Przegląd Bezpieczeństwa Wewnętrznego
2025, nr 32, s. 233–249

https://doi.org/10.4467/20801335PBW.25.011.22177

VARIA

Ochrona polskich obszarów morskich w teorii i praktyce

Duże tempo zmian w środowisku bezpieczeństwa powoduje, że konieczna jest szybka adaptacja do nowych wyzwań. Dotyczy to także domeny morskiej. Jakie są rzeczywiste i potencjalne zagrożenia w tym obszarze dla Rzeczypospolitej Polskiej? Co należy zrobić, by w sposób bardziej efektywny im przeciwdziałać? Jak zabezpieczać obiekty strategiczne usytuowane w polskich obszarach morskich? Na te pytania odpowiada **kmdr ppor. rez. Sebastian Kalitowski**, starszy oficer Marynarki Wojennej, były dowódca grupy specjalnej płetwonurków w Jednostce Wojskowej Formoza i oficer operacyjny wywiadu wojskowego. Pasjonat morza i ekspert w dziedzinie bezpieczeństwa morskiego. Doradza, uczy i dzieli się swoim bogatym doświadczeniem w ramach szkoleń i kursów, które organizuje i prowadzi wraz ze swoim zespołem profesjonalistów w pierwszej w Polsce i jednej z pierwszych w Europie firm z branży *maritime security*. Celem jest rzetelne przygotowanie specjalistów z zakresu ochrony obiektów portowych, morskiej infrastruktury krytycznej, morskich farm wiatrowych i statków.

Daria Olender: Panie Komandorze, czy we współczesnym środowisku morskim jest coś, co Pana zaskakuje?

Kmdr ppor. rez. Sebastian Kalitowski: Sytuacja geopolityczna i poziom zagrożeń na świecie w ostatnich dwóch latach znacznie się zmieniły. Nie należy zatem oczekiwać, że pozostanie to bez wpływu na globalną architekturę bezpieczeństwa morskiego. Długo wydawało się, że zagrożenia asymetryczne na morzu są właściwie rozpoznane i zdefiniowane – że mamy problemy z piractwem, terroryzmem, nielegalną imigracją, pasażerami na gapę, przemytem narkotyków, nielegalnymi połowami czy z cyberterroryzmem. Pojawiły się jednak nowe, np. wynikające z zakłócania sygnału GPS, wykorzystania statków z floty cieni oraz platform bezzałogowych. Wiele się zmieniło w związku z rozpoczętymi w 2023 r. działaniami Huti wymierzonymi w żeglugę międzynarodową, początkowo głównie w statki powiązane z Izraelem, co miało być wyrazem solidarności jemeńskich rebeliantów z Palestyną. Aktywność Huti próbują wykorzystać somalijscy piraci, którzy zwiększyli liczbę ataków w tym rejonie. Mam wrażenie, a wywiadem morskim i analizą bezpieczeństwa morskiego zajmuję się od 2007 r., że wszystko znacznie przyspieszyło w tym obszarze. To powoduje, że rozpoznanie zagrożeń i poszukiwanie skutecznych rozwiązań mitygujących ryzyko jest dużym wyzwaniem.

Jak ocenia Pan sytuację na Morzu Bałtyckim?

Bałtyk od 2023 r. stał się obszarem wysokiego ryzyka obok Morza Czarnego, Morza Czerwonego, Basenu Somalijskiego, zatok Perskiej i Omańskiej, Morza Południowochińskiego czy Zatoki Gwinejskiej. Obserwujemy na nim zwiększenie aktywności wywiadowczej, mapowanie dna przy morskiej infrastrukturze krytycznej (IK), sabotaże związane ze zrywaniem kabli podmorskich, sabotaże kinetyczne i niekinetyczne, zakłócenia systemu GNSS[1]. Rosja prowadzi na tym akwenie „wojnę cieni" wymierzoną w państwa Zachodu i NATO. Nie powinno to dziwić, bo przygotowywała się do niej od dziesięcioleci. Sporządzała m.in. matryce potencjalnych celów na morzu, ze świadomością, jak podatna na sabotaż i dywersję jest podwodna IK i jak wiele można osiągnąć,

[1] GNSS (ang. *Global Navigation Satellite System*) – Globalny System Nawigacji Satelitarnej. Wszystkie przypisy pochodzą od redakcji.

gdy zastosuje się środki poniżej progu wojny, ogólnodostępne i tanie. Do działań sabotażowych Rosjanie wykorzystują statki floty handlowej, aby nie można było uruchomić artykułu 5 traktatu północnoatlantyckiego. Wiedzą też, że takim działaniom niełatwo przypisać atrybucję i można wiarygodnie zaprzeczać sprawstwu. Jeśli w ciągu roku dochodzi średnio do ok. 200 uszkodzeń kabli podmorskich przez statki, które wloką kotwicę po dnie głównie z powodu ludzkich zaniedbań czy błędów, to trudno udowodnić umyślność takich działań. Wykorzystanie statków do sabotażu i dywersji jest znacznie tańsze niż użycie okrętów. Nie wspomnę już o maskowaniu i monitorowaniu. Rosjanie wiedzą, że są stale obserwowani przez siły NATO. Co ciekawe, stanowiska dowodzenia, okręty i jednostki Floty Bałtyckiej od września ubiegłego roku przeszły na systemy łączności *command and control communications* (C3), w paśmie VLF-SHF[2], których Rosjanie używają w czasie wojny. Wcześniej korzystali z nich podczas zimnej wojny.

Czy uprawnione jest stwierdzenie, że aktualna sytuacja w obszarze bezpieczeństwa morskiego to coś, z czym nie mieliśmy do czynienia od niemal 20 lat?

Tak, to prawda. Z podobną skalą zagrożeń mieliśmy do czynienia ok. 2008 r., kiedy doszło do nasilenia się piractwa w rejonie Rogu Afryki. Apogeum nastąpiło w 2010 r., gdy odnotowano 45 ataków na świecie, a 53 statki z 1174 marynarzami uprowadzono na wiele miesięcy dla okupu. Pomimo działań międzynarodowych i rozpoczęcia misji „Atalanta"[3], a także obecności kilku grup zadaniowych złożonych z okrętów przez wiele lat nie potrafiliśmy sobie poradzić z zagrożeniem w tym rejonie. Okazało się, że zwiększenie obecności marynarki wojennej nie rozwiązuje tego złożonego problemu. Wymierne efekty dało dopiero stworzenie systemu wielu współgrających elementów i przestrzeganie określonych zasad przez załogi statków.

[2] VLF (ang. *very low frequency*) – fale radiowe bardzo długie, o częstotliwości od 3 do 30 kHz, co odpowiada długości od 10 do 100 km. SHF (ang. *super high frequency*) – fale radiowe superkrótkie, o częstotliwości od 3 do 30 GHz i długości od 1 do 10 cm.

[3] European Union Naval Force Somalia – Operation Atalanta to wojskowa operacja morska Unii Europejskiej służąca zwiększeniu bezpieczeństwa w zachodniej części Oceanu Indyjskiego i na Morzu Czerwonym. Cele tej operacji to m.in.: ochrona transportów pomocy humanitarnej World Food Programme dla Somalii, eskortowanie okrętów z zaopatrzeniem dla sił operacji „Amisom" oraz udzielanie pomocy okrętom zaatakowanym przez piratów.

> **W kontekście Rogu Afryki dotknął Pan ważnej kwestii. Skuteczność wdrażanych rozwiązań w dużym stopniu zależy od odpowiedniego poziomu świadomości, przekonania o słuszności podjętych działań i zdyscyplinowania podczas ich realizacji.**

Te czynniki to fundament bezpieczeństwa. Świadomość sytuacyjna, przygotowanie członków załóg do incydentu ataku, stworzenie panic roomu zwanego na statkach cytadelą, ochrona pasywna oraz szersze wprowadzenie uzbrojonej ochrony – to elementy, które pozwoliły powstrzymać falę piractwa w Rogu Afryki. Moim zdaniem udało się to zrobić głównie dzięki działaniom prywatnych dostawców usług z zakresu bezpieczeństwa.

Na Bałtyku dobrze widać, jak Rosjanie wykorzystują to, że w krajach Zachodu brakuje świadomości dotyczącej działań hybrydowych. Dotychczas rozpoznawano i monitorowano okręty i siły Floty Bałtyckiej. Obecnie jednak Rosja posługuje się – jak już wspomniałem – statkami, a nie okrętami i siłami tej floty. W 2023 r. w ramach dziennikarskiego śledztwa niemieckich nadawców publicznych NDR i WDR oraz dziennika „Süddeutsche Zeitung" monitorowano rejsy rosyjskich statków badawczych, które według oficjalnej wersji prowadziły badania hydrograficzne na Bałtyku i Morzu Północnym. Na 400 przeanalizowanych rejsów w co najmniej 60 przypadkach stwierdzono operowanie statków w podejrzanie bliskiej odległości od obiektów IK. Jako przykład przywołam incydent z 17 maja 2025 r. Statek MV Sun z rosyjskiej floty cieni pływał w okolicach podwodnego kabla energetycznego SwePol Link. Zachowywał się, jakby chciał go zerwać za pomocą wleczonej kotwicy. Polska wysłała 20 maja w tamten rejon samolot patrolowo-rozpoznawczy M28B Bryza, a dzień później – okręt. Do momentu przybycia samolotu rosyjski tankowiec miał jednak dużo czasu nie tylko na sabotaż, lecz także na swobodne oddalenie się z miejsca działań. Na szczęście tym razem nie chodziło o zerwanie kabla, lecz o przetestowanie naszej gotowości do identyfikacji zagrożeń. Czego zabrakło po naszej stronie? Świadomości? Działań wywiadu morskiego, który powinien monitorować statki rosyjskiej floty cieni, przynajmmniej te poruszające się po polskiej wyłącznej strefie ekonomicznej (WSE), nie wspominając już o wodach terytorialnych? Powinniśmy wiedzieć, że statek określany w terminologii bezpieczeństwa morskiego jako „czerwona flaga" pojawił się w okolicach SwePol Link. Istnieje kilka, niestety bardzo drogich, narzędzi do monitorowania. Jedno z nich pozwala typować i śledzić podejrzane, nieintuicyjnie zachowujące

się jednostki, zmieniające nazwy i banderę, podszywające się pod statki, które już dawno zostały zezłomowane, czy wyłączające lub manipulujące nadajnikami AIS, czyli systemami automatycznej identyfikacji.

Powróćmy do problemu ewoluowania zagrożeń na morzu, wynikającego m.in. z wykorzystywania nowych technologii. Huti do atakowania statków używali np. dronów.

Gdy w 2021 r. doszło do ataku na tankowiec MT Mercer Street, który był pierwszym śmiertelnym atakiem terrorystycznym na statek przeprowadzonym z wykorzystaniem UAV[4], świat poznał kolejne zagrożenie. Zginęło wówczas dwóch członków załogi. Analizowaliśmy ten przypadek w Maritime Safety & Security, ale nie sądziliśmy, że tego typu ataki staną się tak powszechne i dwa lata później sparaliżują ruch na Morzu Czerwonym, Morzu Arabskim i w cieśninie Bab al-Mandab. Huti używali rakiet balistycznych i właśnie dronów, w tym dronów pływających. Działo się to na jednym z najważniejszych szlaków żeglugowych na świecie. Od rozpoczęcia patroli morskich w regionie w ramach operacji „Prosperity Guardian" i „Aspides" siły morskie Unii Europejskiej i brytyjska marynarka wojenna przechwyciły łącznie 32 bezzałogowe statki powietrzne, dwa drony pływające, a nawet jeden dron podwodny. Zniszczono również setki dronów typu Shahed, rakiet balistycznych i pocisków przeciwokrętowych.

Drony stały się istotnym elementem działań na morzu również podczas wojny rosyjsko-ukraińskiej.

To prawda, drony nawodne i podwodne są częścią działań asymetrycznych na Morzu Czarnym, a Ukraińcy dzięki nim skutecznie walczą ze znacznie silniejszymi siłami morskimi Federacji Rosyjskiej. Co więcej, wykorzystują te drony jako platformy do startów dronów latających FPV[5], a po uzbrojeniu skutecznie niszczą nimi cele powietrzne. Przykładowo, 2 maja 2025 r. w pobliżu Noworosyjska ukraiński dron morski zniszczył rosyjski samolot myśliwski Su-30. To był pierwszy w historii

[4] UAV (ang. *unmanned aerial vehicle*) – bezzałogowy statek powietrzny.

[5] FPV (ang. *first person view*, dosłownie: widok z pierwszej osoby) – to sposób sterowania dronem, w którym pilot widzi na żywo obraz przekazywany z drona.

wojen morskich przypadek, gdy dron pływający zniszczył nie jednostkę nawodną czy śmigłowiec przeciwnika, lecz samolot myśliwski.

Doświadczenia z działań wojennych na Morzu Czarnym pokazują, że platformę bezzałogową można dziś zbudować niemalże w warunkach garażowych, stworzyć ją na bazie skutera wodnego. Sterowana za pomocą łączności satelitarnej może wykonywać komendy operatora odległego nawet o 1000 km. W ten sposób Ukraińcy pozbawili Rosjan panowania na tym morzu. Koronnym przykładem schyłku teorii wojny morskiej adm. Alfreda Thayera Mahana[6] jest zniszczenie flagowego okrętu rosyjskiej Floty Czarnomorskiej – fregaty projektu 11356M Moskwa. Prawdopodobnie ta akcja będzie omawiana w uczelniach wojskowych i morskich. Rosja, widząc skuteczność ukraińskich dronów Sea Baby, Mamai, Magura, Magura V, Sea Baby II Awdijiwka oraz działań Huti na Morzu Czerwonym, również opracowała swoje bezzałogowe pojazdy nawodne. W ubiegłym roku Zakład Budowy Maszyn Kingisepp w Sankt Petersburgu zaprezentował pojazd o nazwie Oduvanchik. Dzięki możliwości przewożenia ładunku o masie do 600 kg stanowi on elastyczną platformę do realizacji misji o różnym charakterze. Rosjanie dysponują swoimi konstrukcjami dronów morskich: Riverine, Dandelion, Sargol.

Morskie farmy wiatrowe i inne obiekty morskiej IK mogą być atakowane tanimi improwizowanymi środkami bojowymi, takimi jak drony rekreacyjne FPV, których koszt produkcji i przygotowania do działań bojowych wynosi mniej niż 1000 euro. W konflikcie rosyjsko-ukraińskim są wykorzystywane tysiące takich dronów, także do ataków na instalacje energetyczne w Ukrainie i Rosji. Detonacja półtorakilogramowej bomby termobarycznej, wartej 1500 euro, może skutecznie przebić stalowy pancerz o grubości 40 mm. Lepiej znany ukraiński dron – AQ-400 Scythe wydaje się zbudowany głównie z drewna. Jego podawany zasięg to 750 km, ma on zdolność przenoszenia 32-kilogramowej głowicy bojowej. Koszt jednostkowy tych dronów stanowi ułamek ceny irańskich dronów Shahed, dostarczanych Rosji po 375 000 dolarów za sztukę.

[6] Alfred Thayer Mahan – amerykański oficer marynarki wojennej uważany za jednego z najwybitniejszych teoretyków strategii morskiej, zwany Clausewitzem wojny morskiej. Teoria wojny morskiej (doktryna Mahana) zakłada, że potęga morska stanowi klucz do sukcesu państwa zarówno w sferze gospodarczej, jak i militarnej. Najlepszym sposobem ochrony nowoczesnej floty handlowej jest budowa równie nowoczesnej floty wojennej. Dopiero połączenie tych flot decyduje o potędze państwa. Kraje pozbawione silnych flot nie rozwijają się cywilizacyjnie i ekonomicznie, co prowadzi do ich upadku.

Nie zapominajmy, że w ramach działań podprogowych Rosja może zaatakować za pomocą dronów również obiekty IK należące do Polski. Skuteczność, niskie koszty produkcji i trudności z jednoznaczną identyfikacją sprawców w przypadku ich wykorzystania do ataku czynią je idealną bronią nie tylko dla terrorystów, lecz także dla podmiotów państwowych prowadzących działania hybrydowe. W tym kontekście nasuwa mi się smutna refleksja dotycząca niedoceniania w Polsce znaczenia bezpieczeństwa morskiego. To nie tylko zaniedbywana i niedoinwestowana Marynarka Wojenna, lecz także zaprzepaszczenie rozwiązań w zakresie bezpieczeństwa, którymi kiedyś dysponowaliśmy. Niewiele osób wie, że w 2011 r. Akademia Marynarki Wojennej wraz z producentem łodzi Sportis zrealizowali projekt budowy bezzałogowej jednostki nawodnej o nazwie Edredon, przeznaczonej do wykorzystania w celach militarnych oraz do zabezpieczania morskiej IK przed atakami terrorystycznymi. Ten projekt był innowacją na skalę światową. Edredon był sterowany za pomocą fal radiowych, ale dziś można byłoby to bez problemu zmienić. Centrum Techniki Morskiej w Gdyni opracowało z kolei system Kryl. Reagował on na zagrożenia ze strony nurków, małych okrętów podwodnych oraz jednostek nawodnych. Niestety, prace badawczo-naukowe prowadzone w ramach obu tych projektów, wiążące się nie tylko z wysiłkiem naukowców, lecz także z dużymi nakładami finansowymi, nie zostały właściwie wykorzystane.

> **Może wprowadzane regulacje prawne przyniosą pozytywne zmiany w sektorze szeroko rozumianej ochrony. W Polsce doczekaliśmy się ustawy o ochronie ludności i obronie cywilnej, w toku nowelizacja ustawy o zarządzaniu kryzysowym. W tle mamy unijne dyrektywy: CER i NIS 2, rozporządzenie DORA[7]. Jak to się ma, Pana zdaniem, do ochrony morskiej i portowej infrastruktury krytycznej w naszym kraju?**

Ochrona od strony morza obiektów IK była podyktowana dotychczas głównie wymaganiami wynikającymi z międzynarodowego kodeksu

[7] CER – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych; NIS 2 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/255 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE; DORA – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego.

ISPS[8] oraz krajowymi przepisami będącymi odzwierciedleniem jego zapisów, tj. *Ustawą z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich*. Celem ISPS jest zwiększenie zabezpieczenia żeglugi i portów przed aktami przestępczości kryminalnej, piractwem i terroryzmem. Niestety, ten kodeks w niewielkim stopniu odpowiada na aktualne zagrożenia w domenie morskiej. Na przykład dzisiejsze środki bojowe wykorzystywane przez podmioty państwowe są znacznie bardziej zaawansowane i rozwinięte niż te, którymi dysponowali terroryści z Al-Kaidy czy ISIS. Kodeks ISPS nie nakładał na obiekt IK obowiązku ochrony od strony morza. W związku z tym na niektórych obiektach w Polsce nie było i nie ma takiej ochrony. Nie wspominając już o zabezpieczeniu podwodnym. Spełniano jedynie minimalne wymagania wynikające z ISPS i polskich przepisów prawnych. Co z tego, że na jednym z obiektów kończymy po wielu latach działania związane z uruchomieniem systemu identyfikacji zagrożeń w dolnej półsferze, skoro nawet jeśli odkryjemy pod wodą obecność płetwonurka dywersanta, to niewiele będziemy mogli z tą informacją zrobić. Pominę fakt, że prawdopodobieństwo przeprowadzenia ataku w ten sposób maleje w dobie możliwości wykorzystania platform autonomicznych. Po co wysyłać płetwonurków, którzy będą w stanie przenieść kilka kilogramów materiału wybuchowego w minach limpet, skoro prościej i skuteczniej skorzystać z drona z 400-kilogramową głowicą bojową, bo tyle mogły przenosić pierwsze ukraińskie drony Sea Baby. Dzisiaj, jak deklarują Ukraińcy, mogą one przenieść nawet do 1000 kg materiałów wybuchowych. Ostatnio wykorzystali oni, do kolejnej próby uszkodzenia mostu Krymskiego, drona UUV[9] Mariczka, który może przenieść ponad tonę ładunku wybuchowego. Inny ukraiński dron, TLK 150, przenoszący 150 kg ładunku wybuchowego, może być wodowany z jachtu czy motorówki, co umożliwia jego skryte wykorzystanie. Systemy detekcji podwodnej na naszych obiektach morskiej IK należało zatem mieć wiele lat temu i są podmioty, które o to zadbały. Myślenie, że wszystkie nasze obiekty morskiej IK są dziś w stanie sprostać wyzwaniom w sferze ochrony, oznacza brak świadomości. Przy obecnej taktyce użycia środków bojowych, nawet tych wykorzystywanych poniżej progu wojny, nie jesteśmy w stanie zabezpieczyć tych obiektów w stu procentach.

[8] International Ship and Port Facility Security Code (pol. Międzynarodowy Kodeks Ochrony Statku i Obiektu Portowego) powstał w 2002 r. w następstwie ataków terrorystycznych z 11 września 2001 r. Zaczął obowiązywać od 1 lipca 2004 r.

[9] UUV (ang. *unmanned underwater vehicle*) – bezzałogowy pojazd podwodny.

Budujmy jednak sensowne elementy ochrony warstwowej, które zmniejszą podatność na ataki, zamiast stosować półśrodki.

> **Trudno nie dostrzec analogii do trwających wiele lat działań związanych z zabezpieczeniem obiektów przed bezzałogowymi statkami powietrznymi.**

Przez długi czas myśleliśmy, że problem rozwiążą tabliczki z zakazami wchodzenia i lotów umieszczane przy takich obiektach. Niestety, nawet systemy przeciwdronowe do zakłócania częstotliwości pracy tych urządzeń mogą być nieskuteczne. Pokazują to doświadczenia w Ukrainie, gdzie drony atakują w roju, a częstotliwości pracy są zmieniane w czasie lotu albo dronami steruje się za pomocą kabli światłowodowych kupowanych za grosze na chińskich portalach aukcyjnych. Ta wojna daje nam najlepszą możliwość wglądu w taktykę rosyjskich działań. Do identyfikacji i prognozowania możliwości ataku z wykorzystaniem UAV niezbędne są wiedza i doświadczenie operatorów FPV. W ten sposób można myśleć o systemie doboru środków do ochrony warstwowej obiektów morskich.

Ochrona obszaru morskiego państwa przed zagrożeniami asymetrycznymi przez wiele lat była traktowana marginesowo. Zdarza się, że za bezpieczeństwo ważnych obiektów odpowiadają osoby bez odpowiedniej wiedzy i przygotowania. Wieloletnia polityka kadrowa promująca, także w sektorze bezpieczeństwa, ludzi z klucza partyjnego i mających koneksje, a już niekoniecznie wiedzę specjalistyczną, odcisnęła swoje piętno. Przerzucanie się zakresem odpowiedzialności, niedostatek profesjonalistów, brak znajomości aktualnej wywiadowczej analizy zagrożeń i niechęć do uczenia się oraz wyciągania wniosków prowadzą do tak nielogicznych działań, jak chociażby 200-metrowa strefa zakazu zbliżania się do jednego z naszych najważniejszych obiektów morskiej IK. Według mnie jest to jedynie próba przeniesienia popularnych rozwiązań ze wschodniej granicy kraju na grunt obiektu, który będzie atakowany w inny sposób niż przez wtargnięcie migrantów o nieuregulowanym statusie. Takie nieadekwatne do realnych zagrożeń działania dają jedynie złudne poczucie bezpieczeństwa.

Zdarzenia z ostatnich lat pokazały, jak mocno narażone na działania hybrydowe są instalacje morskie na Bałtyku i jak ważne jest wzmocnienie ich ochrony.

Od czasu rosyjskiej inwazji na Ukrainę na Morzu Bałtyckim dochodzi do wielu działań hybrydowych, o które oskarża się Federację Rosyjską. Uszkodzone zostały m.in. gazociągi Nord Stream, Nord Stream 2 i Balticconnector, a od października 2023 r. – co najmniej 11 kabli podmorskich. Naprawę Balticconnectora, uszkodzonego przez chiński statek MV Newnew Polar Bear, oszacowano na 35 mln euro, a kabla energetycznego EstLink2 – na ok. 60 mln euro. Inny chiński statek MV Yi Peng 3 uszkodził na Bałtyku kable optyczne C-Lion 1 i BCS East-West Interlink. Początkowo postrzegałem te zdarzenia jako wspólne działania Chin i Rosji, ale ze względu na możliwe tarcia między tymi krajami częściowo weryfikuję swój punkt widzenia. Twierdzenie przez rosyjską Federalną Służbę Bezpieczeństwa czy Służbę Wywiadu Zagranicznego, że postrzega chińskie Ministerstwo Bezpieczeństwa Państwowego jako wroga, i oskarżanie Chin o rekrutację rosyjskich naukowców, aby zdobywać informacje na temat rosyjskiej technologii wojskowej, badań arktycznych i technologii podwójnego zastosowania, nie wydają się dobrą płaszczyzną do współpracy wywiadowczej przy działaniach sabotażowych. Wzajemną nieufność potęguje też prowadzenie przez Chińczyków silnego wywiadu przeciwko Rosji. Jest bardzo prawdopodobne, że Chińczycy mają swój wkład w sabotaże IK na Bałtyku, tym bardziej że często stosują takie działania na Morzu Północnochińskim przeciwko Tajwanowi.

Warto dodać, że obecne działania Rosji w rejonie Bałtyku są kontynuacją wielu lat pracy rosyjskich służb wywiadowczych i powstałego w 1965 r. Głównego Zarządu Badań Głębinowych. GUGI to wyspecjalizowana służba, która nie jest częścią regularnej rosyjskiej marynarki wojennej, ale podlega bezpośrednio Ministerstwu Obrony jako organizacja wywiadowcza i zaangażowana w misje specjalne. Rosjanie od dawna mapowali morskie farmy wiatrowe, gazociągi, kable energetyczne i internetowe na wodach wokół Danii, Norwegii, Finlandii, Szwecji i Polski. Na podstawie źródeł otwartych zidentyfikowano 50 statków, które przez ostatnie 10 lat mogły prowadzić na Bałtyku i Morzu Północnym operacje wywiadowcze na rzecz Rosji. Państwo to od wielu lat uprawia agresywną politykę, do czego wykorzystuje działania hybrydowe, asymetryczne i dezinformację. Po fazie zbierania informacji przez statki badawcze

GUGI: Yantar i Admirał Władimirski oraz statki z floty cieni, które przez ostatnie lata zatrzymywały się nawet na kilkanaście dni niedaleko podmorskich kabli energetycznych i telekomunikacyjnych, weszliśmy w fazę testowania i nękania.

Jaki to ma związek z inwestycjami w regionie Morza Bałtyckiego planowanymi przez Polskę?

Rejon, w którym powstaną nasze morskie farmy wiatrowe, również mógł zostać rozpoznany przez Federację Rosyjską. Od września 2022 r. do kwietnia 2023 r. dwa statki MV WL Totma oraz MV WL Kirillov kotwiczyły na wodach polskiej WSE, tuż za pasem morza terytorialnego, w odległości 12,623 mil morskich od linii brzegowej na wysokości Dębek. Kotwiczyły na obszarze, który zamknięty w wielobok pokrywa powierzchnię 24 364 km^2. Jeśli skanowały dno, to taki obszar mogły zeskanować w rejonie, gdzie powstaną nasze morskie farmy wiatrowe i planuje się położenie kabla podwodnego. Oba statki pływające pod banderą Panamy należą do cypryjskiego armatora White Lake Shipping. W zarządzie tej firmy są Rosjanie, stanowią oni także większość kadry kierowniczej. W sierpniu 2022 r. White Lake Shipping, przez swoją firmę zależną Gravelor Shipping Line, zakupiło kilka statków, m.in. dwa wymienione, od rosyjskich państwowych firm leasingowych GTLK Asia M5 Limited i GTLK Asia M6 Limited, które są objęte unijnymi i amerykańskimi sankcjami. W czasie kotwiczenia w rejonie planowanej lokalizacji polskich morskich farm wiatrowych oba statki wyłączały – niezgodnie z prawem i konwencją SOLAS[10] – nadajniki AIS. Na tych nadajnikach miały zadeklarowany status „w oczekiwaniu na zlecenie". Co jakiś czas jednostki te płynęły do portu w Bałtijsku i wracały do polskiej WSE, aby rzucić kotwice w miejscu, gdzie nie ma żadnego kotwicowiska, i czekać ok. 13 mil morskich od brzegu na kolejne zlecenie. W ciągu siedmiu miesięcy powtórzyły te operacje kilka razy. Według mnie najbardziej logicznym wytłumaczeniem ich obecności jest mapowanie dna. Gdyby prowadziły obserwację, to postój w niewielkiej odległości od siebie byłby bez sensu. Jeśli ze względów politycznych Polska nie chciała skorzystać z prawa do wizyty na tych statkach, to na czas ich pobytu w naszej

[10] International Convention for the Safety of Life at Sea (pol. Międzynarodowa konwencja o bezpieczeństwie życia na morzu) z 1974 r.

WSE należało postawić przy nich jednostkę, jeśli nie Straży Granicznej czy Marynarki Wojennej, to chociaż Urzędu Morskiego, i monitorować je, zwłaszcza że były to statki państwa wrogo nastawionego do Polski. Nieskuteczne działania ze strony służb państwa, ograniczające się do lotów rozpoznawczych samolotem Bryza czy okazjonalnego patrolowania przez jednostkę Straży Granicznej rejonu kotwiczenia statków, to w mojej ocenie poważny błąd, który umożliwił Rosjanom zdobycie istotnych informacji wywiadowczych.

Czy jako były płetwonurek bojowy przygotowywany do działań dywersyjnych na morzu uważa Pan, że na Bałtyku istnieje zagrożenie również z ich strony?

Chociaż dziś znaczenie płetwonurków dywersantów może wydawać się mniejsze w kontekście wykorzystania platform bezzałogowych, to nadal mogą oni stanowić poważne zagrożenie. Wystarczy przypomnieć ataki na Nord Stream 1 i Nord Stream 2. Jedna z trzech hipotez mówi, że nitki rurociągów zostały zniszczone przez ukraińskich płetwonurków, którymi dowodził pułkownik Służby Bezpieczeństwa Ukrainy. Od lutego 2025 r. na Morzu Śródziemnym doszło do uszkodzeń czterech statków rosyjskiej floty cieni: MV Grace Ferrum, MV Seacharm, MV Seajewel oraz MV Vilamoura. Z charakteru uszkodzeń wynika, że zostały zaatakowane za pomocą min limpet. Wszystko wskazuje na to, że były to działania ukraińskich płetwonurków bojowych.

Dziś o siłach specjalnych Federacji Rosyjskiej nieco zapomnieliśmy. Na Bałtyku rolę pierwszoplanową powierzyła ona statkom handlowym i jednostkom badawczym GUGI. Obawiam się, że to celowe działanie psychologiczne ze strony Rosjan. Chodzi im o to, aby skupić uwagę państw NATO na działaniach hybrydowych i skłonić je do zaangażowania sił wojskowych w ochronę, czyli sił, które mogłyby stawić czoła ewentualnym regularnym działaniom bojowym przeciwnika. To kolejne z potencjalnych zagrożeń asymetrycznych. Płetwonurkowie rosyjskiego Specnazu są rozmieszczeni w Obwodzie Królewieckim w strukturach 390 Punktu Rozpoznawczego Specjalnego Przeznaczenia Floty Bałtyckiej (JW nr 43104) w mieście Parusnoje. Dysponują m.in. nowoczesnymi skuterami podwodnymi Black Shadow, zakupionymi od niemieckiej firmy Rotinor. Te praktycznie niewykrywalne skutery umożliwiają poruszanie się z prędkością ok. 7 węzłów na głębokości do 60 m

i pokonywanie dystansu do 50 km. Pozwala to wejść do rejonu działania spoza morza terytorialnego wynoszącego 12 mil morskich. Siły Specnazu, jak większość pododdziałów specjalnych, są wręcz stworzone do działań hybrydowych i mogą je realizować na Morzu Bałtyckim i w państwach regionu.

Jakie działania ma Pan na myśli?

Rozpoznanie obiektów morskiej IK i prowadzenie wobec nich działań dywersyjnych, w tym pod fałszywą flagą, podsłuch, niszczenie podwodnych kabli komunikacyjnych i sieci energetycznych, porywanie wartościowych celów i osób w rejonie wybrzeża. To wszystko się wpisuje w działania zgodne z doktryną Gierasimowa i jest elementem wojny podprogowej, która na każdym etapie może się przerodzić w otwarty konflikt.

Porozmawiajmy o rosyjskich działaniach wywiadowczych w Polsce wymierzonych w sektor morski. Pominę analizę i ocenę podatności z obszaru bezpieczeństwa osobowego, bo to temat na osobny wywiad.

Rosjanie zdobywają informacje na temat każdego interesującego ich obiektu jeszcze przed rozpoczęciem inwestycji. Warto wspomnieć, że w 2014 r. skazano obywatela RP, który od 2012 r. wykonywał zadania wywiadowcze – pozyskiwał informacje o Gazoporcie w Świnoujściu i osobach w nim zatrudnionych, brał udział w posiedzeniach sejmowej komisji ds. energetyki. Aby zobrazować skuteczność i rozmach działania rosyjskiego wywiadu w zdobywaniu informacji o polskich obiektach strategicznych, należy przypomnieć, że Gazoport w Świnoujściu został otwarty w 2015 r., a pierwszy gazowiec wpłynął do niego 11 grudnia 2015 r. Agent został więc aresztowany na długo przed otwarciem portu. W przypadku naszej nowej strategicznej inwestycji związanej z morskimi farmami wiatrowymi na Bałtyku Rosjanie pokazali, jak skutecznie pracują wywiadowczo. Zmapowali dno morskie, na którym zostaną one usadowione, i to jeszcze przed ostatecznym przydzieleniem działek inwestorom, co nastąpiło decyzją ministra infrastruktury w maju 2023 r. Jestem pewien, że rosyjski wywiad prowadzi również silne działania

operacyjne, aby pozyskać osobowe źródła agenturalne mające zarówno możliwości wywiadowcze, jak i wiedzę o powstającej inwestycji.

Rozwińmy wątek działań szpiegowskich Rosji.

Dotychczas rosyjski wywiad poszukiwał na terenie Polski przede wszystkim osób, które mają możliwości wywiadowcze, tj. mogą dostarczać cennych informacji, są zatrudnione w instytucjach lub obiektach interesujących dla wywiadu, są w partiach politycznych, w rządzie, mogą być wykorzystane w operacjach wpływu, mogą wspierać i zabezpieczać działalność wywiadowczą oraz pracę innych agentów czy też typować kandydatów na potencjalnych agentów. Obecnie do wykonywania prostych zadań, chociażby takich jak podkładanie ładunków zapalających, są poszukiwani także „agenci jednorazowi", czyli dywersanci bez specjalnej wiedzy i przeszkolenia. Kandydatem na takiego agenta może być każdy, kto posiada telefon komórkowy do robienia zdjęć obiektów, ma możliwość oznaczenia umownym znakiem obiektu do zniszczenia, potrafi umocować kamerę IP na drzewie, zostawić paczkę we wskazanym miejscu czy wzniecić ogień. Jedynym warunkiem wydaje się pobyt na terenie Polski. Należy zauważyć, że do 26 lutego 2023 r. na teren naszego kraju wjechało 9,797 mln osób narodowości ukraińskiej. W ubiegłym roku Agencja Bezpieczeństwa Wewnętrznego zatrzymała 16 członków siatki szpiegowskiej, w tym 12 Ukraińców, 3 Białorusinów i Rosjanina. Mieli oni prowadzić obserwację portów w Gdyni i Gdańsku, dworców kolejowych, np. w Rzeszowie, wojskowego lotniska w Jasionce używanego przez Stany Zjednoczone, a także zakładać kamery IP w pobliżu linii kolejowych, którymi transportowano sprzęt do Ukrainy. W przyszłości mieli zająć się też dywersją. Oczywiście do takiej działalności Rosjanie werbują również Polaków. Najbardziej znany przykład to sprawa Pawła K., który na lotnisku w Rzeszowie przygotowywał zamach na prezydenta Wołodymyra Zełenskiego.

Przykładów takich działań jest więcej. Do współpracy i zdobywania informacji wywiadowczych rosyjski wywiad agenturalny od wielu lat pozyskuje również marynarzy.

Agentów wśród marynarzy i osób mających możliwości wywiadowcze w sektorze morskim werbowały dwa ośrodki wywiadowcze GRU, czyli 1194 Centrum Wywiadowcze w Murmańsku i 264 Centrum Wywiadowcze w Kaliningradzie. Nie można wykluczyć, że ze względu na położenie i port morski praca typowniczo-werbunkowa mająca na celu pozyskiwanie źródeł osobowych i agentów mogła być prowadzona również siłami 73 Centrum Wywiadowczego w Sankt Petersburgu. Te komórki GRU miały niejako przypisane werbowanie zagranicznych marynarzy. Według raportu Baltic and International Maritime Council oraz International Chamber of Shipping z 2021 r.[11] rosyjscy marynarze stanowią 10,5% pracowników w żegludze międzynarodowej. Szacuje się, że jest ich obecnie 198 000. Dla rosyjskiego wywiadu to ogromna i cenna baza. Każdy marynarz musi mieć kontakt ze służbami specjalnymi przed rozpoczęciem pracy, przed otrzymaniem paszportu i książeczki żeglarskiej Seamans Book. W związku z wymogami konwencji STCW[12] co pięć lat muszą oni odnawiać większość szkoleń. Mają więc częsty kontakt z organami państwowymi, dzięki czemu służby wywiadowcze są w stanie ich kontrolować i wyznaczać im zadania do wykonania. Nie wyobrażam sobie, żeby marynarze ich nie realizowali. W najlepszym przypadku zostaliby pozbawieni możliwości wykonywania dobrze płatnego zawodu. Wykorzystanie rosyjskich marynarzy przez wywiad może być szerokie, m.in. polegać na zdobywaniu przez nich informacji o miejscach i obiektach morskich, do których przypływają ich statki, na typowaniu i wskazywaniu osób interesujących dla rosyjskiego wywiadu, a także przekazywaniu czy odbieraniu materiałów wywiadowczych. Załogi statków mogą poruszać się po strzeżonych obiektach portowych. Rosyjscy marynarze zawijają do nich statkami zarejestrowanymi pod banderami innymi niż rosyjska, dzięki czemu nie wzbudzają zbytnich podejrzeń i można im zlecać również działania sabotażowe na terenie obiektów portowych Europy Zachodniej.

[11] *Seafarer Workforce Report: The Global Supply and Demand for Seafarers in 2021*, https://www.bimco.org/products/publications/titles/seafarer-workforce-report/.

[12] International Convention on Standards of Training, Certification and Watchkeeping (pol. Międzynarodowa konwencja o wymaganiach w zakresie wyszkolenia marynarzy, wydawania świadectw oraz pełnienia wacht).

Rysunek 1. Obecne działania asymetryczne Federacji Rosyjskiej na Bałtyku.
Źródło: materiały własne S. Kalitowskiego.

Czego w związku z tym możemy się spodziewać w najbliższej przyszłości?

Łatwość werbowania agentów, którzy nie muszą mieć specjalnych umiejętności wywiadowczych, oraz brak konieczności długotrwałego procesu rozpracowania i osobistego kontaktu oficera wywiadu będą sprzyjać werbowaniu źródeł osobowych i sprawców aktów sabotażu w obiektach morskiej IK. W najbliższym czasie możemy się spodziewać działań sabotażowych w obiektach morskich, np. takich, do których doszło ostatnio w Hamburgu. Nieznani sprawcy uszkodzili silniki we fregacie FGS EMDEN (F266) przez wrzucenie kilku kilogramów stalowych wiórów. Z kolei na niemieckim okręcie FGS Homburg (M1068) poprzecinano w stoczni wiązki kabli, a na FGS Hessen (F221) „omyłkowo" nalano ropy do zbiornika wody pitnej. Sabotaż jest genialną bronią! Chociaż nie wygrywa się nim wojny, to niewielkim kosztem można sparaliżować funkcjonowanie, wzbudzić strach i niepokój, narazić zaatakowanego na ogromne straty i wydatki. Większość scenariuszy takich działań mieści się w sferze błędu ludzkiego czy braku profesjonalizmu. W ten sposób mogą być sabotowane nasze stocznie, porty, a także porty serwisowe i elementy łańcucha dostaw dla morskich farm wiatrowych. Dziwi mnie, że jeszcze nie było informacji o podejrzanych dronach latających nad

naszymi obiektami morskiej IK. Już kilka razy takie akcje miały miejsce w Niemczech czy Danii, gdzie roje dronów obserwacyjnych wystartowały ze statków na morzu. Skontrolowano podejrzane jednostki, ale nie znaleziono dowodów.

> **Panie Komandorze, dziękuję za trafne, czasem gorzkie, ale prawdziwe spostrzeżenia. Wierzę, że skłonią one do refleksji.**

Jestem zwolennikiem mówienia wprost i uświadamiania, gdzie mamy miękkie podbrzusze. Dotyczy to zwłaszcza sfer, w których w grę wchodzi szeroko pojmowane bezpieczeństwo. Nie łudźmy się, że Rosjanie o naszych słabościach dowiedzą się z tego wywiadu. Oni mają je bardzo dobrze rozpoznane! Poszukiwanie słabych miejsc i ich wzmacnianie to element budowania świadomości zagrożeń i motywacji do zwiększania bezpieczeństwa. Uczmy się na przykładzie Ukraińców, którzy wielokrotnie przyznali, że bagatelizowali zagrożenie. Nie wierzyli, że Rosjanie mogą zaatakować.

Chciałbym, aby ta rozmowa przyczyniła się do zwiększenia świadomości naszych polityków, decydentów oraz szefów służb na temat tego, jak ważny jest wywiad morski oraz właściwe rozpoznanie zagrożeń hybrydowych na Bałtyku. Trzeba nad tym zacząć pracować szybko i intensywnie, bo to zadanie na wczoraj. Nie możemy się oglądać na NATO, Stany Zjednoczone i inne kraje. Sami musimy zadbać o pozyskanie informacji wywiadowczych. Moim zdaniem to także ostatni dzwonek na rozwijanie szerokiej i silnej współpracy prywatno-państwowej w sektorze bezpieczeństwa morskiego.

Rozmawiała: Daria Olender