

Rafał Miętkiewicz

Zuzanna Nowak

B E Z P I E C Z E Ń S T W O

BAŁTYKU

Od rozpoznania sytuacji
do skoordynowanej reakcji



impulse.
INSTITUTE

ICEYE



Autorzy:



kmdr dr hab.
Rafał Andrzej Miętkiewicz
prof. AMW

Profesor uczelni w Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni. Ekspert Instytutu Polityki Energetycznej im. I. Łukasiewicza w Rzeszowie, członek Polskiego Towarzystwa Bezpieczeństwa Narodowego i Polskiego Towarzystwa Nautologicznego. Analityk ds. bezpieczeństwa morskiego państwa i ochrony infrastruktury krytycznej na morzu. Specjalizuje się w problematyce nowoczesnych technologii, ze szczególnym uwzględnieniem technologii autonomicznych. Publikuje liczne komentarze i raporty tematyczne, bierze udział w programach mentoringowych w ramach NATO DIANA.



Zuzanna Nowak

Dyrektor wykonawcza Impulse Institute. Analityk ds. polityki energetycznej i klimatycznej w Instytucie Polityki Energetycznej im. I. Łukasiewicza i non-resident fellow w Fundacji im. K. Pułaskiego. Specjalizuje się w tematyce bezpieczeństwa energetycznego, transformacji rynków energii i wielostronnej dyplomacji klimatycznej. Doradza instytucjom publicznym, przedsiębiorstwom energetycznym, organizacjom międzynarodowym i środowisku naukowemu w zakresie strategii, analiz i współpracy projektowej. Jest członkinią grupy eksperckiej NATO ISEG oraz ewaluatorką projektów Europejskiej Rady ds. Innowacji (EIC).

*Eksperci przedstawiają w raporcie własne, niezależne opinie.

Redakcja:
Zuzanna Nowak

Korekta:
Dorota Dul

Grafika:
Marzena i Paweł Oświęcimscy

Fundacja Impulse Institute
www.impulseinstitute.pl
ii@impulseinstitute.pl

**„Bezpieczeństwo Bałtyku
– od rozpoznania sytuacji
do skoordynowanej reakcji”**

Warszawa, wrzesień 2026 r.
Raport 1/2026
ISBN: 978-83-982914-0-8

impulse.
INSTITUTE

ICEYE

PARTNERZY:



W raporcie wykorzystano ilustracje pochodzące z serwisu Shutterstock, Depositphotos i Adobe Stock oraz materiały udostępnione na licencjach Creative Commons (Wikimedia Commons) – o ile nie wskazano źródła inaczej. Niektóre fotografie poddano modyfikacji AI.

Kilka godzin.
Tyle mamy, żeby zauważyć,
uzgodnić i zareagować.



Rafał Modrzewski
CEO i współzałożyciel ICEYE



Statek może przeciąć polskie obszary morskie w kilka godzin. Tyle może być czasu, w którym trzeba coś zauważyć, ocenić i zdążyć zareagować. Ten raport jest o tym oknie czasowym.

Sfinansowaliśmy opracowanie, w którym technologia satelitarna zajmuje tylko jeden rozdział. Dlaczego?

W rozmowach o bezpieczeństwie morskim pierwsze pytania dotyczą zwykle obserwacji. Jak często można spojrzeć na dany rejon. Co widać w nocy i przez chmury. Jak szybko dostarczymy obraz. Na te pytania potrafimy odpowiadać, a odpowiedzi są dziś znacznie lepsze niż kilka lat temu.

Potem pytania się zmieniają.

Widzimy jednostkę, która od dwóch dni zachowuje się przy kablu inaczej niż setki innych. Co dalej? Kto zestawi to z tym, co widzą pozostali? Kto oceni, czy to awaria, przypadek, a może coś więcej? Kto podejmuje decyzję i ile ma na nią czasu?

To już nie są pytania o obserwację.

Presja na Bałtyku rzadko wygląda jak gwałtowny incydent, zwykle rozkłada się na godziny i dni, w zachowaniach, które osobno nie znaczą nic, a razem znaczą

wszystko. Takich wzorów nie da się uchwycić w jednym meldunku. Widzi się je wtedy, gdy kilka instytucji patrzy na to samo i komunikuje się w czasie liczonym w minutach.

Dlatego uznaliśmy, że najbardziej użyteczną rzeczą, jaką możemy dziś zrobić, nie jest kolejny materiał o możliwościach satelitów. Pozyskanie obrazu jest w dużej mierze problemem technicznym, a więc rozwiązywalnym i policzalnym. Ciekawsze jest to, co dzieje się między obrazem na ekranie a decyzją. Tego nie kupuje się razem z technologią – to powstaje w uzgodnieniach, które wypracowuje się przed zdarzeniem, a nie w jego trakcie.

Polska buduje dziś kolejne elementy tego systemu, a moment jest dobry: łatwiej spinać je w całość teraz, gdy powstają, niż łączyć je później. Kierunek jest wybrany, a partnerów, którzy są gotowi to robić, przybywa.

Zostaje pytanie, na które nie odpowie ani liczba sensorów, ani rozdzielczość zobrazowania: ile czasu mija od pierwszego sygnału do reakcji?

To ten czas jest miarą, która się liczy. Obserwacja pozwala zacząć go liczyć wcześniej. Koordynacja decyduje, czy z tego czasu skorzystamy.

**To ten czas jest miarą,
która się liczy.**





Ochrona infrastruktury morskiej zaczyna się od wiedzy: w warunkach zagrożeń hybrydowych to ona odbiera potencjalnym sprawcom anonimowość. Stała obserwacja Bałtyku nie jest więc narzędziem śledczym, ale formą odstraszenia. Dane z orbity mamy już w zasięgu ręki: to łatwiejsza część odpowiedzi. Trudniejszą jest rozmowa między tymi, którzy je udostępniają, tymi, którzy je agregują i analizują, oraz tymi, którzy odpowiadają za ochronę infrastruktury. Chcemy, żeby ten raport był punktem wyjścia do takiej dyskusji.

Witold Witkowicz

prezes zarządu, ICEYE Polska



W ostatnich latach Morze Bałtyckie stało się jednym z najważniejszych obszarów koncentracji infrastruktury energetycznej w Europie – funkcjonują tutaj gazociągi, ropociągi, połączenia elektroenergetyczne, terminale i platformy wydobywcze, a także nowe źródła energii, w tym rozwijane przez Grupę ORLEN morskie farmy wiatrowe. W obliczu narastających napięć geopolitycznych i zagrożeń hybrydowych współpraca na rzecz ochrony infrastruktury krytycznej pozostaje jednym z filarów bezpieczeństwa Morza Bałtyckiego i całej Europy.

Paweł Wojtunik

wiceprezes zarządu ds. bezpieczeństwa i ryzyka, ORLEN



Podstawą bezpieczeństwa Morza Bałtyckiego jest jednolity obraz aktywności na jego wodach. Nie tworzy go jeden system, lecz zbiór platform i ich integracja. Rola Polskiej Grupy Zbrojeniowej jest jasna: dostarczamy zdolności potrzebne do ochrony polskich interesów na Bałtyku. Budujemy je w kraju na kolejne dekady.

Jan Grabowski

wiceprezes zarządu, Polska Grupa Zbrojeniowa



Jednym z kluczowych zadań Polskiej Agencji Kosmicznej jest wykorzystanie potencjału polskiego sektora kosmicznego na rzecz budowania operacyjnych zdolności państwa. Mamy nadzieję, że tworzona satelitarna tarcza dla Bałtyku, która pozwoli szybciej i efektywniej niż dotychczas weryfikować wykryte anomalie, wzmocni bezpieczeństwo i niezależność informacyjną Polski.

Marta Wachowicz

prezes, Polska Agencja Kosmiczna

SPIS TREŚCI

Bezpieczeństwo Bałtyku – od rozpoznania sytuacji
do skoordynowanej reakcji

8

1 | Bałtyk

Strategiczna przestrzeń operacyjna

14

2 | Jeden akwen, wiele misji

Użytkownicy systemu bezpieczeństwa morskiego

18

3 | Wiele systemów, jeden obraz?

Wyzwania dla bezpieczeństwa morskiego

30

4 | Od anomalii do reakcji

Incydent jako test systemu

34

5 | Wspólna warstwa obserwacji

Rola technologii satelitarnych na Bałtyku

40

6 | Od danych do działania

Priorytety wdrożeniowe dla Polski



Helsinki
Petersburg
Ust-Luga
Tallinn
Ryga
Klaipeda
Primorsk
Bałtyjsk
Gdynia
Gdańsk
Swinoujście
Szczecin
Rostock
Kiel
Trelleborg
Nynäshamn
Sztokholm

1 | Bałtyk: strategiczna przestrzeń operacyjna

Bałtyk jest akwenem niewielkim, lecz stanowi poważne wyzwanie z punktu widzenia utrzymania wielowymiarowego bezpieczeństwa. Nakładają się na nim intensywny ruch cywilny, działalność gospodarcza, aktywność wojskowa oraz funkcjonowanie infrastruktury krytycznej. Wysoka koncentracja użytkowników i aktywów sprawia, że te same zachowania lub zdarzenia mogą mieć jednocześnie znaczenie nawigacyjne, gospodarcze, przestępcze, hybrydowe lub militarne. Skuteczna ochrona akwenu wymaga więc nie tylko wykrywania obiektów i incydentów, lecz przede wszystkim utrzymywania ciągłego, regularnie aktualizowanego obrazu sytuacji, który pozwala odróżniać działalność rutynową i zdarzenia przypadkowe od działań celowych oraz odpowiednio wcześniej uruchamiać właściwą reakcję.

AKWEN WYSOKIEJ KONCENTRACJI RUCHU I INFRASTRUKTURY

Duża intensywność użytkowania:

Na Bałtyk przypada 8–15% światowej wymiany handlowej drogą morską, co sprawia, że jest jednym z najbardziej zatłoczonych akwenów na świecie. Na jego wodach znajduje się w dowolnym momencie około 1,5 tys. dużych statków morskich mających numer IMO (Międzynarodowej Organizacji Morskiej). Pełny obraz ruchu obejmuje dodatkowo kilka tysięcy innych jednostek, w tym te niepodlegające obowiązkowi wyposażenia w system automatycznej identyfikacji statków AIS (m.in. małe jednostki rybackie, rekreacyjne, turystyczne).

Gęsta sieć szlaków handlowych:

Ruch na Bałtyku koncentruje się w kilku silnie obciążonych korytarzach, cieśninach i podejściach portowych. Przez główną linię w rejonie Skaw odnotowuje się blisko 50–60 tys. przejść rocznie. Statki towarowe stanowią około 47% dużej floty na Bałtyku, zbiornikowce 23%, a pasażerskie zaledwie 4%, choć odpowiadają za blisko 50% wszystkich zawinięć do portów. Polskie porty przeładowały w 2025 r. 128 mln ton to-

warów (+3,1% r./r.), z czego sam Port Gdańsk obsłużył 3650 statków handlowych i 80,4 mln ton ładunków.

Rosnące znaczenie strategiczne:

Dostęp do morza stanowi podstawowy element bezpieczeństwa energetycznego Polski. Najważniejsze polskie projekty strategiczne na Bałtyku to terminal LNG w Świnoujściu (8,3 mld m³ rocznie), gazociąg Baltic Pipe (do 10 mld m³), budowany terminal FSRU w Zatoce Gdańskiej (6,1 mld m³), Naftoport (37,4 mln ton ropy w 2025 r.) oraz kabel SwePol Link (600 MW). Dopełnieniem są morskie farmy wiatrowe o mocy 5,9 GW do 2030 r. oraz powstająca w Lubiatowie-Kopalinie elektrownia jądrowa (do 3,75 GWe po 2036 r.). Na Bałtyku są także międzynarodowe korytarze gazowe i elektroenergetyczne (m.in. Balticconnector, EstLink 1 i 2, NordBalt czy wyłączony z użytku Nord Stream), a na jego dnie przebiega ponad 35 kabli telekomunikacyjnych.

AKWEN UTRUDNIONEJ OBSERWACJI I REAKCJI

Uwarunkowania hydrometeorologiczne zależne od pory roku utrudniają obserwację Bałtyku. Wiosną (marzec–maj) dominują mgły adwekcyjne o częstotliwości 15–25% na otwartym morzu, ograniczające widzialność do 200–800 m. Natomiast w okresie jesienno-zimowym głównym utrudnieniem są wysoka aktywność cyklonalna (gęste zachmurzenie), sezon sztormowy (około 40 dni sztormowych rocznie) oraz krótki dzień – w grudniu na polskim wybrzeżu (około 54,5°N) noc trwa ponad 16 godzin na dobę.

Uwarunkowania batymetryczne Bałtyku obniżają techniczny próg dostępu do infrastruktury podmorskiej. Średnia głębokość akwenu wynosi około 50 m. Maksymalna głębokość na polskich obszarach morskich wynosi 118 m (Głębia Gdańska), a w kluczowych przejściach cieśnin duńskich spada do kilku-kilkunastu metrów, co ułatwia oddziaływanie z wykorzystaniem kotwic, nurków technicznych oraz systemów bezzałogowych pojazdów podwodnych (UUV).



Źródło: Nasz Bałtyk

Uwarunkowania przestrzenne Bałtyku ograniczają czas dostępny na rozpoznanie i reakcję. Długość głównej osi akwenu wynosi około 1600 km, lecz odległości pomiędzy przeciwległymi wybrzeżami są znacznie mniejsze – na trasie Świnoujście–Trelleborg wynoszą około 177 km. Jednostka poruszająca się z prędkością 12–15 węzłów pokonuje ten dystans w ciągu 6–8 godzin. Identyfikacja, ocena sytuacji, podjęcie decyzji i skierowanie sił musi nastąpić w ciągu kilku godzin.

AKWEN INCYDENTÓW I PRESJI PONIŻEJ PROGU WOJNY

Bałtyk jest przestrzenią trwałej presji poniżej progu wojny, w której legalny ruch cywilny bywa wykorzystywany jako osłona działań przestępczych, rozpoznawczych i dywersyjnych. Ich cechą jest niejednoznaczność: są tak prowadzone, by utrudnić przypisanie sprawstwa, a ich funkcją jest zarówno testowanie odporności państw regionu, jak i oddziaływanie na jego krytyczne zasoby.

Wyzwaniem operacyjnym nie jest zatem wyłącznie samo wykrycie anomalii, lecz jej natychmiastowa weryfikacja i wstępna klasyfikacja – odróżnienie awarii technicznej, błędu nawigacyjnego i rutynowej aktywności od działania celowego. Pełna atrybucja wymaga złożonego postępowania wyjaśniającego oraz dostępu do danych wywiadowczych, co zajmuje tygodnie lub miesiące. Utrudniają ją brak wiarygodnych wzorców zdarzeń przypadkowych: w regionalnej sprawozdaw-

czości wypadków morskich przyczyny zdecydowanej większości zgłoszeń pozostają niewyjaśnione, przez co punkt odniesienia dla oceny zdarzenia podejrzanego jest z założenia ograniczony.

Presja hybrydowa rozwija się dwutorowo: w domenie infrastruktury podmorskiej oraz w sferze widzialności sygnałowej.

Od października 2023 r. uszkodzono na Bałtyku kilkanaście podmorskich kabli energetycznych i telekomunikacyjnych, w tym interkonektor EstLink 2, który po przerwaniu 25 grudnia 2024 r. wyłączono na blisko sześć miesięcy (koszt naprawy oszacowano na 60 mln euro). Działania masowca Yi Peng 3 (powiązanego z przerwaniem 17 i 18 listopada 2024 r. kabli Litwa–Gotlandia oraz C-Lion1) i tankowca Eagle S (powiązanego z uszkodzeniem pięciu kabli na odcinku 90 km) dowodzą, że nieuzbrojona jednostka cywilna może w krótkim czasie wyrządzić szkody strategiczne, a pociągnięcie sprawców do odpowiedzialności może okazać się bardzo trudne ze względu na ograniczenia jurysdykcyjne, standard dowodowy i konstrukcję międzynarodowego prawa morza. Postępowanie w sprawie Eagle S jest w toku: w pierwszej instancji Sąd Rejonowy w Helsinkach pozostawił zarzuty wobec kapitana i dwóch oficerów jednostki bez rozpoznania, uznając, że w świetle Konwencji Narodów Zjednoczonych o prawie morza (UNCLOS) fińskie prawo karne nie znajduje zastosowania do czynów popełnionych poza morzem terytorialnym. Rozstrzygnięcie zostało

zaskarżone przez prokuraturę i nie jest prawomocne. Przypadek ten pokazuje, że jednostka cywilna może podczas pojedynczego przejścia zagrozić kilku systemom infrastrukturalnym, podczas gdy skutki techniczne i operacyjne utrzymują się przez miesiące.

Środowisko sprzyjające takim działaniom tworzą dwa zjawiska: ruch floty cieni oraz manipulowanie danymi identyfikacyjnymi i nawigacyjnymi. Miesięcznie przez Bałtyk przechodzi 150–170 tankowców floty cieni (w samym 2025 r. jednostki objęte sankcjami UE wykonały 292 rejsy przez wody duńskie), ukrywających trasy, tożsamość i strukturę własnościową. Równolegle prowadzone są działania zakłócające globalny system nawigacji satelitarnej (GNSS). EUROCONTROL zarejestrował w 2024 r. ponad 2500 takich zdarzeń w lotnictwie. W domenie morskiej eksperymentalny system TDOA, wdrożony na polskim wybrzeżu Zatoki Gdańskiej, umożliwia ustalenie położenia emitery zakłóceń w czasie krótszym niż 300 sekund, wskazując jego położenie w rejonie obwodu królewieckiego. Dopętnieniem jest fałszowanie danych AIS (spoofing) przy użyciu fikcyjnych numerów IMO.

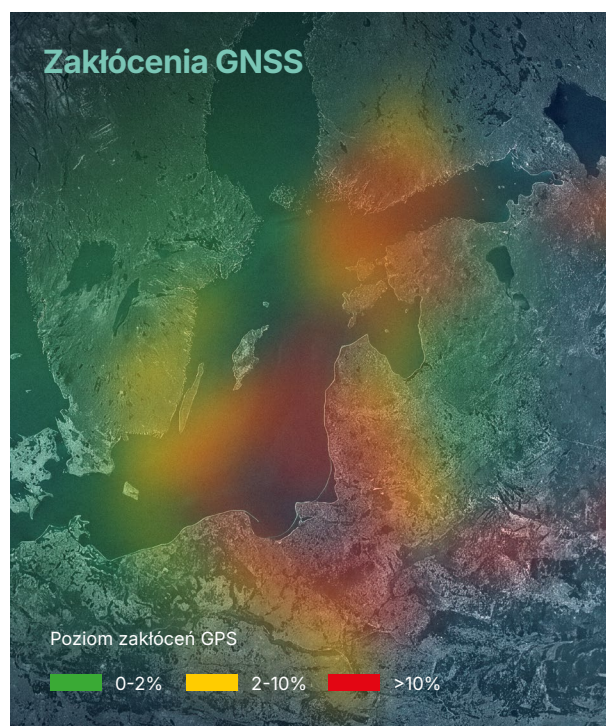
Ochrona tysięcy kilometrów infrastruktury podmorskiej wymaga zatem przejścia z biernego monitorowania na wyprzedzające reagowanie operacyjne.

Ten kierunek został już przełożony na konkretne rozwiązania, których wspólnym celem jest skrócenie czasu od wykrycia anomalii do skierowania właściwych sił. Odpowiedzią NATO jest powołanie w październiku 2024 r. dowództwa Commander Task Force Baltic (CTF Baltic) w Rostocku (z polskim oficerem na stanowisku zastępcy dowódcy, a od końca 2028 r. – przejęciem roli dowodzenia przez POLMARFOR w Gdyni) oraz uruchomienie w styczniu 2025 r. operacji Baltic Sentry. Według MARCOM skrócono czas reakcji na zdarzenie z 17 godzin do zaledwie godziny. W czerwcu 2025 r. w ramach inicjatywy Task Force X-Baltic NATO wykorzystało podczas trzytygodniowych ćwiczeń ponad 70 systemów bezzałogowych (powietrznych, nawodnych i podwodnych) prowadzących patrole rozpoznawcze i dozór kluczowych obszarów. Doświadczenia te przełożono na dalsze działania: w lutym 2026 r. osiem państw NATO, w tym Polska, uzgodniło przyspieszenie pozyskiwania i integracji wielodomenowych zdolności służących bezpieczeństwu Bałtyku. Działania te pokazują, że odpowiedź na presję poniżej progu wojny nie może opierać się wyłącznie na zwiększaniu obecności sił na morzu. Jej skuteczność zależy od równoległego uporządkowania architektury technicznej oraz podziału informacji, kompetencji i odpowiedzialności pomiędzy uczestników systemu.

Z tego wynikają dwa zasadnicze wnioski dla bezpieczeństwa Bałtyku.

Pierwszy ma charakter technologiczny. Wobec braku możliwości stałej obecności fizycznej na całej długości korytarzy infrastrukturalnych wartość operacyjna zależy od warstwowej integracji danych, która pozwala wykryć anomalię, sklasyfikować ją i skierować środek interwencyjny, zanim potwierdzone zostaną skutki zdarzenia. Wymaga to narzędzi o otwartej architekturze systemowej, zdolnych przyjmować nowe rozwiązania bez przebudowy całości, zarówno ze względu na tempo rozwoju technologii, jak i na rosnącą świadomość bezpieczeństwa wśród podmiotów komercyjnych dysponujących własnymi sensorami.

Drugi ma charakter instytucjonalny. Uszkodzenie kabla, rurociągu lub interkonektora nie jest zdarzeniem jednego sektora: zwykle oznacza jednocześnie skutki energetyczne, komunikacyjne, gospodarcze i polityczne. Ten sam incydent wchodzi równocześnie w zakres kompetencji sił zbrojnych, służb granicznych, administracji morskiej i operatora infrastruktury, z których żaden podmiot nie dysponuje ani pełnym obrazem sytuacji (choćby branżowym profilem skutków wystąpienia zdarzenia), ani całością środków reagowania. Rozproszenie zdolności monitoringu pomiędzy te podmioty o różnym charakterze działania jest obecnie stanem trwałym, a nie przejściową niedoskonałością. To właśnie ono, a nie liczba sensorów czy narzędzi, wyznacza granicę skuteczności systemu.



Źródło: GPSJAM wg danych na 21.08.2026

Ochrona infrastruktury energetycznej na Bałtyku



Julia Ćwiek
ORLEN



Rafał Sadowski
ORLEN

W ostatnich latach **Bałtyk przekształcił się z akwenu peryferyjnego w obszar o strategicznym znaczeniu dla bezpieczeństwa energetycznego Europy Środkowej i Północnej**. Zmiana ta jest wynikiem dwóch równoległych procesów: przyspieszenia transformacji energetycznej państw nadbałtyckich i ich odchodzenia od rosyjskich surowców i nośników energii oraz narastania zagrożeń bezpieczeństwa wywołanych agresywnymi działaniami Rosji. Tempo przemian w regionie Morza Bałtyckiego ma istotne znaczenie dla bezpieczeństwa energetycznego całej Unii Europejskiej, choćby dlatego, że na państwa tego obszaru przypada 35% unijnego zużycia energii.

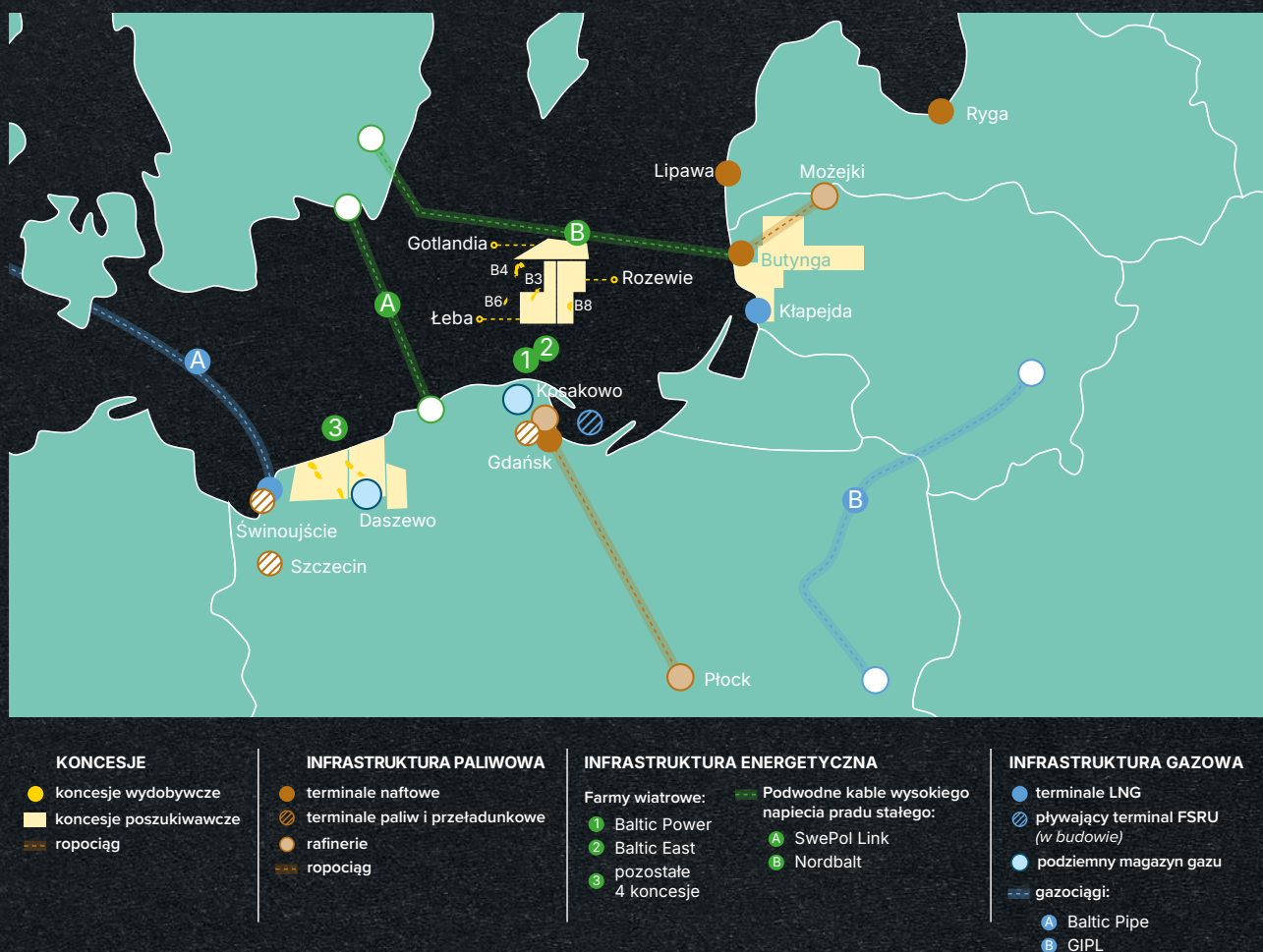
Bałtyk stał się jednym z najważniejszych obszarów europejskiej infrastruktury energetycznej. Przebiegają przez niego dwa strategiczne podmorskie gazociągi – Baltic Pipe, prowadzący z Norwegii przez Danię do Polski, oraz Balticconnector, łączący Finlandię z Estonią, o łącznej przepustowości rocznej 12,6 mld m³, a także dziewięć transgranicznych połączeń elektroenergetycznych o łącznej mocy 5,2 GW i 35 podmorskich systemów kabli telekomunikacyjnych. Krytyczne znaczenie ma również infrastruktura lądowa i przybrzeżna: terminale LNG (lądowy i FSRU), terminale naftowe i paliwowe, rafinerie – m.in. w Polsce, Finlandii, na Litwie i w Szwecji – a także bazy paliwowe. Terminale importowe umożliwiają dostawy do blisko 70 mln ton ropy naftowej rocznie (około 63 mln ton w 2025 r.) oraz do około 22 mln ton LNG (około 17 mln ton w 2025 r.). Znaczenie tej infrastruktury przesyłowej i importowej wykracza poza sam region, w coraz większym stopniu oddziałując na bezpieczeństwo energetycz-

ne państw Europy Środkowej oraz sąsiadów Unii Europejskiej, w tym Ukrainy.

Bałtyk odgrywa też coraz istotniejszą rolę w transformacji energetycznej. Szczególne znaczenie ma rozwój morskiej energetyki wiatrowej. Obecnie moc zainstalowana farm wiatrowych na Bałtyku wynosi około 3,1 GW – 10 lipca 2026 r. ORLEN uruchomił morską farmę wiatrową Baltic Power – a do 2030 r. ma wzrosnąć do 19,6 GW, przy szacowanym potencjale 93 GW. Region stwarza również obiecujące możliwości rozwoju infrastruktury wodorowej – rozważane są obecnie dwa projekty połączeń prowadzących z Finlandii przez państwa bałtyckie do Niemiec, NBHC i BHC – a także projektów wychwytywania, wykorzystania i składowania dwutlenku węgla (CCUS).

Wraz z rozwojem projektów i współpracy energetycznej na Bałtyku znacząco wzrosły zagrożenia dla bezpieczeństwa infrastruktury energetycznej w regionie. Od rozpoczęcia przez Rosję wojny przeciwko Ukrainie w 2022 r. akwen stał się obszarem intensywnej rosyjskiej aktywności hybrydowej ukierunkowanej na osłabienie odporności państw NATO i Unii Europejskiej oraz wywieranie presji politycznej i gospodarczej. Infrastruktura energetyczna regionu jest jednym z głównych celów tych działań, które przybierają rozmaite formy – od rozpoznania i szpiegostwa po działania sabotażowe i prowokacje militarne.

Najpoważniejsze skutki przyniosły **uszkodzenia infrastruktury podmorskiej**: gazociągu Balticconnector w październiku 2023 r., kabla elektroenergetycznego



EstLink 2 w grudniu 2024 r. oraz 13 kabli telekomunikacyjnych. Szczególne zagrożenie stanowi tzw. **flota cieni**, czyli tankowce przewożące rosyjską ropę naftową z obejściem sankcji. Jednostki te są wykorzystywane do prowadzenia rozpoznania infrastruktury krytycznej i działań sabotażowych, np. uszkodzenia infrastruktury podmorskiej poprzez wleczenie kotwic po dnie morskim. Ponadto zły stan techniczny statków floty cieni, któremu często towarzyszy brak odpowiedniego ubezpieczenia i doświadczonych załóg, zwiększa ryzyko wypadków morskich i katastrof ekologicznych.

Coraz częściej obserwuje się również **rosyjskie prowokacje militarne**. Należą do nich naruszenia przestrzeni powietrznej przez rosyjskie statki powietrzne, incydenty z udziałem rosyjskich jednostek pływających w wyłącznych strefach ekonomicznych, a także zbliżanie się do obiektów infrastruktury energetycznej. Kolejnym przykładem jest eskortowanie statków floty cieni przez rosyjską marynarkę wojenną, co utrudnia egzekwowanie sankcji. Tego rodzaju działania Rosji zwiększają ryzyko niekontrolowanych incydentów

i destabilizują środowisko bezpieczeństwa w regionie. Odrębnym wyzwaniem pozostają utrzymujące się zakłócenia **systemów nawigacji satelitarnej na Bałtyku**. Utrudniają one żeglugę, zwiększają ryzyko kolizji i komplikują realizację inwestycji morskich, takich jak budowa i serwisowanie morskich farm wiatrowych czy platform wydobywczych. Równocześnie rośnie liczba cyberataków wymierzonych w operatorów infrastruktury krytycznej, porty i terminale oraz armatorów.

Wobec narastających zagrożeń bezpieczeństwo infrastruktury energetycznej na Bałtyku wymaga aktywnego systemowego podejścia. Istotne znaczenie mają działania obejmujące bezpieczeństwo całego łańcucha wartości: od szlaków transportowych i infrastruktury przesyłowej po terminale, porty, bazy paliwowe, rafinerie i morskie instalacje energetyczne. ORLEN odpowiada na te wyzwania, rozwijając systemy monitorowania zagrożeń, wzmacniając odporność infrastruktury krytycznej oraz łańcuchów dostaw, a także zwiększając nakłady na cyberbezpieczeństwo i technologie ochrony aktywów energetycznych.



2 | Jeden akwen, wiele misji.

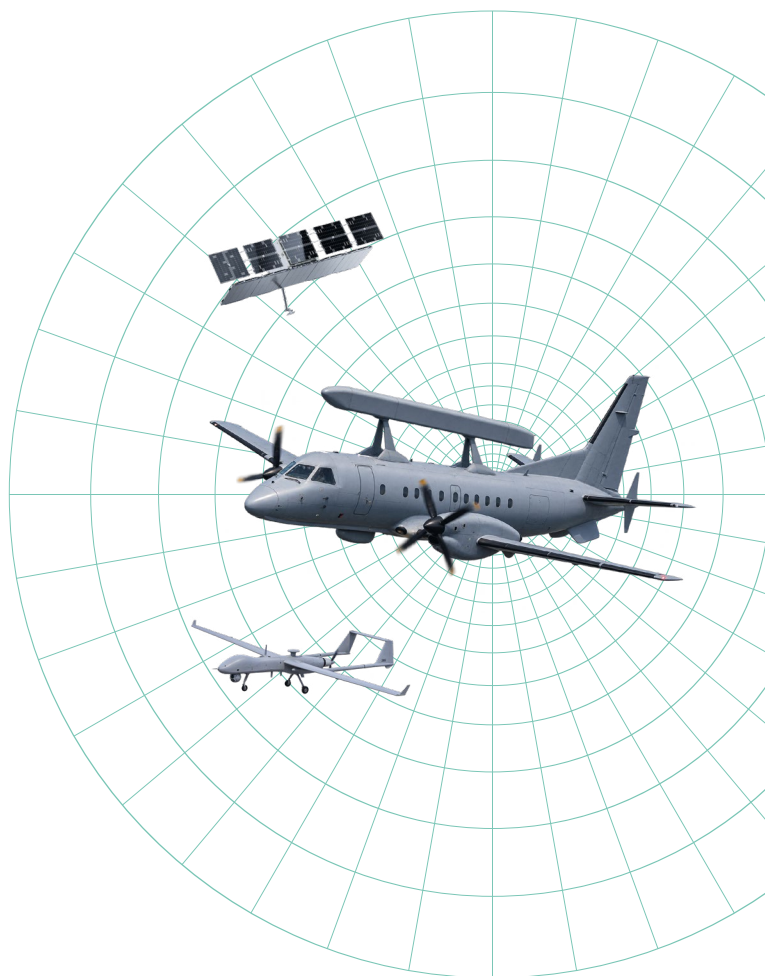
Użytkownicy systemu bezpieczeństwa morskiego

Bezpieczeństwo polskich obszarów morskich nie stanowi wyłącznej domeny jednej instytucji ani jednego sektora. Obejmuje równolegle obronę państwa, ochronę granicy i porządku prawnego, zabezpieczenie infrastruktury krytycznej, utrzymanie ciągłości gospodarki morskiej, bezpieczeństwo żeglugi, ratownictwo oraz ochronę środowiska naturalnego. Za realizację tych zadań odpowiadają różne podmioty, działające na podstawie odmiennych ustaw, procedur i reżimów prawnych, a zakres ich uprawnień, nie zaś zakres ich świadomości sytuacyjnej, wyznacza granice tego, jakie działania każdy z nich może podejmować na morzu.

Główne ramy prawne bezpieczeństwa morskiego RP wyznaczają ustawy dotyczące obrony Ojczyzny, funkcjonowania Straży Granicznej, ochrony granicy państwowej, obszarów morskich RP i administracji morskiej, bezpieczeństwa morskiego, ochrony żeglugi i portów morskich, zapobiegania zanieczyszczaniu morza przez statki, działalności Państwowej Komisji Badania Wypadków Morskich, zarządzania kryzysowego oraz gospodarki wodnej. Ramy te uzupełnia ustawa z 18 grudnia 2025 r. dotycząca działań Sił Zbrojnych na polskich obszarach morskich i bezpieczeństwa Morza Bałtyckiego – tzw. ustawa Bezpieczny Bałtyk – a także prowadzone w 2026 r. prace legislacyjne i organizacyjne nad utworzeniem Centrum Bezpieczeństwa Morskiego.

Podział odpowiedzialności nie oznacza jednak rozdzielania samych zagrożeń. Ta sama jednostka, aktywność lub anomalia może jednocześnie stanowić przedmiot zainteresowania Marynarki Wojennej, Straży Granicznej, administracji morskiej, innych służb państwowych oraz operatora infrastruktury krytycznej. Pojawienie się statku w pobliżu gazociągu może być oceniane jako zagrożenie dla aktywa gospodarczego, naruszenie przepisów żeglugowych, element rozpoznania infrastruktury albo przygotowanie działania o charakterze dywersyjnym. Każda z tych kwalifikacji uruchamia inną ścieżkę postępowania, inny standard dowodowy, a także inne tempo działania.

Co więcej, poszczególni uczestnicy systemu odpowiadają za różne obszary bezpieczeństwa Bałtyku i w znacznej mierze korzystają z różnych źródeł informacji, zasobów obserwacyjnych, systemów łączności, środków patrolowych i procedur reagowania. Skuteczność systemu zależy od zdolności łączenia tych perspektyw bez naruszania ustawowych kompetencji tych instytucji, a od 2026 r. – także od uporządkowania obszarów, w których kompetencje te zaczęły się dublować.



MISJA 1

Obrona i rozpoznanie

Siłły Zbrojne RP, a przede wszystkim Marynarka Wojenna, odpowiadają za obronę państwa, utrzymanie swobody działania na morzu oraz rozpoznawanie zagrożeń militarnych i działań prowadzonych poniżej progu wojny.

Zadania

- budowanie rozpoznanego obrazu sytuacji morskiej i jego wymiana w ramach NATO;
- wykrywanie i śledzenie potencjalnych zagrożeń oraz ostrzeganie przed nimi;
- ochrona morskich linii komunikacyjnych i obrona interesów państwa na polskich obszarach morskich;
- niedopuszczenie do blokady morskiej państwa;
- współdziałanie z siłami NATO i państw regionu;
- ochrona infrastruktury krytycznej na morzu, z możliwością użycia uzbrojenia na warunkach ustawy Bezpieczny Bałtyk;
- kontrola obcych statków w zakresie określonym przepisami obowiązującymi od 2026 r.;
- wsparcie Morskiego Oddziału Straży Granicznej;
- udział w ratowaniu życia na morzu – element powietrzny SAR (Search and Rescue) oraz siły okrętowe.

MISJA 2

Ochrona granicy i egzekwowanie prawa

Morski Oddział Straży Granicznej jest uzbrojoną formacją odpowiedzialną za ochronę morskiej granicy państwa oraz egzekwowanie prawa wobec jednostek znajdujących się na polskich obszarach morskich.

Zadania

- ochrona morskiej granicy państwa;
- przeciwdziałanie przemytowi i przestępczości transgranicznej;
- identyfikowanie jednostek ukrywających pozycję, trasę lub tożsamość;
- typowanie statków do kontroli i kierowanie środków interwencyjnych;
- zatrzymanie statku i skierowanie go do wskazanego portu (w ramach ochrony infrastruktury krytycznej);
- dokumentowanie naruszeń i zabezpieczanie materiału dowodowego;
- od 2027 r. – prowadzenie Centrum Bezpieczeństwa Morskiego.

MISJA 3

Bezpieczeństwo żeglugi i ciągłość gospodarki morskiej

Urzędy morskie, kapitanaty portów i służby VTS odpowiadają za bezpieczeństwo żeglugi i ciągłość funkcjonowania transportu oraz gospodarki morskiej.

Zadania

- monitorowanie ruchu i ryzyka nawigacyjnego;
- nadzór nad redami, kotwicznymi i torami podejściowymi;
- zarządzanie ruchem w warunkach zagrożenia;
- ustanawianie stref ochronnych wokół infrastruktury;
- decyzje o zamknięciu lub ograniczeniu użytkowania akwenu;
- utrzymanie ciągłości pracy portów i dostaw surowców;
- przywracanie normalnego funkcjonowania po incydencie.

MISJA 4

Odporność infrastruktury krytycznej

Operatorzy infrastruktury strategicznej odpowiadają za jej bezpieczeństwo techniczne, odporność na zakłócenia oraz utrzymanie i odtworzenie ciągłości świadczonych usług.

Zadania

- monitorowanie otoczenia farm wiatrowych, platform, gazociągów, kabli i terminali;
- wykrywanie naruszeń stref bezpieczeństwa i nietypowej aktywności jednostek;
- wczesne ostrzeganie organów państwa;
- uruchamianie procedur awaryjnych i wnioskowanie o wsparcie;
- ograniczanie skutków incydentu i odtwarzanie zdolności;
- rekonstrukcja zdarzeń na potrzeby dochodzeń i roszczeń.

MISJA 5

Ratownictwo i ochrona środowiska morskiego

Morska Służba Poszukiwania i Ratownictwa odpowiada za poszukiwanie i ratowanie osób znajdujących się w niebezpieczeństwie na morzu oraz za zwalczanie zagrożeń i zanieczyszczeń środowiska morskiego.

Informacje hydrometeorologiczne wspierają prowadzenie akcji ratowniczych, bezpieczeństwo żeglugi i funkcjonowanie infrastruktury.

Zadania

- poszukiwanie i ratowanie życia oraz mienia na morzu, lokalizacja jednostek i osób;
- wykrywanie rozlewów i nielegalnych zrzutów;
- określanie skali i źródła zanieczyszczenia;
- prowadzenie akcji zwalczania zanieczyszczeń;
- dokumentowanie skutków środowiskowych incydentów.

MISJA 6

Ustalanie przyczyn i ściganie

Państwowa Komisja Badania Wypadków Morskich (PKBWM) niezależnie bada przyczyny wypadków i incydentów morskich, natomiast odpowiedzialność prawną ustalają właściwe organy ścigania, izby morskie i sądy.

Zadania

- niezależne badanie okoliczności i przyczyn wypadków i incydentów;
- formułowanie zaleceń służących zapobieganiu podobnym zdarzeniom;
- zabezpieczanie materiału dowodowego przez właściwe służby;
- ustalanie okoliczności wypadków i konsekwencji zawodowych przez izby morskie;
- prowadzenie postępowań karnych przez właściwe organy ścigania i prokuraturę;
- rozstrzyganie odpowiedzialności karnej i cywilnej przez właściwe sądy.

Wspólna przestrzeń działania

Ta sama aktywność może jednocześnie zainteresować Siły Zbrojne, służby, administrację i operatora infrastruktury.

Różne są ich kompetencje i zakres odpowiedzialności, lecz wspólne pozostają:

- potrzeba utrzymywania i regularnego aktualizowania obrazu sytuacji;
- identyfikacja jednostek i analiza ich zachowania;
- dostęp do wiarygodnych danych oraz ich konsolidacja;
- możliwość szybkiego przekazywania informacji;
- dysponowanie środkami do kontroli, obserwacji lub interwencji;
- wsparcie procesu dowodzenia i kierowania;
- ciągłość działania na styku sektorów i po przekroczeniu granic państwowych.

Ochrona Bałtyku wymaga zatem nie jednego użytkownika i nie jednego systemu dowodzenia, lecz wspólne środowisko informacyjne, które pozwala różnym podmiotom wykonywać ich własne misje na podstawie spójnego obrazu sytuacji.

W przypadku incydentu wywołującego skutki wykraczające poza domenę morską reakcja operacyjna powinna być powiązana z krajowym systemem zarządzania kryzysowego, w tym z funkcjami Rządowego Centrum Bezpieczeństwa (RCB). Dotyczy to zwłaszcza oceny skutków kaskadowych, koordynacji międzyresortowej, komunikacji kryzysowej oraz ustalania priorytetów odtworzenia ciągłości usług kluczowych.

Obszary niejednoznaczności

Marynarka Wojenna – Straż Graniczna: znowelizowane przepisy nie wskazują jednoznacznie podmiotu kierującego działaniami wobec obcego statku w przypadku zagrożenia dla infrastruktury krytycznej w wyłączonej strefie ekonomicznej (WSE).

Administracja morska – organy ścigania: przepisy nie wyznaczają jednoznacznego momentu, w którym naruszenie zasad żeglugi lub strefy ochronnej powinno uruchomić postępowanie karne obok toczącego się postępowania administracyjnego.

Operator – państwo: układ kompetencyjny rozdziela wiedzę o podatności i skutkach uszkodzenia infrastruktury od informacji o jednostce (potencjalnym sprawcy), jej kontekście operacyjnym i dostępnych środkach interwencji.

Morze terytorialne – wyłączna strefa ekonomiczna: ograniczone uprawnienia państwa nadbrzeżnego w WSE utrudniają zatrzymanie podejrzanej jednostki i przenoszą ciężar działania na śledzenie, dokumentowanie oraz współpracę z państwem bandery i portu.

3 | Wiele systemów, jeden obraz?

Użytkownicy systemu bezpieczeństwa morskiego

Siły Zbrojne RP, Straż Graniczna, administracja morską, służby ratownicze, porty oraz operatorzy infrastruktury krytycznej dysponują własnymi systemami obserwacji, zasobami informacyjnymi i procedurami reagowania. Rozwijane są również nowe zdolności techniczne, mechanizmy współpracy oraz rozwiązania instytucjonalne. Elementy te powstawały jednak osobno dla różnych użytkowników i zadań, dlatego nie tworzą jednego spójnego

systemu, który umożliwia wykrycie zdarzenia, wymianę danych, zbudowanie jednolitego obrazu sytuacji, ocenę ryzyka, przekazanie informacji i całościowe zadysponowanie siłami. Selektywne rozbudowywanie zdolności poszczególnych służb i sił prowadzi do niedostatecznie skoordynowanych działań. Może to skutkować nieefektywnym wykorzystaniem ograniczonych zasobów bez osiągnięcia efektu synergii.

Rozbudowane, lecz sektorowe zdolności

Obserwacja polskich obszarów morskich opiera się na wielu równolegle funkcjonujących źródłach informacji, które obejmują zarówno elementy Krajowego Systemu Bezpieczeństwa Morskiego (KSBM), jak i systemy Sił Zbrojnych, innych służb oraz operatorów infrastruktury:

AIS-PL/VTS

Sieć stacji AIS oraz systemy służby kontroli ruchu statków (Vessel Traffic Service, VTS) umożliwiają identyfikację statków, śledzenie ich tras i zarządzanie ruchem na głównych podejściach portowych.

RADARY KSBM

27 radarów (w tym 6 radarów brzegowych i 3 portowe w rejonie VTS Zatoka Gdańska oraz radar dalekiego zasięgu na Baltic Beta) zapewnia obserwację ruchu nawodnego.

CCTV KSBM

26 kamer wspiera obserwację optyczną portów, red i podejść, przy czym kamera VTS na Helu ma zasięg do 7 Mm.

ZSRN STRAŻY GRANICZNEJ

Wiele posterunków obserwacyjnych tworzy obraz sytuacji na potrzeby ochrony granicy i działań Straży Granicznej na polskich obszarach morskich.

SENSORY WOJSKOWE

Stacjonarne i mobilne środki rozpoznania z brzegu, morza i powietrza wspierają wykrywanie, śledzenie i ocenę zagrożeń na potrzeby Sił Zbrojnych.

STACJE HYDRO-METEOROLOGICZNE KSBM

14 stacji dostarcza dane o warunkach wpływających na bezpieczeństwo żegluga i prowadzenie działań na morzu

RADIONAMIERNIKI RDF KSBM

5 urządzeń wspiera lokalizację źródeł emisji radiowej oraz identyfikację jednostek prowadzących korespondencję.

MONITORING DGPS KSBM

2 stacje monitorują jakość i dostępność różnicowego systemu pozycjonowania wykorzystywanego przez żegluga.

ŁĄCZNOŚĆ VHF KSBM

12 stacji zapewnia komunikację operacyjną ze statkami i wspiera zarządzanie ruchem morskim.

MONITORING OPERATORSKI

Rozproszone systemy operatorów monitorują stan i parametry infrastruktury energetycznej i telekomunikacyjnej.

DANE REJESTROWE, WYWIADOWCZE I KOMERCYJNE

Rozproszone źródła uzupełniają obraz sensorowy o dane dotyczące tożsamości, historii ruchu, własności jednostki i kontekstu zagrożenia.

Każdy z tych elementów odpowiada na określoną potrzebę operacyjną. Ich połączenie tworzy zdolność do budowania obrazu sytuacji morskiej (Recognized Maritime Picture, RMP) oraz świadomości sytuacyjnej w domenie morskiej (Maritime Situational Awareness, MSA).

RMP to kompleksowy, aktualizowany w czasie rzeczywistym obraz aktywności morskiej na wyznaczonym obszarze. Tworzony na podstawie danych radarowych, satelitarnych, AIS i innych, podlega ocenie właściwego, uprawnionego podmiotu przed dystrybucją, dzięki czemu umożliwia dowódcom śledzenie jednostek pływających,

wykrywanie anomalii i podejmowanie szybkich, świadomych decyzji taktycznych.

MSA to zrozumienie zdarzeń, działań i okoliczności o charakterze militarnym i niemilitarnym w środowisku morskim istotnych dla prowadzonych i planowanych operacji. Poszczególne organizacje i instytucje doprecyzowują tę definicję odmiennie.

Ograniczeniem pozostają jednak zasięg sensorów brzegowych, wysokie koszty utrzymywania stałej obecności na morzu oraz zależność dostępności lotnictwa i sił okrętowych od warunków hydrometeorologicznych.

Obserwacja polskich obszarów morskich

Kosmos

Satelita SAR



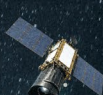
Satelita SIGINT



Satelita GNSS



Satelita optyczny



Powietrze

Samolot patrolowy



Śmigłowiec



UAV



Powierzchnia i brzeg

Statek handlowy



Baltic Beta



Flota cieni



Okręt wojenny



MEW



USV



ZSRN/SG

Radary

VHF/RDF

CCTV

AIS/VTS



Toń wodna i dno morskie

UUV



Sonary



Hydrofony i sonary



Sensor



Sensor



Monitoring operators



Bez sprawnego przepływu informacji żadna ze stron nie ma samodzielnie pełnego obrazu sytuacji.

LUKA INFORMACYJNA: OD SENSORÓW DO SPÓJNEGO OBRAZU

Istnienie wielu systemów obserwacji nie oznacza pełnego i ciągłego rozpoznania sytuacji.

Poszczególne źródła mają swoje ograniczenia:

- AIS opiera się na danych nadawanych przez jednostki i może być wyłączany, fałszowany lub manipulowany;
- transpondery AIS są wykorzystywane przez statki o określonym tonażu i charakterystyce; jednostki poniżej limitu nie mają obowiązku korzystania z AIS;
- radary brzegowe zapewniają stałą obserwację wybranych obszarów, lecz ich możliwości ograniczają zasięg, geometria wybrzeża i warunki propagacji;
- działanie systemów optycznych zależy od pory dnia, zachmurzenia, mgły i widzialności;
- sensory wojskowe i podległe innym służbom działają w odrębnych systemach i reżimach dostępu;
- monitoring operatorów koncentruje się na konkretnych aktywach i strefach, nie zaś na pełnym obrazie sytuacji na morzu.

Luka nie polega zatem wyłącznie na braku permanentnego monitoringu określonych obszarów. Obejmuje też brak ciągłości działań pomiędzy wykryciem obiektu, jego identyfikacją, analizą zachowania, oceną ryzyka oraz podjęciem decyzji.

LUKA PUBLICZNO-PRYWATNA: WIEDZA O AKTYWIE I ZDOLNOŚĆ DZIAŁANIA

Ochrona infrastruktury morskiej wymaga współpracy państwa z jej operatorami. Każda ze stron ma informacje i możliwości, których nie ma druga (lub ma w ograniczonym zakresie). Wynika to wprost z zadań przez nie realizowanych.

Operatorzy dysponują szczegółową wiedzą o:

- stanie technicznym infrastruktury;
- znaczeniu konkretnych instalacji dla ciągłości usług;
- strefach szczególnie wrażliwych;
- normalnych wzorcach działalności wokół aktywów;
- skutkach potencjalnej awarii lub uszkodzenia.

Państwo posiada natomiast:

- szerszy obraz sytuacji bezpieczeństwa;
- dostęp do informacji pochodzących od służb i z systemu obronnego;
- kompetencje kontrolne i administracyjne;
- środki patrolowe, rozpoznawcze i interwencyjne;
- możliwość współpracy międzynarodowej i transgranicznej wymiany danych;
- instrumenty prawne oddziaływania na potencjalnych adversarzy;
- możliwość prowadzenia działań przekraczających granice pojedynczego aktywa.

Bez sprawnego przepływu informacji żadna ze stron nie ma samodzielnie pełnego obrazu sytuacji ani nie jest w stanie w sposób skoordynowany zadysponować posiadanymi zasobami. Operator może dostrzec nietypową aktywność wokół instalacji, ale nie znać szerszego kontekstu bezpieczeństwa. Służby mogą wykryć jednostkę i przeanalizować jej zachowanie, ale bez wiedzy operatora nie zawsze prawidłowo ocenią znaczenie zagrożenia dla konkretnego elementu infrastruktury. Jednocześnie operator odpowiednio wcześniej ostrzeżony o potencjalnym niebezpieczeństwie może wdrożyć procedury wzmacniające odporność i ostatecznie skracające czas powrotu do funkcjonowania, nawet jeśli atak



okaże się częściowo skuteczny. Luka publiczno-prywatna dotyczy zatem nie tylko wymiany danych, lecz także zasad alarmowania, eskalacji, ochrony informacji wrażliwych oraz odpowiedzialności za reakcję. Istotny jest również dwukierunkowy przepływ danych o zagrożeniach z zachowaniem odpowiedniego wyprzedzenia.

LUKA KOORDYNACYJNA: OD WYKRYCIA DO REAKCJI

Rosnąca liczba danych może zwiększać obciążenie systemu, jeżeli nie towarzyszą jej zdolności do ich filtrowania, korelacji i priorytetyzacji (mgła informacyjna i przytłoczenie informacyjne). Przewaga informacyjna nie wynika z samego posiadania informacji, lecz z możliwości przekształcenia ich w użyteczny produkt decyzyjny (zarządzanie informacją) zasilający z odpowiednim wyprzedzeniem procesy dowodzenia i kierowania. Co więcej, ta sama anomalia może zmieniać charakter wraz z rozwojem sytuacji. Nietypowe zachowanie jednostki może początkowo zostać uznane za problem bezpieczeństwa żeglugi, następnie uzasadniać kontrolę Straży Granicznej, a ostatecznie zostać ocenione jako zagrożenie dla infrastruktury krytycznej lub element działania hybrydowego (maskowanie działań). System musi zatem odpowiadać nie tylko na pytanie, kto wykrywa zdarzenie, lecz także:

- kto łączy informacje pochodzące z różnych źródeł;
- kto tworzy wspólny obraz sytuacji;
- kto klasyfikuje anomalię i określa poziom ryzyka;
- kto decyduje o przekazaniu informacji poszczególnym użytkownikom;
- kto i na jakich zasadach przekazuje odpowiedzialność między administracją, służbami i wojskiem;

- kto kieruje reakcją i dysponuje dostępnymi siłami i środkami;
- kto utrzymuje ciągłość obrazu podczas zmiany podmiotu prowadzącego;
- kto finansuje utrzymanie i rozwój wspólnej warstwy systemu;
- kto odpowiada za rozwój i wdrażanie rekomendacji umożliwiających sprawne wprowadzanie zmian.

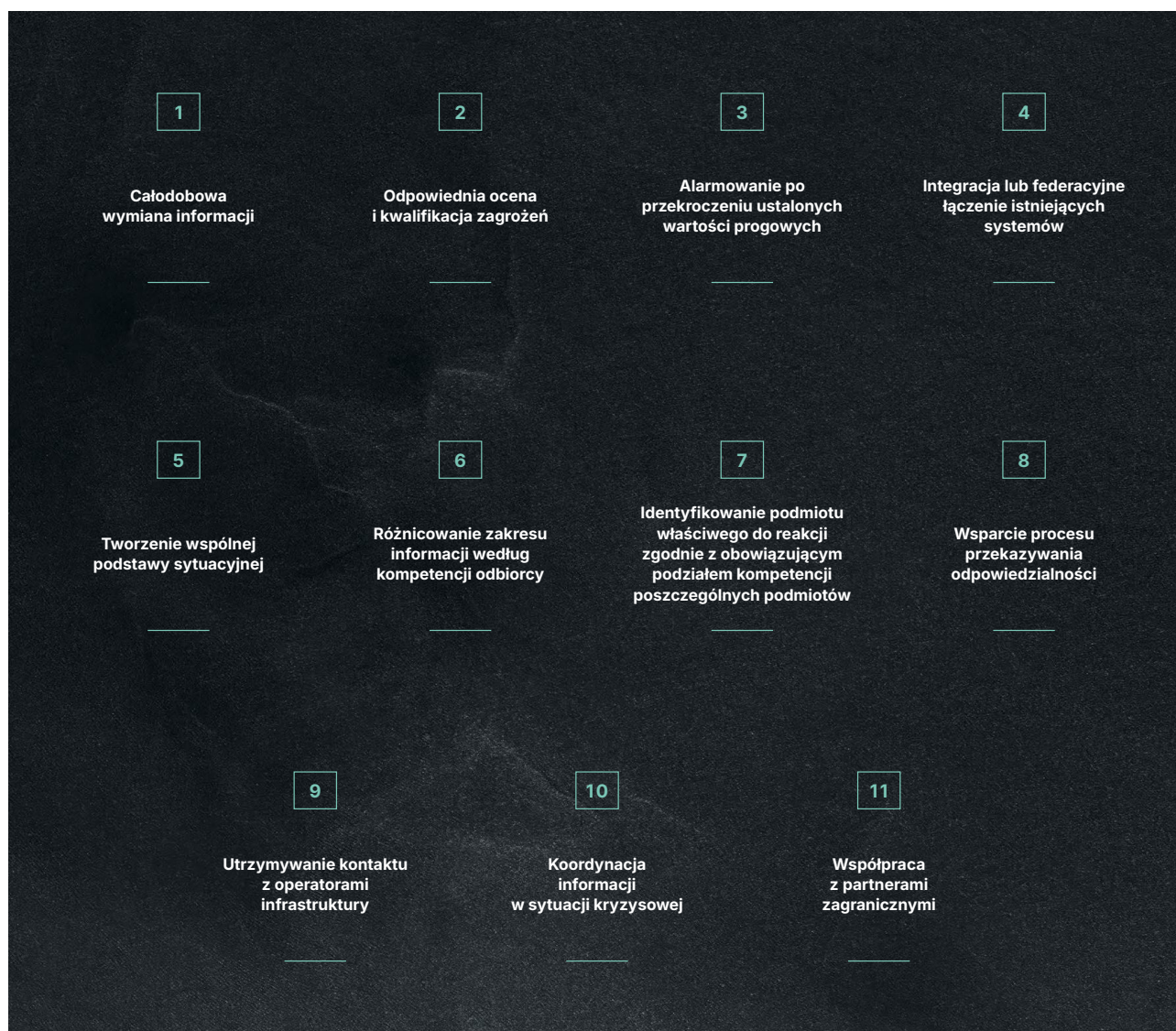
Najważniejszym wyzwaniem pozostaje brak w pełni ujednoliconego i przeciwiczonego mechanizmu łączącego informacje, kompetencje instytucjonalne i reakcję (dowodzenie i kierowanie działaniami na poziomie wielu resortów o nakładających się kompetencjach).

Centrum Bezpieczeństwa Morskiego: odpowiedź instytucjonalna w budowie

Część danych jest już integrowana w ramach Krajowego Systemu Bezpieczeństwa Morskiego, w tym poprzez System Wymiany Informacji Bezpieczeństwa Żeglugi i systemy VTS. Odrębne zdolności rozwija Straż Graniczna w ramach ZSRN. Obecna integracja nie obejmuje jednak w jednolity sposób wszystkich domen, użytkowników i etapów procesu prowadzącego od wykrycia zdarzenia do

reakcji. Powstające Centrum Bezpieczeństwa Morskiego (CBM) ma odpowiadać na potrzebę stałej wymiany informacji i koordynacji pomiędzy wojskiem, służbami, administracją morską oraz innymi podmiotami odpowiedzialnymi za bezpieczeństwo polskich obszarów morskich. Warto nadmienić, że OMMB stanowi zaplecze technologiczno-analityczne dla CBM w zakresie warstwy satelitarnej.

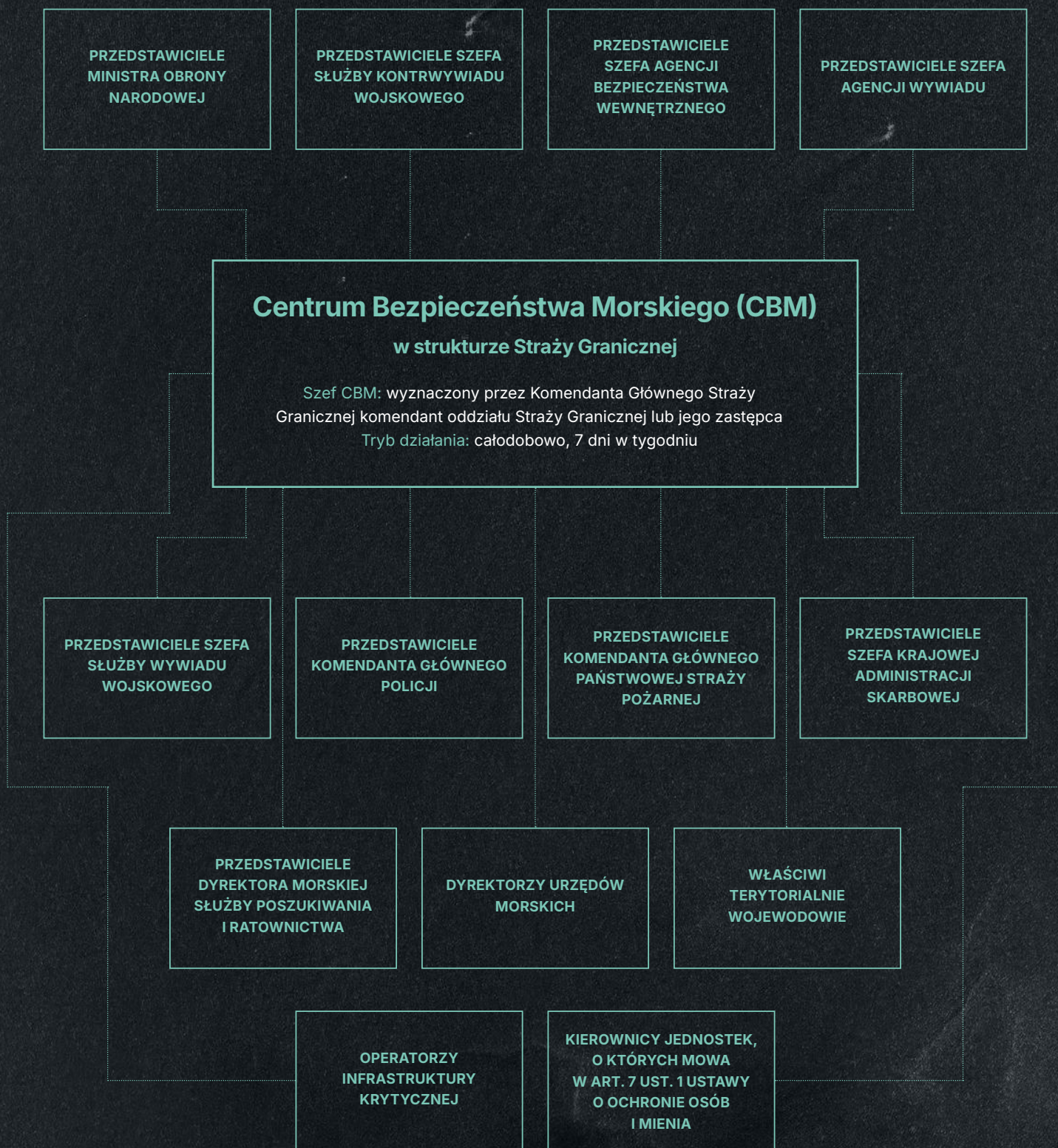
Ostateczny model funkcjonowania Centrum nie jest jeszcze w pełni ukształtowany. Można natomiast wskazać funkcje, które powinny zostać zapewnione niezależnie od przyjętej formuły organizacyjnej:



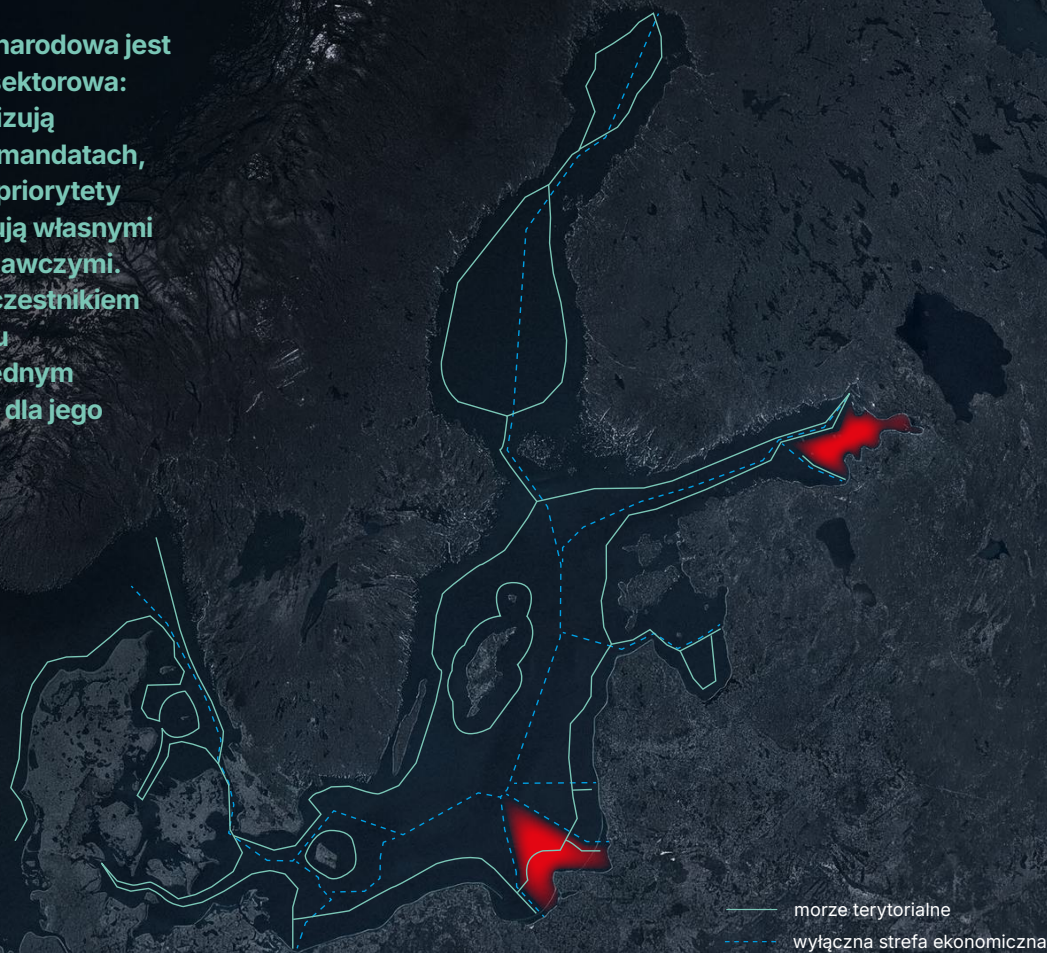
CBM może stać się krajowym węzłem systemu bezpieczeństwa morskigo, ale jego skuteczność nie będzie zależeć tylko od formalnego utworzenia instytucji. Decydujące będą rzeczywisty dostęp do danych, zdolność ich łączenia oraz jednoznaczne procedury dalszego działania.

Ustawowe podmioty Centrum Bezpieczeństwa Morskiego

Art. 25a–25d Ustawy o ochronie żeglugi i portów morskich



Współpraca międzynarodowa jest rozbudowana, lecz sektorowa: te same funkcje realizują struktury o różnych mandatach, a fora uzgadniające priorytety z reguły nie dysponują własnymi zdolnościami wykonawczymi. Rosja nie jest dziś uczestnikiem wspólnego porządku regionalnego, lecz jednym z głównych wyzwań dla jego bezpieczeństwa.



RAMY NADRZĘDNE

tworzą wspólne ramy regulacyjne i bezpieczeństwa dla ośmiu z dziewięciu państw nadbałtyckich

UE	Unia Europejska				
NATO	Organizacja Traktatu Północnoatlantyckiego · MCSCUI · Baltic Sentry				

ZDOLNOŚCI I MECHANIZMY OPERACYJNE

zapewniają systemy, dane, procedury lub struktury wykorzystywane w obserwacji i reagowaniu

CTF Baltic	Dowództwo Zespołu Zadaniowego – Bałtyk				
JEF	Połączone Siły Ekspedycyjne · Nordic Warden				
NORDEFCO	Nordycka współpraca obronna				
SUCBAS	Współpraca w regionie Morza Bałtyckiego w zakresie nadzoru morskigo				
MARSUR III	Sieć nadzoru morskigo Europejskiej Agencji Obrony				
EMSA	Europejska Agencja Bezpieczeństwa Morskigo · SafeSeaNet · CleanSeaNet · LRIT				
CISE	Wspólny mechanizm wymiany informacji dla obszarów morskich UE				
Frontex	Europejska Agencja Straży Granicznej i Przybrzeżnej				
EUROSUR	Europejski system nadzorowania granic				
BSRBCC	Współpraca Służb Granicznych Państw Regionu Morza Bałtyckiego				
HELCOM	Komisja Helsińska – Komisja Ochrony Środowiska Morskigo Bałtyku				

KOORDYNACJA POLITYCZNA I REGIONALNA

wypracowują stanowiska, plany i standardy, ale wykonanie należy do państw

Shadow Fleet TF	Grupa Zadaniowa G7/NB8++ ds. floty cieni				
CBSS	Rada Państw Morza Bałtyckiego				
EUSBSR	Strategia Unii Europejskiej dla Regionu Morza Bałtyckiego				
VASAB	Komitet Rozwoju Przestrzennego Regionu Morza Bałtyckiego				
BSPC	Konferencja Parlamentarna Morza Bałtyckiego				
BSSSC	Subregionalna Organizacja Współpracy Państw Morza Bałtyckiego				
NB8	Nordycko-bałtycka ósemka				
B3	Zgromadzenie Bałtyckie i Bałtycka Rada Ministrów				

bezpieczeństwo i odporność	obraz sytuacji i dane morskie	środowisko	koordynacja i rozwój regionu
•	•	•	•
•	•	○	
•	•		
•	•	○	
•	•	•	
○	•	○	
•	•		
•	•		
•	•	•	
	○	•	
•	•	•	
•			•
•		•	•
•		•	•
○		○	•
○		•	•
•			•
•			•

• funkcja podstawowa ○ funkcja wspierająca

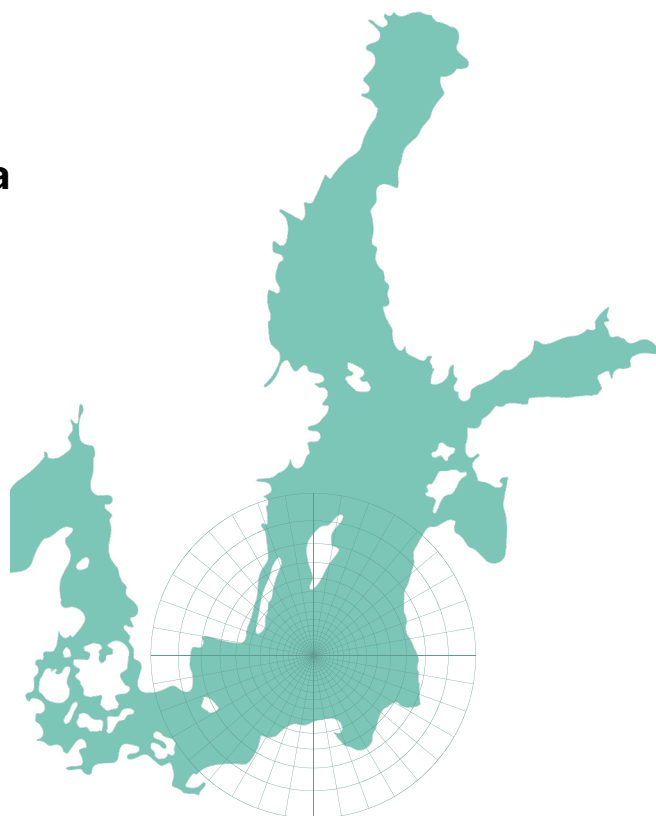
Współpraca międzynarodowa: rozbudowana, lecz wielowarstwowa

Transgraniczny charakter Bałtyku sprawia, że system krajowy musi współpracować z partnerami regionalnymi. Jednostki przemieszczają się pomiędzy jurysdykcjami, infrastruktura łączy kilka państw, a skutki incydentów mogą obejmować cały region.

Współpraca odbywa się w wielu równoległych ramach wojskowych, granicznych, administracyjnych, środowiskowych i organizacyjnych.

Obejmuje m.in.:

- **współpracę administracji i straży granicznych** – wymiana danych operacyjnych jest jednym z głównych czynników warunkujących skuteczność służb granicznych państw członkowskich Unii Europejskiej. Szczególną rolę w ochronie jednej z najdłuższych granic zewnętrznych UE, choćby w zakresie analizy ryzyka, odgrywa współpraca z Europejską Agencją Straży Granicznej i Przybrzeżnej (Frontex);
- **współpracę wywiadowczą** – stanowiąc jeden z filarów utrzymania bezpieczeństwa, wymiana danych operacyjnych zyskuje na znaczeniu w obliczu stosowania niekonwencjonalnych środków charakterystycznych dla działań hybrydowych;
- **mechanizmy NATO dotyczące ochrony infrastruktury podmorskiej** – zintensyfikowana działalność Sojuszu ukierunkowana na zabezpieczenie obiektów dolnej półsfery wymaga aktywnego udziału polskich podmiotów państwowych w przekazywaniu informacji o zagrożeniach właściwym komórkom NATO (Maritime Centre for Security of Critical Undersea Infrastructure – MCSCUI), procesie ich analizy i formułowania wniosków oraz rekomendacji, a także w odbieraniu, dystrybucji i wdrażaniu wypracowywanych na tym poziomie rozwiązań;
- **unijne systemy wymiany informacji morskiej** – Europejska Agencja Bezpieczeństwa Morskiego (EMSA) wraz z centrum danych systemu identyfikacji i śledzenia statków dalekiego zasięgu Unii Europejskiej oraz unijnym systemem wymiany informacji morskich (SafeSeaNet) stanowią narzędzia ujednolicania standardów i poziomu bezpieczeństwa morskiego. Niezwykle istotna jest tu rola UE jako regulatora w ujednolicaniu przepisów prawa;



- **współpracę środowiskową i ratowniczą** – ochrona wrażliwego ekosystemu półzamkniętego Morza Bałtyckiego wymaga wykorzystania istniejących mechanizmów monitorowania i reagowania, w tym rozwijanych w ramach Komisji Ochrony Środowiska Morskiego Bałtyku (HELCOM). Skala ruchu towarowego i pasażerskiego oraz ryzyko poważnych zdarzeń ekologicznych mogą przekraczać zdolności reagowania pojedynczych państw, dlatego ścisła koordynacja międzynarodowa pozostaje warunkiem skutecznego działania;
- **dwustronne i regionalne kontakty operacyjne**, które zwiększają zaufanie i pozwalają na wypracowanie szybkich kanałów powiadamiania oraz wymiany doświadczeń i dobrych praktyk.

Nie tworzą jednak jednego, ciągłego mechanizmu wymiany informacji, utrzymywania obserwacji i przekazywania odpowiedzialności za reakcję. Poszczególne mechanizmy działają na podstawie odmiennych mandatów, standardów i poziomów dostępu. Współpraca jest więc rozbudowana, ale nadal sektorowa i wielowarstwowa. Warunkiem skutecznej współpracy międzynarodowej jest uporządkowanie systemu krajowego: określenie, jakie informacje mogą być przekazywane, kto odpowiada za ich weryfikację oraz kto utrzymuje kontakt operacyjny podczas incydentu przekraczającego granice państwowe.

Podsumowanie: warunki wspólnego obrazu sytuacji

System docelowy powinien:

1

integrować i korelować dane z różnych źródeł, w tym z nowoczesnych sensorów i platform działających we wszystkich przestrzeniach domeny morskiej (stacjonarnych i mobilnych)

4

wykrywać anomalie

2

zachowywać informacje o źródle, czasie i wiarygodności (gromadzenie rzetelnych danych, potwierdzanych w różnych, niezależnych źródłach)

5

różnicować zakres informacji zależnie od roli odbiorcy

3

rejestrować historię obiektu i zdarzenia (archiwizacja jako element dokumentowania i gromadzenia materiałów dowodowych na potrzeby działań procesowych)

6

umożliwiać bezpieczny import i eksport danych (cyberbezpieczeństwo)

7

wskazywać podmiot właściwy
do reakcji

10

zapewniać dostęp do bazy danych
analitycznych

8

wspierać procesy decyzyjne, w tym
dowodzenie i kierowanie działaniami
interwencyjnymi

11

mieć otwartą architekturę,
umożliwiającą integrację nowych
elementów

9

umożliwiać przekazywanie
odpowiedzialności za prowadzenie
sprawy bez utraty ciągłości informacji
i aktualności obrazu sytuacji

12

umożliwiać generowanie scenariuszy
do szkolenia operatorów systemów
oraz prowadzenia symulacji na różnych
poziomach kierowania i dowodzenia
działaniami

Wspólna warstwa obserwacji musi być odporna także na degradację własnych zdolności – cyberataki, zakłócenia GNSS i łączności, utratę pojedynczych sensorów oraz manipulację danymi wejściowymi. Architektura powinna więc ograniczać ryzyko pojedynczych punktów awarii dzięki redundancji źródeł, sieci transmisji i dostawców oraz możliwości wzajemnego zastępowania sensorów i ścieżek dostępu do danych.

Digital Baltic i architektura wspólnego obrazu



Anna Salomon

Członek Zarządu



Przemysław Pozański

Dyrektor Rozwoju Platform i Systemów

Zapewnienie bezpieczeństwa infrastruktury morskiej – nie tylko tej krytycznej – to podstawowe zadanie wielu służb i instytucji, zarówno publicznych, jak i prywatnych. Do tej pory organizacje te działały asynchronicznie, wymieniając się niezbędnymi informacjami bezpośrednio między sobą za pośrednictwem tradycyjnych kanałów komunikacji. Przyspieszenie i standaryzowanie tej komunikacji na jednej platformie technologicznej jest dziś kluczowym wyzwaniem architektury bezpieczeństwa morskiego.

Integracja nie oznacza jednak zastąpienia istniejących rozwiązań jednym, nowym systemem. Systemy wojskowe, administracyjne, operatorskie i służbowe powstały dla różnych zadań, pozostają własnością różnych podmiotów i podlegają odmiennym rygorom dostępu do informacji, w tym różnym klauzulom niejawności. **Zadaniem integratora jest doprowadzenie do ich współdziałania bez pozbawiania właścicieli kontroli nad własnymi systemami i danymi przy zachowaniu autonomii istniejących rozwiązań oraz kompetencji ich właścicieli.**

INTEGRACJA ODBYWA SIĘ NA INTERFEJSACH

Najtrudniejszym elementem nie jest samo techniczne podłączenie kolejnego źródła danych. Problem pojawia się na styku systemów i organizacji: trzeba określić, jakie informacje mogą zostać wymienione, w jakiej postaci, z jakim poziomem wiarygodności, do jakiego użytkownika i na jakim etapie zdarzenia.

Dlatego architektura platformy Digital Baltic uwzględnia separację informacji jawnych i niejawnych oraz mechanizmy kontroli dostępu, zarządzania rolami użytkowników i audytu. Zakres informacji różnicowany jest zgodnie z rolą, kompetencjami i poziomem uprawnień użytkownika, a integracja z systemami partnerów ma charakter dwukierunkowy: platforma zarówno odbiera dane, jak i dystrybuje alerty do upoważnionych odbiorców. To rozróżnienie ma zasadnicze znaczenie: interoperacyjność informacyjna nie jest tym samym co wspólne dowodzenie. System może zapewnić ciągłość informacji pomiędzy instytucjami, lecz nie zastępuje rozstrzygnięcia co do kwalifikacji prawnej zdarzenia, użycia sił czy wydania decyzji administracyjnej – te pozostają w kompetencji uprawnionych podmiotów.

CIĄGŁOŚĆ INFORMACJI PRZY ZMIANIE PODMIOTU PROWADZĄCEGO

Kluczem do zapewnienia bezpieczeństwa na Bałtyku nie jest dziś samo posiadanie danych, lecz zdolność do ich błyskawicznej selekcji i umiejętnego przetwarzania. Warstwa integracyjna powinna zatem przede wszystkim utrzymywać ciągłość informacji o obiekcie i zdarzeniu w sytuacji, gdy zmienia się właściwy użytkownik. Incydent może zmieniać swój charakter wraz z rozwojem sytuacji i przechodzić pomiędzy obszarami odpowiedzialności różnych podmiotów. Nietypowe zachowanie jednostki może zostać początkowo ocenione jako kwestia bezpieczeństwa żegluga, następnie wymagać działania Straży Granicznej, a w dalszej kolejności zo-



Ustandaryzowanie komunikacji na jednej platformie technologicznej jest kluczowym wyzwaniem architektury bezpieczeństwa morskiego.

stać zakwalifikowane jako zagrożenie dla infrastruktury krytycznej lub bezpieczeństwa państwa.

Na każdym z tych etapów zmienia się podmiot odpowiedzialny za działanie, lecz nie powinny być tracone historia zdarzenia, źródła informacji ani jego aktualny kontekst. Zdolność do przekazywania sprawy pomiędzy użytkownikami bez utraty obrazu sytuacji jest jednym z warunków skuteczności systemu.

INTEGRATOR MUSI PROJEKTOWAĆ Z UŻYTKOWNIKIEM

Takiej architektury nie da się zaprojektować wyłącznie na podstawie parametrów technicznych. Trzeba poznać rzeczywisty sposób pracy instytucji: sposoby i okoliczności przekazywania informacji, progi eskalacji, ograniczenia w udostępnianiu danych i potrzeby poszczególnych użytkowników.

Dlatego w rozwój Digital Baltic zaangażowani byli przedstawiciele Sił Zbrojnych RP, Straży Granicznej, administracji państwowej, służb mundurowych oraz operatorów infrastruktury krytycznej. Funkcjonalności projektowano na podstawie rzeczywistych potrzeb operacyjnych i weryfikowano podczas ćwiczeń typu Table Top Exercise (TTX). W takim zastosowaniu TTX pozwala weryfikować przepływ informacji pomiędzy użytkownikami, momenty przekazywania odpowiedzialności, procedury eskalacji oraz funkcjonalności wymagane na kolejnych etapach obsługi zdarzenia.

Warstwa integracyjna musi być również otwarta na nowe źródła informacji. W przypadku Digital Baltic

dotyczy to m.in. danych satelitarnych SAR i produktów powstających w wyniku ich automatycznej analizy. Ich znaczenie wzrasta wraz z rozwojem krajowych zdolności rozpoznania satelitarnego, w tym wojskowej konstelacji radarowej POLSARIS.

KRAJOWA WARSTWA INTEGRACYJNA

Kompetencja integracyjna Ośrodka Badawczo-Rozwojowego Centrum Techniki Morskiej SA, powołanego w 1982 r. i wchodzącego w skład Polskiej Grupy Zbrojeniowej, wyrasta z projektów realizowanych dla Marynarki Wojennej i Sił Zbrojnych RP. W systemach okrętowych integracja polega na zapewnieniu, że sensory, system dowodzenia i elementy wykonawcze tworzą jeden układ. Ta sama logika przenosi się z poziomu pojedynczej platformy na poziom całego systemu bezpieczeństwa morskiego: wiele autonomicznych elementów zachowuje swoje funkcje, wymieniając jednocześnie informacje w sposób, który pozwala osiągnąć wspólny efekt operacyjny.

Digital Baltic powstaje z myślą o wsparciu zadań Centrum Bezpieczeństwa Morskiego poprzez integrację istniejących systemów, usprawnienie analizy informacji oraz współpracy podmiotów odpowiedzialnych za bezpieczeństwo polskich obszarów morskich.

Z perspektywy integratora zasadniczym wyzwaniem nie jest już pozyskanie kolejnego źródła danych, lecz zapewnienie, aby istniejące systemy potrafiły przekazać sobie właściwą informację bez utraty czasu, kontekstu i odpowiedzialności.

4 | Od anomalii do reakcji.

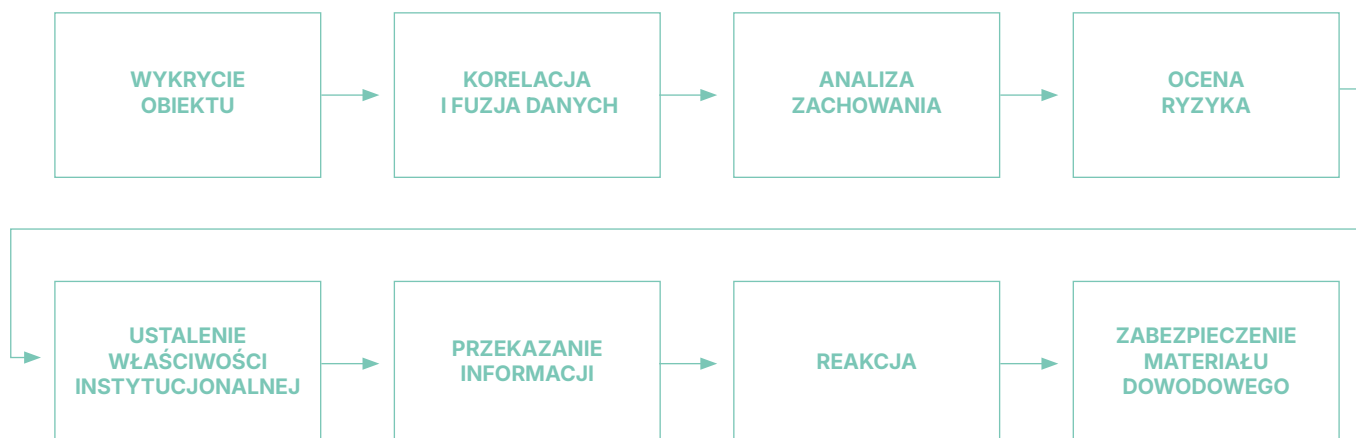
Incydent jako test systemu

Wykrycie nietypowej aktywności jest dopiero początkiem procesu. Rzeczywistym testem systemu bezpieczeństwa morskiego jest czas i jakość przejścia od pojawienia się pierwszej wiarygodnej przesłanki anomalii do adekwatnej reakcji.

W środowisku działań poniżej progu wojny pełne ustalenie zamiaru i przypisanie działania konkretnemu podmiotowi może być niemożliwe w czasie

określonym w procedurach reagowania na konkretne sytuacje. Wynika to z niejednoznacznego charakteru działań strony przeciwnej. System musi zatem rozpoznawać narastające ryzyko i stopniować reakcję, zanim wystąpią nieodwracalne skutki. Na Bałtyku ma to wyjątkowe znaczenie: potencjalny sprawca zmienia rejon działania lub opuszcza jurysdykcję państwa w ciągu kilku godzin.

W teorii proces powinien być oceniany jako jeden spójny ciąg, np.:



W praktyce nie jest on realizowany przez jeden podmiot ani w jednym systemie. Jego poszczególne etapy są rozdzielone między wojsko, służby, administrację i operatorów infrastruktury, dlatego skuteczność zależy nie tylko od dostępności informacji, lecz także od progów uruchamiania kolejnych działań, zasad przekazywania odpowiedzialności za prowadzenie działań i czasu podejmowania decyzji. Przypadek MV SUN pozwala przeanalizować te zależności na przykładzie rzeczywistego zdarzenia.

Celem studium nie jest rozstrzygnięcie, czy jednostka przygotowywała akt sabotażu. Służy ono sprawdzeniu, jak działa system w sytuacji typowej dla presji poniżej progu wojny: gdy zachowanie jest w pełni obserwowalne, a zamiar pozostaje nieznanym.

PRZYPADEK MV SUN



Czas	12–22 maja 2025 r.
Obszar	Bałtyk właściwy, w tym polska WSE i rejon przebiegu SwePol Link
Jednostka	MV SUN, zbiornikowiec typu suezmax, rok budowy: 2005, bandera Antigui i Barbudy, IMO 9293117, zaliczana do floty cieni
Anomalia	odejście od trasy, zmniejszenie prędkości do około 2,5 w, wielokrotne manewry przy strategicznej infrastrukturze podmorskiej
Skutek	brak uszkodzeń infrastruktury



MV SUN

SwePol Link



12–14.05.2025

Według rekonstrukcji trasy AIS MV SUN manewruje w okolicach kabli podmorskich Energinet LyngsÅ–Læsø oraz GlobalConnect 2 (GC2), położonych w wyłączonej strefie ekonomicznej Królestwa Danii.

15.05.2025

Jednostka wpływa na Bałtyk przez cieśniny duńskie (Kattegat, Wielki Belt). Kieruje się kursem na Zatokę Fińską, wykorzystując trasę żeglugową pomiędzy wybrzeżem szwedzkim a Bornholmem.

16.05.2025

Po minięciu Stenshamn, na wysokości Olandii, jednostka zmniejsza prędkość i wykonuje zwrot na południe, opuszczając tor żeglugowy.

16–20.05.2025

Jednostka wykonuje kilkanaście manewrów polegających na cyklicznym zbliżaniu się do rejonu przebiegu połączenia SwePol Link. Pierwsze wejście na kontrkurs następuje nad ranem 17.05. Od tego czasu jednostka kilkakrotnie przecina trasę ułożenia kabla, raz za razem wchodząc w obszar polskiej WSE i opuszczając go.

ANALIZA

Możliwe kwalifikacje

Na podstawie samej trajektorii AIS nie można rozstrzygnąć zamiaru jednostki. System powinien być zdolny do równoległego rozpatrywania trzech hipotez:

- zdarzenie o charakterze niewrogim – przyczyny techniczne, nawigacyjne lub eksploatacyjne;
- działanie rozpoznawcze – rozpoznanie infrastruktury, wzorców obserwacji albo reakcji państwa;
- przygotowanie do oddziaływania – stworzenie warunków do uszkodzenia infrastruktury lub pozostawienia w jej pobliżu urządzenia.

Skutek zdarzenia MV SUN – brak uszkodzeń – nie pozwala rozstrzygnąć, która z tych hipotez jest trafna. Nie wiadomo, czy nic się nie stało, ponieważ nic nie było zamierzone, czy dlatego, że demonstracja obecności zadziałała odstraszająco.

Brak pewności co do zamiaru nie może oznaczać bierności, lecz prowadzić do adekwatnej reakcji. Im więcej niezależnych sygnałów ryzyka występuje jednocześnie, tym intensywniejsza powinna być obserwacja, weryfikacja i obecność sił.

Status sankcyjny jako wskaźnik opóźniony

W chwili rozpoczęcia manewrów MV SUN nie był jeszcze objęty sankcjami UE, choć jego profil ryzyka był już rozpoznawany. 11 kwietnia 2025 r. Ukraina objęła sankcjami kapitana jednostki, a ukraiński wywiad klasyfikował ją jako element floty cieni. Sam statek został objęty sankcjami UE 21 maja 2025 r., już po opuszczeniu rejonu SwePol Link. Status sankcyjny nie może więc

pełnić funkcji podstawowego wskaźnika operacyjnego. Ocena ryzyka musi uwzględniać także profil jednostki i jej bieżące zachowanie, m.in. trasę, prędkość, powtarzalność manewrów oraz położenie i zachowanie względem chronionej infrastruktury.

Podstawa prawna reakcji zależy od miejsca zdarzenia

W czasie gdy doszło do incydentu w rejonie SwePol Link, nie istniał reżim strefy bezpieczeństwa, który pozwalałby kwalifikować samo manewrowanie jednostki jako naruszenie ustanowionego zakazu. Po incydencie ochrona została wzmocniona: zarządzeniem z 8 lipca 2025 r. ustanowiono 250-metrową strefę bezpieczeństwa wzdłuż odcinka kabla przebiegającego przez polskie morze terytorialne, z zakazem m.in. kotwiczenia, nurkowania i prowadzenia prac podwodnych. Strefa nie obejmuje jednak odcinka SwePol Link położonego w polskiej WSE. Zmiana ograniczyła więc lukę regulacyjną, ale nie usuwa problemu kwalifikacji i reakcji na podejrzane zachowanie jednostki w rejonie infrastruktury położonej poza morzem terytorialnym.

MV SUN JAKO TEST SYSTEMU

Przypadek ujawnia trzy odrębne problemy. Po pierwsze, rozpoznanie ryzyka nie może zależeć od formalnego statusu sankcyjnego jednostki – sygnały behawioralne i profil ryzyka mogą pojawić się wcześniej. Po drugie, możliwość reakcji zależy nie tylko od rozpoznania zagrożenia, ale też od miejsca zdarzenia i dostępnych podstaw prawnych. Po trzecie, zasadniczą zmienną operacyjną pozostaje czas potrzebny do przejścia od



18.05.2025

W odległości około 30 Mm na południe, na wodach terytorialnych manewrują okręt rakietowy ORP Orkan oraz jednostka Straży Granicznej SG-111. Brak publicznie dostępnych informacji o ich zadaniach w związku z MV SUN.

20.05.2025

Jednostka zostaje rozpoznana. Dowódca Operacyjny RSZ poleca wykonanie lotu patrolowego – w rejon kierowany jest samolot M28B Bryza. W godzinach popołudniowych MV SUN odchodzi kursem na północ, wraca na trasę żeglugową i kontynuuje rejs. Tego samego dnia Siły Zbrojne Szwecji informują, że jednostki NATO zidentyfikowały statek manewrujący w sposób budzący podejrzenia w pobliżu podmorskiej infrastruktury krytycznej.

21-22.05.2025

Oficjalna reakcja władz RP. W rejon kieruje się okręt hydrograficzny ORP Heweliusz z zadaniem sprawdzenia sytuacji. PSE potwierdzają prawidłową pracę SwePol Link.



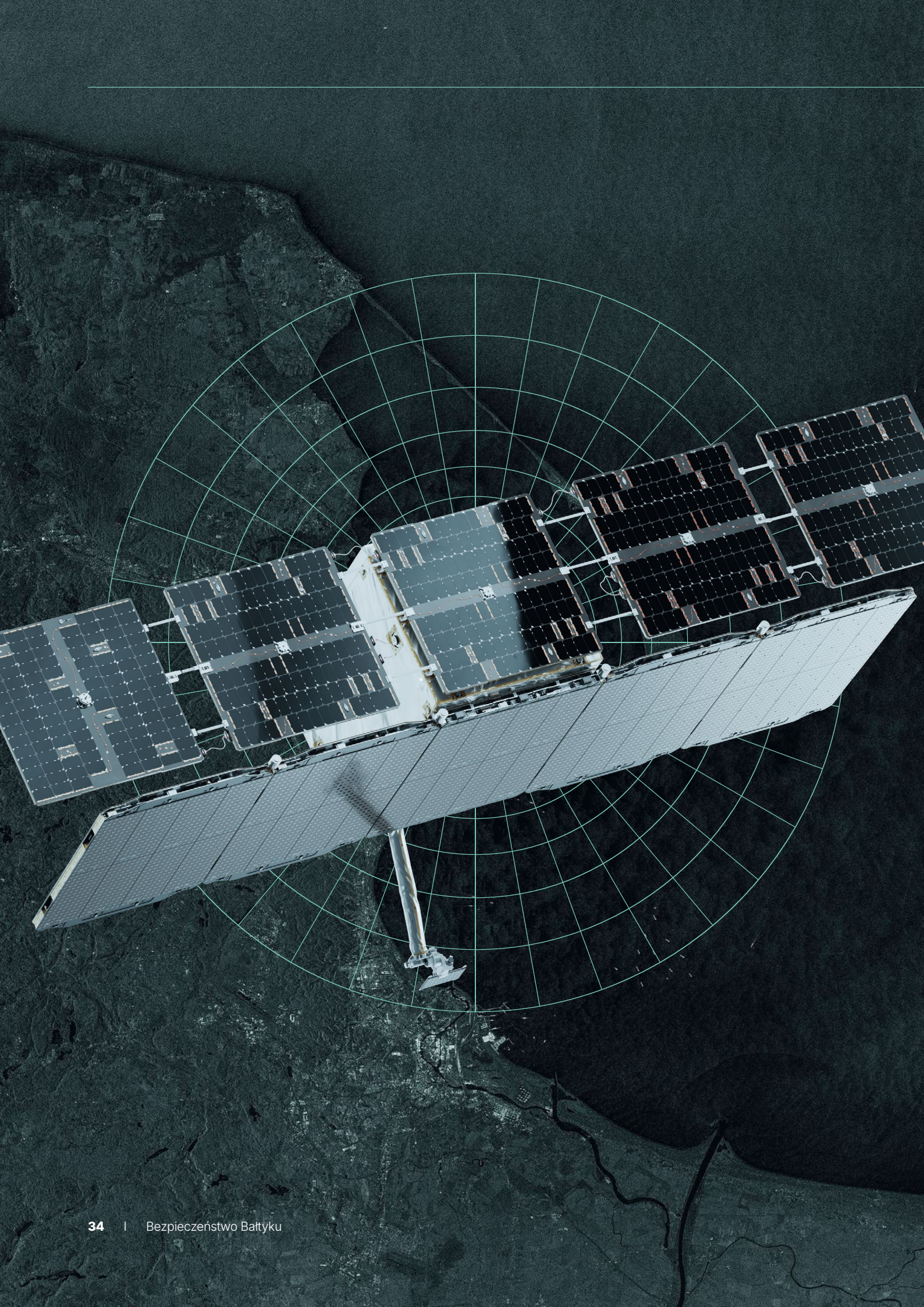
anomalii, przez jej weryfikację i ocenę, do decyzji. Na podstawie publicznie dostępnych informacji nie można ustalić, kiedy polskie instytucje po raz pierwszy uznały zachowanie MV SUN za anomalię ani jakie działania prowadzono przed 20 maja. Nie ma więc podstaw do twierdzenia, że państwo wcześniej pozostawało bierne. Istotnym pytaniem systemowym pozostaje natomiast czas od pojawienia się wiarygodnych przesłanek ryzyka do uruchomienia adekwatnej reakcji.

Od chwili wystąpienia incydentu zmieniły się elementy otoczenia prawnego i instytucjonalnego: rozszerzono uprawnienia Sił Zbrojnych w zakresie bezpieczeństwa polskich obszarów morskich, rozwijany jest ZSRN 2.0, a uruchomienie CBM jest planowane na 2027 r. Dlatego MV SUN powinien być traktowany jako scenariusz referencyjny dla projektowanego systemu, a nie jako rozliczenie decyzji podjętych w 2025 r.

Czy po wdrożeniu nowych rozwiązań analogiczna anomalia zostanie rozpoznana, zweryfikowana i zakwalifikowana, a adekwatna reakcja wobec niej zostanie podjęta w czasie liczącym w godzinach, a nie w dobach?

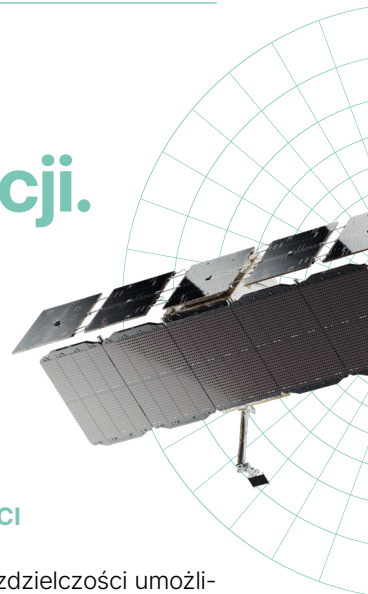
Miarą skuteczności systemu jest nie tylko sam czas wykrycia jednostki, ale też czas od pojawienia się pierwszych wiarygodnych przesłanek anomalii do odpowiedniej reakcji. Należy zakładać, że sprawność systemu i determinacja państwa będą poddawane kolejnym próbom. Odpowiednio wczesne wykrycie zagrożenia – zarówno przy użyciu własnych środków, jak i dzięki współpracy transgranicznej – oraz jego właściwa kwalifikacja pozwalają na podjęcie skoordynowanej reakcji mimo ograniczonych zasobów i rosnących kosztów operacyjnych.





5 | Wspólna warstwa obserwacji.

Rola technologii satelitarnych na Bałtyku



Technologie satelitarne pozwalają ograniczyć wiele luk ujawnionych w dotychczasowym systemie bezpieczeństwa morskiego. Umożliwiają obserwację rozległych obszarów, weryfikację informacji pochodzących ze źródeł kooperujących, przede wszystkim z AIS, uzupełniają monitoring brzegowy i operatorski oraz dostarczają porównywalnych danych wielu użytkownikom.

Ich rolą nie jest jednak zastępowanie istniejących sensorów ani tworzenie odrębnego systemu obserwacji. Największą wartość uzyskują jako wspólna warstwa zintegrowana z AIS, radarami brzegowymi, systemami wojskowymi, monitoringiem infrastruktury oraz informacjami administracyjnymi i środowiskowymi.

Technologia satelitarna może zatem wzmacniać zdolności obserwacyjne i cały proces prowadzący od wykrycia obiektu do oceny sytuacji i podjęcia działania.

CHARAKTERYSTYKA ZDOLNOŚCI OBSERWACYJNYCH

Obrazowanie optyczne wysokiej rozdzielczości umożliwia szczegółową interpretację obiektów i warunków na powierzchni morza, ale jego użyteczność ograniczają na Bałtyku zachmurzenie, mgła i brak światła dziennego. Systemy radarów z syntetyczną aperturą (Synthetic Aperture Radar, SAR) rejestrują sygnał radarowy odbity od powierzchni i obiektów, dzięki czemu mogą prowadzić obserwację niezależnie od pory dnia i przy dużym zachmurzeniu.

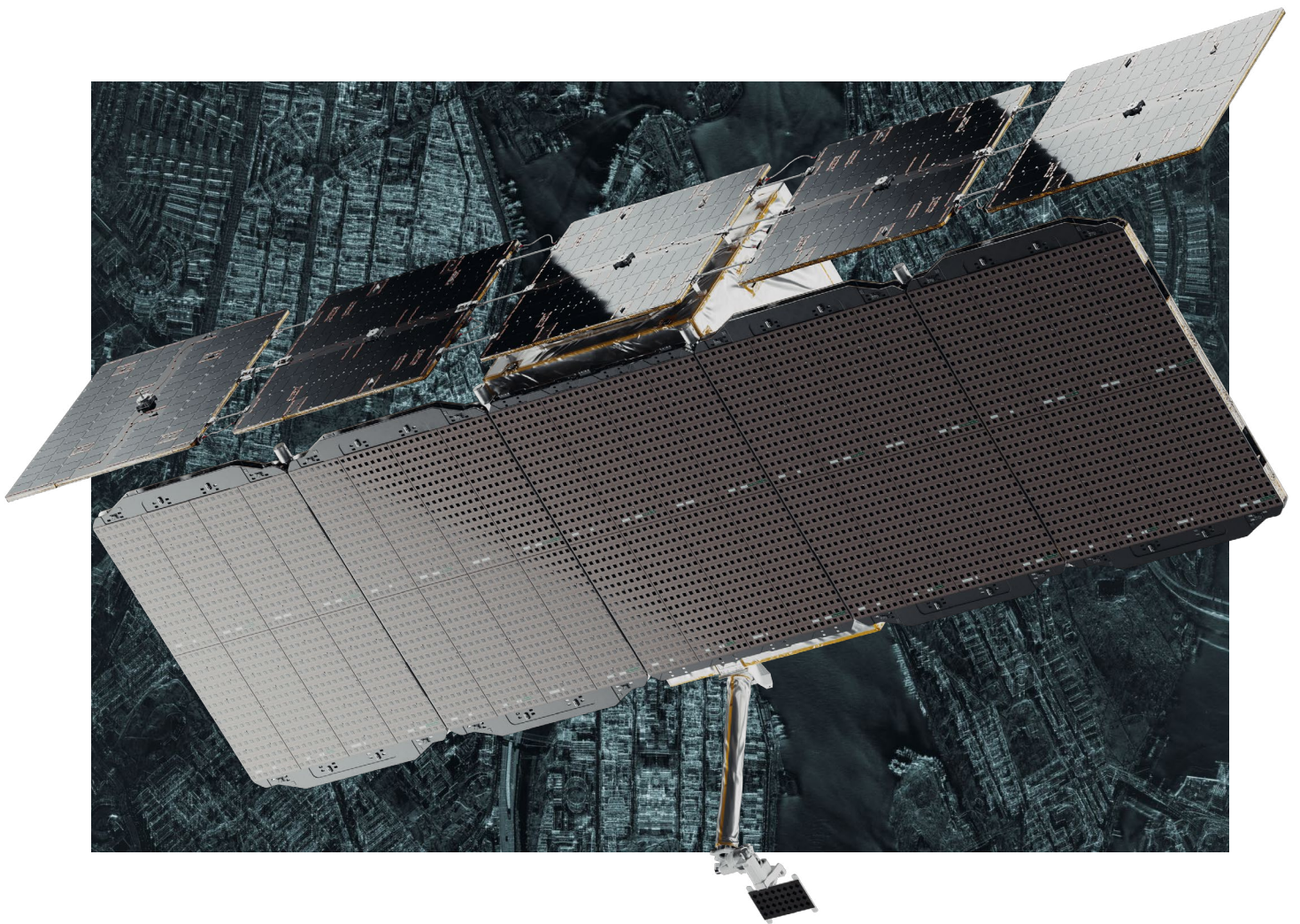
W warunkach bałtyckich dane SAR są szczególnie użyteczne do monitorowania rozległych akwenów, wykrywania jednostek oraz kontroli obszarów położonych poza efektywnym zasięgiem sensorów brzegowych. Powinny być wykorzystywane łącznie z AIS, radarami brzegowymi, systemami optycznymi i monitoringiem operatorskim.

ZAKRES INFORMACJI MOŻLIWYCH DO POZYSKANIA

Obrazowanie satelitarne może wspierać:



Poziom szczegółowości obserwacji może być dostosowany do zadania: tryby szerokoobszarowe służą do monitorowania dużych akwenów, a zobrazowania o wyższej rozdzielczości – do analizy wybranych obiektów i rejonów.



Pełny obraz sytuacji powstaje poprzez fuzję danych. Zobrazowania satelitarne potwierdzają obecność obiektów, AIS dostarcza deklarowane dane identyfikacyjne i nawigacyjne, radary umożliwiają ich śledzenie, systemy optyczne wspierają identyfikację, a monitoring operatorski i platformy bezzałogowe uzupełniają ocenę sytuacji w rejonie zainteresowania. Ochrona infrastruktury podmorskiej wymaga dodatkowo danych z sensorów hydroakustycznych, sonarów oraz systemów UUV/AUV i ROV, ponieważ zobrazowanie satelitarne nie pozwala bezpośrednio ocenić zdarzeń zachodzących na dnie morza. Narzędzia wykorzystujące sztuczną inteligencję mogą dodatkowo wspierać automatyczne wykrywanie i klasyfikację obiektów, identyfikowanie zmian pomiędzy kolejnymi zobrazowaniami oraz typowanie anomalii wymagających dalszej analizy przez człowieka. Połączenie tych elementów pozwala przejść od detekcji pojedynczego obiektu do analizy jego zachowania, oceny kontekstu operacyjnego i przygotowania produktu informacyjnego dla odpowiedniego odbiorcy.

ŁAŃCUCH WYKORZYSTANIA DANYCH

Operacyjne wykorzystanie danych satelitarnych obejmuje następujący proces:

zadaniowanie → pozyskanie zobrazowania → przetworzenie → detekcja obiektów → korelacja z innymi źródłami

→ analiza zachowania → ocena ryzyka → przygotowanie produktu informacyjnego → dystrybucja → decyzja. Rozstrzygające znaczenie ma czas przejścia pomiędzy kolejnymi etapami oraz jednoznaczne przypisanie odpowiedzialności za analizę, zatwierdzenie i przekazanie informacji.

ROZWIĄZANIA DLA POSZCZEGÓLNYCH UŻYTKOWNIKÓW

Zakres informacji powinien odpowiadać kompetencjom i zadaniom odbiorcy.

Marynarka Wojenna potrzebuje danych wspierających rozpoznany obraz sytuacji morskiej, śledzenie obiektów i planowanie działań. Straż Graniczna potrzebuje informacji umożliwiających identyfikację jednostki, typowanie jej do kontroli oraz kierowanie sił interwencyjnych. Administracja morska wykorzystuje dane do oceny bezpieczeństwa żeglugi i zarządzania ruchem. Operator infrastruktury powinien otrzymywać alerty dotyczące konkretnego aktywa i charakteru zagrożenia. Morska Służba Poszukiwania i Ratownictwa potrzebuje informacji o położeniu obiektów i warunkach prowadzenia akcji. Partnerzy zagraniczni powinni otrzymywać zweryfikowany zakres danych niezbędny do utrzymania ciągłości obserwacji po wejściu jednostki w obszar innej jurysdykcji.

Nie wszyscy użytkownicy potrzebują dostępu do pełnego zobrazowania czy pełnego zbioru danych źródłowych. Zakres dystrybucji powinien uwzględniać ochronę informacji niejawnych, wrażliwych danych operatorskich oraz właściwe oznaczenia i ograniczenia udostępniania.

Dostępne są także rozwiązania komercyjne dla operatorów infrastruktury umożliwiające monitorowanie określonego obszaru morza (np. morska farma wiatrowa w dyspozycji konkretnego operatora).

Dalszy rozwój systemu powinien obejmować automatyczną fuzję danych, wykrywanie anomalii i generowanie produktów dostosowanych do odbiorcy. Modele uczenia maszynowego mogą wspierać analizę ruchu i priorytetyzację alertów, a modele językowe – porządkować i prezentować informacje w sposób dostosowany do odpowiednich użytkowników. Wyniki powinny wskazywać źródła i poziom pewności oraz podlegać weryfikacji analitycznej.

INTEGRACJA Z SYSTEMEM KRAJOWYM

Dane satelitarne powinny zasilać istniejące środowisko informacyjne, w tym KSBM wraz z Systemem Wymiany Informacji Bezpieczeństwa Żegluga (SWIBŻ) i systemami VTS, ZSRN, systemy wojskowe, rozwiązania operatorskie oraz przyszłe funkcje CBM.

Architektura integracyjna powinna zapewniać:

- automatyczny import danych i produktów analitycznych;
- korelację z AIS i innymi źródłami;
- zarządzanie poziomami dostępu;
- rejestrowanie źródła, czasu pozyskania i historii przetwarzania informacji;
- kontrolowane udostępnianie produktów uprawnionym użytkownikom krajowym i zagranicznym;
- archiwizację danych na potrzeby analizy, postępowania i odtwarzania przebiegu zdarzeń.

CZYNNIKI DECYDUJĄCE O SKUTECZNOŚCI

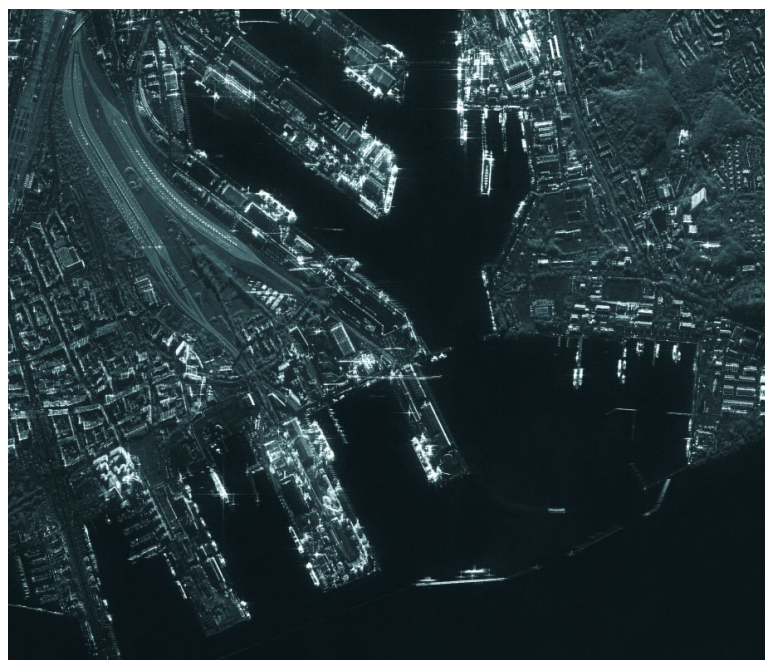
O wartości operacyjnej danych satelitarnych decyduje nie tylko jakość zobrazowania, lecz przede wszystkim czas od zgłoszenia potrzeby obserwacji do dostarczenia informacji użytecznej w procesie decyzyjnym. Składają się na niego: rzeczywista dostępność satelity dla danego zadania, możliwość priorytetowego zadaniowania satelity, wykonanie obserwacji, transmisja do segmentu naziemnego, przetworzenie, analiza oraz dystrybucja produktu do właściwego użytkownika. Parametry te należy rozpatrywać łącznie z częstotliwością rewizyt, trybem obrazowania, rozdzielczością, obszarem objętym pojedynczym zobrazowaniem oraz jakością automatycznej detekcji i wsparcia analitycznego.

Krótki deklarowany czas rewizyty nie oznacza automatycznie ani ciągłości obserwacji, ani krótkiego czasu reakcji. Satelita może często przelatywać nad obszarem

zainteresowania, lecz w konkretnym momencie nie być dostępny dla danego zadania, a pozyskane zobrazowanie wymaga dodatkowego czasu na transmisję, przetworzenie i ocenę. Istotny jest zatem charakter dostępu do zdolności: gwarantowane pierwszeństwo dla zadań państwowych, w tym wojskowych, daje inną wartość operacyjną niż dostęp realizowany zależnie od bieżącej dostępności zasobów.

Stawianie zadań wymaga uprzedniego wskazania obszaru zainteresowania. W przypadku MV SUN przesłanką mógłby być przebieg trasy zarejestrowany w AIS – obserwacja satelitarna nie zastępuje więc pozostałych warstw systemu, lecz je uzupełnia i pozwala weryfikować pochodzące z nich informacje. SAR umożliwia obserwację niezależnie od oświetlenia i zasadniczo niezależnie od zachmurzenia, ale nie zapewnia stałego monitoringu akwenu, a jego skuteczność ograniczają intensywne opady oraz wysoki stan morza, utrudniający detekcję małych jednostek. System dostarcza kolejne zobrazowania w określonych momentach, dlatego największą wartość osiąga jako element systemu wielosensorowego, łączącego dane satelitarne z AIS, radarami brzegowymi, monitoringiem operatorskim oraz środkami powietrznymi, nawodnymi i podwodnymi.

Ostateczną miarą skuteczności nie jest zatem sam czas pozyskania zobrazowania. Czas dostarczenia produktu jest parametrem technicznym i kontraktowym, który może zostać określony w umowie i egzekwowany. Czas podjęcia decyzji zależy natomiast od progów, kompetencji i procedur po stronie państwa. Warstwa satelitarna może więc skrócić pierwszą część łańcucha decyzyjnego; jego druga część pozostaje zadaniem instytucjonalnym.



Wielodomenowy obraz Bałtyku – od danych do odporności państwa



**Marcin
Gałuszkiewicz**

**Krzysztof
Grotkowski**

**Monika
Stachoń**

**Kamila
Tamaka**

DOCELOWĄ ZDOLNOŚCIĄ NIE JEST SAMO POZYSKANIE ZOBRAZOWANIA

Jest nią przejście od wielu rozproszonych sensorów do informacji, od informacji do decyzji, a od pojedynczych systemów narodowych do interoperacyjnego środowiska wymiany danych.

Bałtyk staje się laboratorium europejskiej odporności strategicznej, testując nowe modele wspólnego reagowania i koordynacji służb granicznych, wywiadowczych i wojskowych. Współzależność infrastruktury morskiej sprawia, że bezpieczeństwo portów, instalacji offshore, podmorskiej infrastruktury energetycznej i kabli telekomunikacyjnych ma znaczenie dla stabilności gospodarczej, energetycznej i obronnej całego regionu. Odpowiedź na zagrożenia powinna więc zmierzać do budowy wspólnego, wielodomenowego obrazu sytuacji operacyjnej.

WARSTWA SATELITARNA: WIĘCEJ NIŻ JEDNO ŹRÓDŁO

Warstwa satelitarna takiego obrazu może obejmować zobrazowania radarowe SAR i optyczne wysokiej rozdzielczości, dane hiperspektralne i termalne oraz satelitarne systemy automatycznej identyfikacji jednostek pływających (S-AIS). Zestawienie ich z radarami brzegowymi, VTS, AIS, LRIT i platformami bezzałogowymi zwiększa możliwość weryfikacji informacji pochodzących z pojedynczych źródeł. Jednym z zastosowań jest wykrywanie jednostek tzw. floty cieni (dark vessels), które wyłączyły system AIS, oraz identyfikowanie nietypowej aktywności w rejonie infrastruktury krytycznej.

CZAS JAKO PARAMETR ZDOLNOŚCI

W warunkach Bałtyku czas przejścia od zapotrzebowania na obserwację do informacji użytecznej operacyjnie musi być liczony w godzinach, a nie dniach. Rozwijany w ramach Europejskiej Agencji Kosmicznej program ALPSTAR pokazuje model federacyjnego dostępu do zasobów: zamiast oczekiwania na kontakt satelity z pojedynczą narodową stacją naziemną dane mają być kierowane do najbliższej dostępnej stacji sieci. Zakładany czas od zgłoszenia potrzeby do dostępu do danych dla reagowania kryzysowego ma wynosić poniżej godziny, a dla pilnego zwiadu – poniżej 30 minut od wysłania zadanego do odbioru danych.

ALPSTAR ma integrować trzy typy sensorów – SAR, rozpoznanie elektromagnetyczne (ELINT) i sensory optyczne – umożliwiając obserwację tego samego obszaru w bardzo krótkim czasie. System zakłada również dostarczanie nie tylko surowych danych, lecz także gotowych produktów analitycznych, takich jak mapy i alerty, możliwych do włączenia do narodowych systemów zarządzania operacyjnego i dowodzenia. W sytuacji kryzysowej państwo ma ponadto uzyskiwać możliwość priorytetowego wykorzystania sfederowanych zasobów partnerów, w tym źródeł komercyjnych.

OD DANYCH DO ZDOLNOŚCI PAŃSTWA

Polska rozwija równolegle własną warstwę dostępu do informacji i ich przetwarzania. Narodowy System Informacji Satelitarnej (NSIS) ma stanowić główne źródło informacji satelitarnej dla administracji publicznej. Obejmuje repozytorium danych i metadanych, środowisko oblicze-

niowe, portal analityczny i rynek usług, a infrastruktura GPU/HPC pozwala na masowo równoległe przetwarzanie danych i wykorzystanie sztucznej inteligencji.

Kluczowy jest przy tym mechanizm zadaniowania. We współpracy z Agencją Rozpoznania Geoprzestrzennego i Usług Satelitarnych (ARGUS) wypracowywane są rozwiązania proceduralne i techniczne umożliwiające przekazywanie zapotrzebowania i zadaniowanie satelitów na potrzeby administracji publicznej oraz służb zarządzania kryzysowego.

Drugim elementem jest odporność na zakłócenia nawigacji. Pilotażowy Krajowy System Monitorowania Zakłóceń GNSS, rozwijany przez POLSA, zakłada rozmieszczenie około 100 sensorów w obszarze granicy z Federacją Rosyjską na północy kraju i w rejonie Trójmiasta i monitorowanie jammingu oraz spoofingu w czasie rzeczywistym. Koncepcja Polskiej Tarczy zakłada integrację tego rozwiązania z systemami rozwijanymi przez GUGiK i IŁ-PIB oraz MON w wielowarstwowy system monitorowania zakłóceń GNSS.

OŚRODEK MONITOROWANIA MORZA BAŁTYCKIEGO

Instytucjonalnym rozwinięciem tej architektury ma być planowany w Gdańsku Ośrodek Monitorowania Morza Bałtyckiego (OMMB) – krajowy ośrodek kompetencji w zakresie operacyjnego wykorzystania technologii satelitarnych i danych wielosensorycznych. W myśl idei „łączymy, nie dublujemy” ośrodek ma integrować rozproszone dane i kompetencje bez tworzenia kolejnych, nakładających się struktur.

OMMB ma łączyć zobrazowania SAR i optyczne z danymi z platform bezzałogowych, radarów brzegowych, AIS, sensorów in situ i boi hydrometeorologicznych, przełamując silosy informacyjne i tworząc podstawę sfederowanego środowiska wymiany informacji. Ośrodek jest projektowany jako rozwiązanie podwójnego zastosowania: zarówno na potrzeby bezpieczeństwa i obronności, jak i portów, infrastruktury offshore oraz gospodarki morskiej. Co ważne, OMMB ma pełnić funkcję katalizatora wymiany

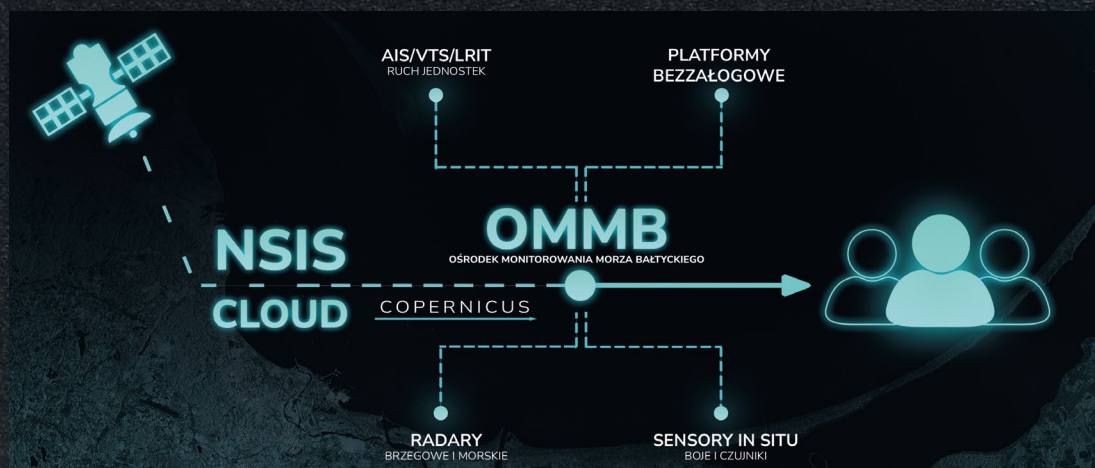
informacji na styku administracji i operatorów infrastruktury krytycznej. Poprzez dostarczanie gotowych produktów analitycznych ośrodek umożliwi operatorom weryfikację normalnych wzorców aktywności wokół ich aktywów (np. farm wiatrowych czy kabli podmorskich) w zestawieniu z szerszym kontekstem bezpieczeństwa kraju. Dzięki temu informacja o anomalii wykrytej przez operatora może być niezwłocznie wzbogacona o dane satelitarne, skracając czas od detekcji do podjęcia decyzji o interwencji.

Uzupełnieniem ma być Cyfrowy Bliźniak Morza Bałtyckiego umożliwiający symulacje i predykcję, m.in. kierunków rozprzestrzeniania się rozlewów olejowych i zanieczyszczeń chemicznych oraz monitoring zakwitów sinic, eutrofizacji i zlodzenia.

Dane satelitarne zachowują wartość również po incydencie – mogą dokumentować jego przebieg na potrzeby postępowań karnych i cywilnych oraz ograniczać dezinformację, dostarczając obiektywny materiał o zdarzeniu. Jednocześnie dane znajdują zastosowanie w szczegółowej analizie przebiegu danego incydentu, umożliwiając identyfikację jego przyczyn, schematu działania oraz potencjalnych słabych punktów. Wnioski z przeprowadzonej analizy mogą wspierać przygotowania do wystąpienia kolejnych, podobnych lub bardziej zaawansowanych incydentów, a tym samym przyczynić się do skuteczniejszego zapobiegania zagrożeniom, ograniczania ich skutków oraz zwiększania poziomu bezpieczeństwa.

OMMB ma być przy tym krajowym elementem szerszej układanki. Integracja zdolności rozpoznawczych państw regionu, oparta na wymianie danych satelitarnych i wieloźródłowej informacji geoprzestrzennej, tworzy podstawę odpornego, interoperacyjnego systemu ochrony infrastruktury krytycznej Bałtyku.

W tej architekturze POLSA pełni funkcję integratora warstwy satelitarnej państwa: łączy źródła danych, infrastrukturę ich przetwarzania, potrzeby administracji publicznej oraz potencjał sektora komercyjnego, tworząc pomost między zdolnościami kosmicznymi i ich wykorzystaniem przez administrację, służby, wojsko oraz gospodarkę.



Zdjęcie Zatoki Gdańskiej (Polska) wykonane 3 grudnia 2025 r. Źródło danych: Copernicus. Satelita Sentinel-1. Kompozycja RGB VH-VV-VV.

6 | Od danych do działania.

Priorytety wdrożeniowe dla Polski

1

Integracja systemowa

Obecny etap tworzenia CBM jest optymalnym momentem na integrację. CBM rozpocznie działalność z początkiem 2027 r., a jego obecna faza organizacyjna obejmuje właśnie zapewnienie funkcjonalności i kompletności systemów teleinformatycznych. Dane i produkty satelitarne, w tym integrowane przez OMMB, powinny zostać od początku wpisane w model wymiany informacji CBM z interfejsami do KSBM/SWIBŻ, ZSRN, systemów wojskowych i systemów służb specjalnych oraz – w odpowiednim zakresie – do systemów operatorów branżowych (sektorów morskiej energetyki wiatrowej oraz ropy i gazu). Jeżeli zostaną dołączone dopiero po uruchomieniu Centrum, państwo ryzykuje utrwalenie kolejnego podziału sektorowego zamiast usunięcia problemu, dla którego CBM powstaje.

2

Model podwójnego zastosowania

Rozwiązania zastosowane na platformie Baltic Beta pokazują, że infrastruktura morska może jednocześnie pełnić funkcję nośnika państwowych zdolności obserwacyjnych – na platformie działa radar KSBM wykorzystywany przez VTS. Rozwój 5,9 GW MEW do 2030 r. należy wykorzystać do przejścia od pojedynczych przypadków do zasady security-by-design: w projektach kwalifikowanych jako potencjalna infrastruktura krytyczna przewidywać już na etapie budowy możliwość instalacji sensorów oraz zapewnienia im zasilania, transmisji danych i bezpiecznej separacji systemów.

3

Suwerenność danych

Polska ma już krajową zdolność SAR: MikroSAR przekazano Siłom Zbrojnym w maju 2026 r., opcję rozszerzającą zamówienie 3+3 uruchomiono, a cztery satelity POLSARIS znalazły się już na orbicie. Kolejnym krokiem powinno być określenie priorytetów stawiania zadań i zasad dystrybucji produktów na potrzeby bezpieczeństwa morskiego, w szczególności SG, CBM, administracji morskiej i ochrony infrastruktury, przy zachowaniu pierwszeństwa potrzeb obronnych. Narodowe zasoby powinny zabezpieczać zadania wymagające suwerenności i gwarantowanego pierwszeństwa, a zdolności EMSA, Copernicus i komercyjne służyć jako warstwa uzupełniająca i skalowalna. Warstwa monitoringowa powinna od początku obejmować automatyczną detekcję, klasyfikację i analizę zmian, tak aby wzrost liczby obrazowań nie przekładał się proporcjonalnie na wzrost obciążenia analityków.

4

Jasny podział odpowiedzialności

Nowelizacja z 2026 r. rozszerzyła uprawnienia Marynarki Wojennej wobec obcych statków, zbliżając je do kompetencji Straży Granicznej. Wymaga to jednoznacznego określenia podmiotu prowadzącego, podmiotu wspierającego, przesłanek przejęcia odpowiedzialności oraz zasad przekazania informacji i materiału dowodowego. Centrum Bezpieczeństwa Morskiego powinno zapewniać spójność tych procedur oraz warunki do ich regularnego ćwiczenia między właściwymi instytucjami. Należy również cyklicznie opracowywać raport o bezpieczeństwie polskich obszarów morskich, by identyfikować zmiany zagrożeń, luki systemowe i postęp w ich ograniczaniu.

5

Pilotaż operacyjny

Należy testować w warunkach operacyjnych pełny łańcuch działania: możliwości sensorów, zdolności do odpowiednio wczesnego wykrycia symptomów zagrożeń przez system, korelację danych, klasyfikację zagrożeń, wskazanie podmiotu właściwego, podjęcie decyzji i skierowanie sił. W ramach pilotażu należy mierzyć czas trwania poszczególnych etapów oraz oceniać sprawność procesu decyzyjnego, tak aby ustalić nie tylko to, czy system działa, lecz także gdzie powstają opóźnienia i dochodzi do utraty informacji.

7

Stały rozwój zdolności

Horyzont wyznacza koniec 2028 r., gdy POLMARFOR ma przejąć rolę regionalnego dowództwa sił morskich NATO na Bałtyku. Do tego czasu Polska musi potrafić nie tylko pozyskiwać dane, lecz także wytwarzać na ich podstawie, weryfikować i udostępniać produkty sytuacyjne użyteczne dla Sojuszu. Archiwum danych powinno od początku służyć dwóm celom: odtwarzaniu scenariuszy opartych na rzeczywistych zdarzeniach na potrzeby szkoleń oraz zachowaniu śladu źródłowego i procesowego zdarzenia. Szkolenie powinno koncentrować się przede wszystkim na decyzjach podejmowanych w warunkach niepełnej informacji, zmianie kwalifikacji zagrożenia i czasie reakcji liczonym w godzinach.

6

Równoległe ścieżki egzekwowania prawa i odpowiedzialności

Jak pokazał przypadek Eagle S, skuteczność ścieżki karnej może zostać ograniczona przez kwestie jurysdykcyjne, dlatego reakcja powinna od początku obejmować równoległe instrumenty karne, administracyjne, portowe, sankcyjne i odszkodowawcze. System obserwacji musi więc wytwarzać nie tylko alert operacyjny, lecz także materiał nadający się do wykorzystania w dalszych postępowaniach.

8

Ciągłość obserwacji

Ograniczona liczba satelitów wojskowych oznacza konieczność priorytetyzacji zadań, przy czym pierwszeństwo powinny zachować potrzeby obronne. Aby zapewnić regularny monitoring Bałtyku i infrastruktury krytycznej, należy równoległe rozbudowywać istniejącą konstelację, rozważyć utworzenie dedykowanej cywilnej zdolności satelitarnej (potencjalnie współfinansowanej przez operatorów infrastruktury lub budowanej w ramach mechanizmów europejskich) albo zapewnić stały dostęp do danych i produktów analitycznych z dostępnych konstelacji komercyjnych. Rozwiązania te mogą być stosowane łącznie, tak aby monitoring infrastruktury nie ograniczał dostępności zasobów wojskowych.

Najważniejsze skróty

AIS	Automatic Identification System – system automatycznej identyfikacji statków
AUV	Autonomous Underwater Vehicle – autonomiczny pojazd podwodny
CBM	Centrum Bezpieczeństwa Morskiego
CCTV	Closed-Circuit Television – telewizja dozorowa
CTF Baltic	Commander Task Force Baltic
DGPS	Differential Global Positioning System – różnicowy system pozycjonowania satelitarnego
EMSA	European Maritime Safety Agency – Europejska Agencja Bezpieczeństwa Morskiego
FSRU	Floating Storage and Regasification Unit – pływająca jednostka magazynowania i regazyfikacji LNG
GNSS	Global Navigation Satellite System – globalny system nawigacji satelitarnej
HELCOM	Komisja Ochrony Środowiska Morskiego Bałtyku
IMO	International Maritime Organization – Międzynarodowa Organizacja Morska; w raporcie także: numer IMO – unikalny numer identyfikacyjny statku
KSBM	Krajowy System Bezpieczeństwa Morskiego
LNG	Liquefied Natural Gas – skroplony gaz ziemny
MARCOM	Allied Maritime Command – Dowództwo Morskie NATO
MCSCUI	NATO Maritime Centre for the Security of Critical Undersea Infrastructure – Centrum NATO ds. Bezpieczeństwa Krytycznej Infrastruktury Podmorskiej
MSA	Maritime Situational Awareness – świadomość sytuacyjna w domenie morskiej
POLSARIS	Polish SAR Intelligence System – wojskowa konstelacja satelitów radarowych
RCB	Rządowe Centrum Bezpieczeństwa
RDF	Radio Direction Finder – radionamiernik
RMP	Recognized Maritime Picture – rozpoznany obraz sytuacji morskiej
ROV	Remotely Operated Vehicle – zdalnie sterowany pojazd podwodny
SAR	Synthetic Aperture Radar – radar z syntetyczną aperturą
SAR	Search and Rescue – poszukiwanie i ratownictwo
SWIBŻ	System Wymiany Informacji Bezpieczeństwa Żeglugi
TDOA	Time Difference of Arrival – metoda lokalizacji emitera na podstawie różnicy czasu dotarcia sygnału
UNCLOS	United Nations Convention on the Law of the Sea – Konwencja Narodów Zjednoczonych o prawie morza
UUV	Unmanned Underwater Vehicle – bezzałogowy pojazd podwodny
VHF	Very High Frequency – pasmo bardzo wysokich częstotliwości
VTS	Vessel Traffic Service – służba kontroli ruchu statków
WSE	wyłączna strefa ekonomiczna
ZSRN	Zautomatyzowany System Radarowego Nadzoru polskich obszarów morskich

B E Z P I E C Z E Ń S T W O

BAŁTYKU

Główne źródła

Raport opracowano na podstawie materiałów i danych publikowanych przez NATO, IMO, HELCOM, Komisję Europejską, EMSA, EDA, EUROCONTROL i program Copernicus, a także przez polskie instytucje państwowe i służby odpowiedzialne za bezpieczeństwo morskie, obronność, zarządzanie kryzysowe i administrację morską, w tym MON, Siły Zbrojne RP, Straż Graniczną, urzędy morskie, GUS, IMGW-PIB i NIK.

Wykorzystano również dane i komunikaty operatorów infrastruktury energetycznej i przesyłowej, w szczególności PSE, GAZ-SYSTEM, PERN, Naftoportu i ORLEN, materiały właściwych instytucji z Finlandii, Szwecji, Danii i Ukrainy oraz recenzowane publikacje naukowe, analizy ośrodków eksperckich i specjalistyczne źródła branżowe dotyczące bezpieczeństwa morskiego (szczególnie Raport wywiadowczy V/2025 pt. „Podejrzana aktywność statku floty cieni MV SUN w okolicach kabla podmorskiego SWEPOL”, 9.07.2025), technologii satelitarnych, infrastruktury krytycznej i bezpieczeństwa energetycznego.

impulse.
INSTITUTE

ICEYE

PARTNERZY:

PGZ



impulse. ICEYE
INSTITUTE

PARTNERZY:

