa (Szawle)	19.12.2022	Bałtyk	An-26 & 2x Su-24M	1
Dania	01.04.2023	Bornholm	Il-20	1
Norwegia	23.08.2023	Daleka Północ	Tu-95 & Su-33	1
Polska (Malbork)	25.04.2025	Bałtyk	Il-20M & 2x Su-30SM	1
Norwegia (Evenes)	12.02.2026	M. Norweskie	2x Tu-160	1
Norwegia	10.03.2026	Wybrzeże Finnmarku	Il-20M	1
Norwegia	11.03.2026	Lofoty / Vesteralen	Il-20M	1
Litwa (Szawle)	18.03.2026	Bałtyk	2x Su-30SM	1
Finlandia	22.03.2026	Wyspy Alandzkie (ADIZ)	Il-20M	1

Źródło: opracowanie własne na podstawie materiałów prasowych.

Polski Instytut Spraw Międzynarodowych (PISM) jest jednym z najważniejszych i największych ośrodków analitycznych w Europie Środkowej i Wschodniej. Sytuując się pomiędzy światem polityki a niezależną analizą, PISM zapewnia wsparcie decydentom i dyplomatom, inicjuje publiczną debatę ekspercką oraz upowszechnia wiedzę o współczesnych stosunkach międzynarodowych. Działalności PISM przyświeca przekonanie, że proces podejmowania decyzji na arenie międzynarodowej powinien się opierać w jak największym stopniu na wiedzy płynącej z rzetelnych i wiarygodnych badań.

Polski Instytut Spraw Międzynarodowych
The Polish Institute of International Affairs
ul. Warecka 1A
00-950 Warszawa
tel. (+48) 22 556 80 00
pism@pism.pl
www.pism.pl

ISBN 978-83-68555-31-8
e-ISBN 978-83-68555-32-5