KLAUDIA SKELNIK, MAJA GŁUCHOWSKA-WÓJCICKA,
DOMINIK BIERECKI

Cyberodporność infrastruktury krytycznej Morza Bałtyckiego – model prawnego i organizacyjnego zarządzania ryzykiem hybrydowym

Cyber Resilience of Baltic Sea Critical Infrastructure: A Model for the Legal and Organisational Management of Hybrid Risk

Abstract

The critical infrastructure of the Baltic Sea is a vital component of the security of the states in the region, and its increasing digitalisation and interconnectedness heighten its vulnerability to hybrid threats. The aim of this article is to develop an original legal and organisational model for managing the cyber resilience of Baltic Sea critical infrastructure under conditions of hybrid threats. The model takes into account requirements arising from European Union law, national law and information security standards. The main research problem concerns whether legal and organisational instruments can be integrated into a coherent risk management system covering cyber, physical and information threats. The study employs the dogmatic legal method, systems analysis, and an analysis of the relevant literature and strategic documents. Particular attention is paid to the provisions of the NIS2 and CER Directives and their significance for shaping the obligations of critical entities with regard to risk and resilience management. The analysis results in an original model that integrates the legal, organisational, informational and operational dimensions of cyber resilience. The approach adopted points to the need to move away from a sectoral view of critical infrastructure protection towards integrated resilience management, encompassing prevention, response, business continuity, recovery and adaptation to an evolving threat environment.

SŁOWA KLUCZOWE: cyberodporność, infrastruktura krytyczna, Morze Bałtyckie, zagrożenia hybrydowe, NIS2, CER, zarządzanie ryzykiem

KEYWORDS: cyber resilience, critical infrastructure, Baltic Sea, hybrid threats, NIS2, CER, risk management

KLAUDIA SKELNIK – doktor nauk prawnych, Uniwersytet WSB Merito w Gdańsku, e-mail: kskelnik@wsb.gda.pl, ORCID – 0000-0003-2771-3900.

MAJA GŁUCHOWSKA-WÓJCICKA – doktor nauk prawnych, Uniwersytet WSB Merito w Gdańsku, e-mail: mgluchowska@wsb.gda.pl, ORCID – 0009-0008-5180-5876.

DOMINIK BIERECKI – doktor habilitowany nauk prawnych, Spółdzielczy Instytut Naukowy w Sopocie, e-mail: dominik.bierecki@sin.edu.pl, ORCID – 0000-0001-6993-3974.

HTTPS://DOI.ORG/10.36128/BSFZ5Y73

1 Wprowadzenie

Region Morza Bałtyckiego stanowi współcześnie jeden z kluczowych obszarów europejskiego systemu bezpieczeństwa, w którym koncentrują się infrastruktura energetyczna, telekomunikacyjna, transportowa i cyfrowa o znaczeniu zarówno krajowym, jak i transgranicznym. Funkcjonowanie państw regionu pozostaje w coraz większym stopniu uzależnione od ciągłości działania infrastruktury obejmującej m.in. porty morskie, terminale paliwowe i gazowe, systemy energetyczne, gazociągi, podmorskie kable elektroenergetyczne i telekomunikacyjne oraz systemy teleinformatyczne wspierające transport i logistykę. Zakłócenie funkcjonowania jednego z tych elementów może powodować konsekwencje wykraczające poza granice pojedynczego państwa i prowadzić do powstawania efektów kaskadowych w innych sektorach gospodarki oraz systemach bezpieczeństwa.

Znaczenie infrastruktury krytycznej Morza Bałtyckiego wzrasta wraz z postępującą cyfryzacją procesów jej zarządzania. Infrastruktura fizyczna jest obecnie ściśle powiązana z systemami teleinformatycznymi, systemami sterowania przemysłowego oraz rozwiązaniami umożliwiającymi zdalne monitorowanie i zarządzanie procesami technologicznymi. Powoduje to stopniowe zacieranie się tradycyjnej granicy pomiędzy bezpieczeństwem fizycznym a cyberbezpieczeństwem. Incydent powstały w cyberprzestrzeni może prowadzić do zakłócenia procesów zachodzących w świecie fizycznym, natomiast fizyczne uszkodzenie infrastruktury może oddziaływać na dostępność usług cyfrowych i komunikacyjnych. W konsekwencji bezpieczeństwo infrastruktury krytycznej powinno być rozpatrywane jako problem systemowy, obejmujący wzajemnie powiązane komponenty fizyczne, cybernetyczne, organizacyjne oraz informacyjne.

Szczególnym wyzwaniem dla państw regionu są w tym kontekście zagrożenia hybrydowe. Ich istotą jest możliwość równoczesnego lub sekwencyjnego wykorzystywania różnych instrumentów oddziaływania, w tym cyberataków, sabotażu, zakłócania systemów komunikacyjnych i nawigacyjnych, presji ekonomicznej oraz operacji informacyjnych i dezinformacyjnych. W przypadku infrastruktury krytycznej Morza Bałtyckiego charakterystyczne jest ponadto występowanie ryzyka dotyczącego infrastruktury podmorskiej, której uszkodzenie lub zakłócenie funkcjonowania może wywoływać skutki w kilku państwach jednocześnie. Powoduje to, że tradycyjne podejście koncentrujące się przede wszystkim

na ochronie poszczególnych obiektów i systemów staje się niewystarczające. Coraz większego znaczenia nabiera odporność, rozumiana jako zdolność do zapobiegania i przygotowania się na wystąpienie zagrożenia, utrzymania podstawowych funkcji w warunkach zakłócenia, skutecznego reagowania, odtworzenia funkcjonowania oraz adaptacji do zmieniającego się środowiska bezpieczeństwa.

Zmianie tej odpowiada ewolucja regulacji prawnych Unii Europejskiej. Szczególne znaczenie mają w tym zakresie dyrektywa NIS2, ustanawiająca wymagania dotyczące zarządzania ryzykiem w cyberbezpieczeństwie, oraz dyrektywa CER, odnosząca się do odporności podmiotów krytycznych. Regulacje te wskazują na potrzebę odejścia od fragmentarycznego postrzegania bezpieczeństwa i uwzględnienia zarówno zagrożeń cybernetycznych, jak i pozacybernetycznych. Wymagają jednocześnie odpowiedniego powiązania z krajowymi regulacjami dotyczącymi cyberbezpieczeństwa, zarządzania kryzysowego i ochrony infrastruktury krytycznej oraz z rozwiązaniami organizacyjnymi stosowanymi przez operatorów infrastruktury.

Luka badawcza wynika z niewystarczającego zintegrowania prawnego i organizacyjnego wymiaru cyberodporności infrastruktury krytycznej w odniesieniu do specyficznych warunków bezpieczeństwa regionu Morza Bałtyckiego. W literaturze oraz regulacjach prawnych zagadnienia cyberbezpieczeństwa, odporności podmiotów krytycznych, ochrony fizycznej, ciągłości działania i zarządzania ryzykiem są często analizowane jako odrębne obszary. Tymczasem współczesne zagrożenia hybrydowe mogą jednocześnie oddziaływać na kilka wymiarów funkcjonowania infrastruktury. Uzasadnia to poszukiwanie modelu umożliwiającego integrację instrumentów prawnych i mechanizmów organizacyjnych w ramach jednego procesu zarządzania cyberodpornością.

Celem artykułu jest wskazanie modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego w warunkach zagrożeń hybrydowych, uwzględniającego współczesne wymagania wynikające z prawa Unii Europejskiej, prawa krajowego oraz standardów bezpieczeństwa informacji.

Realizacji tak określonego celu podporządkowano główny problem badawczy, sformułowany w postaci pytania: Czy obecny system prawny i organizacyjny zapewnia odpowiednią cyberodporność infrastruktury krytycznej Morza Bałtyckiego wobec współczesnych zagrożeń hybrydowych?

Autorzy postawili również pytania szczegółowe:

1) Jak zmienił się charakter zagrożeń bezpieczeństwa morskiego po cyfryzacji infrastruktury?
2) Jakie obowiązki nakładają NIS2, CER oraz polska ustawa o krajowym systemie cyberbezpieczeństwa na operatorów infrastruktury morskiej?
3) Jakie luki występują w obecnym systemie zarządzania ryzykiem?
4) Jakie elementy powinien zawierać model cyberodporności dla regionu Morza Bałtyckiego?

Autorzy przyjmują hipotezę, że współczesne zagrożenia hybrydowe sprawiają, iż klasyczne modele ochrony infrastruktury krytycznej są niewystarczające. Zapewnienie cyberodporności infrastruktury krytycznej Morza Bałtyckiego wymaga zintegrowanego modelu obejmującego jednocześnie aspekty prawne, organizacyjne, technologiczne oraz zarządzanie informacją.

W badaniu zastosowano przede wszystkim metodę dogmatycznoprawną, pozwalającą na analizę obowiązujących regulacji Unii Europejskiej i prawa krajowego, uzupełnioną analizą systemową oraz analizą literatury i dokumentów strategicznych dotyczących cyberbezpieczeństwa, infrastruktury krytycznej i zagrożeń hybrydowych. Na podstawie uzyskanych wyników zastosowano modelowanie konceptualne, którego rezultatem jest propozycja modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego.

Zdaniem autorów skuteczna cyberodporność infrastruktury krytycznej Bałtyku wymaga integracji reżimów cyberbezpieczeństwa i odporności infrastruktury z organizacyjnym zarządzaniem ryzykiem hybrydowym.

2 | Infrastruktura krytyczna Morza Bałtyckiego wobec zagrożeń hybrydowych

Morze Bałtyckie stanowi współcześnie przestrzeń o szczególnym znaczeniu dla bezpieczeństwa państw Europy Północnej i Środkowo-Wschodniej. Jego znaczenie wynika nie tylko z uwarunkowań geopolitycznych i militarnych, lecz również z koncentracji infrastruktury zapewniającej realizację podstawowych funkcji państw regionu. Jak wskazuje Tomasz Szubrycht, problematyka bezpieczeństwa Morza Bałtyckiego powinna być rozpatrywana wielowymiarowo, z uwzględnieniem wzajemnych zależności pomiędzy bezpieczeństwem państwa, bezpieczeństwem morskim oraz możliwością

niezakłóconego wykorzystania akwenów i infrastruktury morskiej[1]. Współczesne znaczenie tego problemu potwierdzają przypadki uszkodzeń kabli podmorskich, które – jak zauważa autor – unaoczniły znaczenie ochrony morskiej infrastruktury krytycznej dla bezpieczeństwa regionu[2].

Specyfika Bałtyku wynika również z jego uwarunkowań geograficznych. Jest to akwen stosunkowo niewielki, półzamknięty, intensywnie wykorzystywany gospodarczo i komunikacyjnie, a jednocześnie otoczony przez państwa posiadające zróżnicowane interesy strategiczne. Andrzej Makowski zwraca uwagę, że fizyczna charakterystyka Bałtyku wpływa na sposób prowadzenia działań w jego obrębie, a sam akwen stanowi zasadniczą przestrzeń realizacji polskich interesów morskich[3]. Oznacza to, że infrastruktury znajdującej się na Bałtyku nie można analizować wyłącznie z perspektywy technicznej. Jest ona elementem szerszego systemu bezpieczeństwa obejmującego wymiar gospodarczy, energetyczny, militarny, polityczny i społeczny.

Zmiana środowiska bezpieczeństwa po agresji Federacji Rosyjskiej na Ukrainę dodatkowo zwiększyła strategiczne znaczenie regionu. W literaturze coraz częściej wskazuje się, że konsekwencją wojny jest m.in. konieczność wzmocnienia ochrony infrastruktury krytycznej oraz dostosowania polityki bezpieczeństwa morskiego NATO do nowych uwarunkowań strategicznych[4]. Bałtyk przestał być zatem postrzegany jedynie jako przestrzeń wymiany gospodarczej i transportowej. Stał się również obszarem konfrontacji interesów strategicznych oraz potencjalnych działań hybrydowych.

Infrastruktura krytyczna regionu Morza Bałtyckiego ma charakter wielosektorowy. Szczególne znaczenie posiada infrastruktura energetyczna, obejmująca gazociągi, podmorskie połączenia elektroenergetyczne, terminale LNG, terminale naftowe, instalacje wydobywcze oraz rozwijające się morskie

1 Zob. Tomasz Szubrycht, *Bałtyckie wymiary bezpieczeństwa* (Gdynia: Wydawnictwo Akademickie AMW, 2010).

2 Tomasz Szubrycht, „Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim" *Bezpieczeństwo Narodowe*, nr 1 (2025): 49–76.

3 Zob. Andrzej Makowski, „Dilemmas Faced in Developing Small Navies" *Naval War College Review*, nr 1 (2023), art. 7; por. także Andrzej Makowski, Tomasz Szubrycht, hasło „Panowanie na morzu", [w:] *Encyklopedia Bezpieczeństwa Narodowego*, red. Jolanta Itrich-Drabarek, Andrzej Misiuk, Szymon Mitkow, Patrycja Bryczek-Wróbel (Warszawa: Dom Wydawniczy Elipsa 2023).

4 Zob. Miłosz Gac, „Wpływ wojny w Ukrainie na politykę bezpieczeństwa morskiego NATO w basenie Morza Bałtyckiego" *De Securitate et Defensione. O Bezpieczeństwie i Obronności*, nr 1 (2025): 7–26.

farmy wiatrowe. Eksperci wskazują, że znaczenie Bałtyku dla bezpieczeństwa energetycznego Polski istotnie wzrosło wraz z rozbudową infrastruktury umożliwiającej dywersyfikację kierunków i źródeł dostaw energii. Do kluczowych elementów tego systemu zaliczają m.in. Baltic Pipe, podmorskie połączenia energetyczne, terminal LNG oraz rozwijającą się energetykę wiatrową[5].

Drugą kategorię tworzy infrastruktura telekomunikacyjna, w szczególności podmorskie światłowody i inne elementy systemów transmisji danych. Ich znaczenie powoduje, że fizyczne uszkodzenie infrastruktury znajdującej się na dnie morskim może prowadzić do konsekwencji typowych dla incydentu cybernetycznego – ograniczenia dostępności danych, usług i systemów informacyjnych. Podział na infrastrukturę „fizyczną" i „cyfrową" staje się w tym kontekście coraz mniej jednoznaczny.

Trzecim obszarem jest infrastruktura transportowa i logistyczna, obejmująca porty morskie, terminale przeładunkowe, szlaki żeglugowe oraz systemy informatyczne i telekomunikacyjne wykorzystywane do obsługi transportu. Port morski nie jest współcześnie jedynie obiektem infrastruktury transportowej. Stanowi złożony system łączący infrastrukturę fizyczną, logistyczną, energetyczną i cyfrową, a jego zakłócenie może wywołać konsekwencje dla wielu sektorów jednocześnie.

Szczególnego znaczenia nabiera infrastruktura podmorska. Jej położenie powoduje trudności w prowadzeniu stałego monitoringu, identyfikacji źródła uszkodzenia oraz jednoznacznym ustaleniu, czy dane zdarzenie było następstwem awarii, działalności przypadkowej czy celowego działania. Szubrycht zwraca uwagę, że przypadki uszkodzenia infrastruktury podmorskiej na Bałtyku oraz aktywność tzw. floty cieni istotnie zmieniły ocenę zagrożeń dla bezpieczeństwa morskiego[6]. Podobnie Miłosz Gac wskazuje na możliwość wykorzystania działań hybrydowych, w tym aktywności

5 Piotr Mickiewicz, „Bałtyk jako obszar występowania najpoważniejszych zagrożeń dla bezpieczeństwa energetycznego Polski" *Teologia Polityczna Co Tydzień*, nr 430 (2024), https://teologiapolityczna.pl/piotr-mickiewicz-baltyk-jako-obszar-wystepowania-najpowazniejszych-zagrozen-dla-bezpieczenstwa-energetycznego-polski-1.

6 Zob. Szubrycht, „Sojusznicza odpowiedź", 49–76.

skierowanej przeciwko infrastrukturze telekomunikacyjnej, energetycznej i gazowej[7].

Jedną z podstawowych cech współczesnej infrastruktury krytycznej jest jej współzależność. System energetyczny wymaga funkcjonowania sieci telekomunikacyjnych i systemów sterowania, infrastruktura portowa zależy od energii elektrycznej i systemów cyfrowych, natomiast transport morski wykorzystuje systemy nawigacji, łączności, pozycjonowania oraz wymiany danych. Zakłócenie pojedynczego komponentu może zatem oddziaływać na pozostałe elementy systemu.

Powoduje to konieczność odejścia od sektorowego modelu postrzegania bezpieczeństwa. W przypadku infrastruktury krytycznej Morza Bałtyckiego zasadne jest przyjęcie perspektywy systemu systemów (*system of systems*), w którym poszczególne elementy zachowują organizacyjną i funkcjonalną autonomię, lecz jednocześnie pozostają od siebie zależne. Bezpieczeństwo jednego sektora może być w konsekwencji determinowane poziomem bezpieczeństwa innych sektorów.

Szczególnego znaczenia nabiera przy tym powiązanie trzech warstw: fizycznej, cyfrowej i informacyjnej. Warstwa fizyczna obejmuje urządzenia, instalacje, kable, gazociągi, porty i pozostałą infrastrukturę materialną. Warstwa cyfrowa obejmuje systemy teleinformatyczne, systemy sterowania i monitorowania oraz sieci komunikacyjne. Warstwa informacyjna związana jest natomiast z pozyskiwaniem, przetwarzaniem i wymianą informacji niezbędnych do podejmowania decyzji dotyczących bezpieczeństwa.

Tak rozumiana współzależność ma istotne znaczenie dla cyberodporności. Cyberatak na system sterowania może doprowadzić do fizycznego zakłócenia funkcjonowania infrastruktury. Sabotaż kabla telekomunikacyjnego może spowodować ograniczenie dostępności usług cyfrowych. Z kolei operacja dezinformacyjna towarzysząca incydentowi może utrudniać ocenę sytuacji i proces decyzyjny. Cyberodporność infrastruktury krytycznej nie powinna być zatem ograniczana do zabezpieczenia systemów informatycznych, lecz rozumiana jako zdolność całego systemu do utrzymania kluczowych funkcji pomimo wystąpienia zakłócenia.

Charakterystyczną cechą infrastruktury Morza Bałtyckiego jest jej transgraniczność. Gazociągi, kable energetyczne i telekomunikacyjne,

7 Zob. Gac, „Wpływ wojny w Ukrainie", 7–26; zob. także Miłosz Gac, „Flota Bałtycka w polityce bezpieczeństwa morskiego Rosji: historia i współczesność" *Rocznik Bezpieczeństwa Międzynarodowego*, nr 2 (2024): 37–62.

szlaki żeglugowe oraz systemy transportowe łączą terytoria i gospodarki wielu państw. W konsekwencji źródło zagrożenia, miejsce wystąpienia incydentu oraz obszar jego skutków nie muszą znajdować się w granicach tego samego państwa.

Już w analizach dotyczących strategii morskich państw bałtyckich wskazywano, że bezpieczeństwo Bałtyku jest rezultatem wzajemnego oddziaływania interesów politycznych, gospodarczych i strategicznych państw regionu[8]. Obecnie zależność ta jest dodatkowo wzmacniana przez rozwój infrastruktury transgranicznej. Ochrona pojedynczego elementu infrastruktury może wymagać współdziałania operatorów, administracji publicznej, służb odpowiedzialnych za cyberbezpieczeństwo, administracji morskiej oraz struktur bezpieczeństwa kilku państw.

Transgraniczny charakter ryzyka rodzi jednocześnie problemy prawne i organizacyjne. Dotyczą one m.in. właściwości organów, wymiany informacji o zagrożeniach i incydentach, koordynacji reagowania oraz odpowiedzialności za zapewnienie ciągłości funkcjonowania usług krytycznych. W środowisku zagrożeń hybrydowych dodatkowym problemem staje się trudność przypisania odpowiedzialności za zdarzenie konkretnemu podmiotowi oraz rozróżnienia pomiędzy awarią, zdarzeniem przypadkowym, przestępstwem a celowym działaniem państwowym lub inspirowanym przez państwo.

Z powyższych względów infrastrukturę krytyczną Morza Bałtyckiego należy traktować jako transgraniczny, wielosektorowy i współzależny system bezpieczeństwa, w którym odporność nie jest prostą sumą zabezpieczeń poszczególnych elementów. Jest ona rezultatem zdolności do identyfikowania zależności, wymiany informacji, wspólnej oceny ryzyka, reagowania na incydenty oraz utrzymania i odtworzenia funkcji krytycznych. Takie ujęcie stanowi punkt wyjścia do dalszej analizy prawnych mechanizmów cyberodporności oraz konstrukcji modelu prawnego i organizacyjnego zarządzania ryzykiem hybrydowym infrastruktury krytycznej Morza Bałtyckiego.

Punktem wyjścia dla analiz cyberodporności jest dorobek dotyczący bezpieczeństwa morskiego. W klasycznych ujęciach obejmuje ono bezpieczeństwo żeglugi, ochronę portów, przeciwdziałanie przestępczości morskiej, ochronę granic i środowiska oraz zabezpieczenie gospodarczych

8 Zob. Piotr Mickiewicz, „Morze Bałtyckie w założeniach strategii morskich i polityk bezpieczeństwa narodowego państw bałtyckich. Wnioski dla koncepcji bezpieczeństwa morskiego RP" *Studia Bezpieczeństwa Narodowego*, nr 1 (2014): 339–365.

interesów państwa. Rozwój infrastruktury energetycznej, cyfrowej i telekomunikacyjnej spowodował jednak, że przedmiotem ochrony stały się także gazociągi, kable elektroenergetyczne i światłowodowe, morskie farmy wiatrowe, terminale LNG oraz cyfrowe systemy zarządzania ruchem i logistyką.

W literaturze przedmiotu słusznie wskazuje się, że morska infrastruktura krytyczna różni się od infrastruktury lądowej zarówno ze względu na warunki jej lokalizacji, jak i transgraniczny charakter oraz trudności związane z obserwacją, przypisywaniem odpowiedzialności i szybkim usuwaniem skutków uszkodzeń. Christian Bueger i Tobias Liebetrau podkreślają, że uznanie określonego obiektu za infrastrukturę krytyczną nie jest wyłącznie decyzją techniczną, lecz także polityczną, wynikającą z oceny jego znaczenia dla społeczeństwa, gospodarki i bezpieczeństwa państwa[9]. W ich ujęciu ochrona infrastruktury morskiej wymaga integracji polityki obronnej, dyplomacji, bezpieczeństwa morskiego, cyberbezpieczeństwa oraz współpracy z prywatnymi operatorami.

Podobne stanowisko prezentują Liebetrau i Bueger w analizie instytucjonalnych uwarunkowań ochrony krytycznej infrastruktury morskiej. Zdaniem autorów głównym problemem nie jest wyłącznie brak zdolności technicznych, lecz trudność w koordynowaniu działań licznych podmiotów publicznych i prywatnych. Ochrona infrastruktury wymaga dialogu, wymiany informacji i uzgodnionych procedur, przy czym wciąż nie jest jasne, jakie rozwiązania instytucjonalne najlepiej odpowiadają specyfice środowiska morskiego[10]. Wnioski te mają podstawowe znaczenie dla modelu BCI-CRGM, ponieważ potwierdzają konieczność wyodrębnienia współpracy międzyinstytucjonalnej jako jednego z filarów cyberodporności.

W literaturze coraz częściej wskazuje się również, że ochrona infrastruktury znajdującej się na dnie morza powinna uwzględniać nie tylko skutki celowych działań, lecz także awarie, oddziaływanie kotwic, działalność rybacką, niewłaściwe manewry jednostek oraz trudności w zabezpieczeniu rozległych obszarów morskich. Badania nad kablami i rurociągami offshore pokazują, że poziom wymaganej ochrony powinien pozostawać proporcjonalny do

9 Christian Bueger, Tobias Liebetrau, „Critical Maritime Infrastructure Protection: What's the Trouble?" *Marine Policy* 155 (2023), art. 105772.

10 Zob. Tobias Liebetrau, Christian Bueger, „Advancing Coordination in Critical Maritime Infrastructure Protection: Lessons from Maritime Piracy and Cybersecurity" *International Journal of Critical Infrastructure Protection*, 46 (2024), art. 100683.

znaczenia danego elementu infrastruktury i potencjalnych skutków jego niedostępności[11].

Drugi nurt badań dotyczy hybrydowego charakteru zagrożeń. Współczesne działania wymierzone w infrastrukturę krytyczną mogą obejmować jednocześnie sabotaż, cyberataki, manipulację systemami nawigacyjnymi, operacje informacyjne, presję ekonomiczną oraz wykorzystywanie podmiotów formalnie cywilnych. Ich cechą jest funkcjonowanie poniżej progu otwartego konfliktu zbrojnego i utrudnione przypisanie odpowiedzialności określonemu państwu lub organizacji.

Bueger i Liebetrau zaliczają do podstawowych zagrożeń dla infrastruktury morskiej wypadki, działania przestępcze, terroryzm, sabotaż oraz aktywność w szarej strefie. Podkreślają przy tym, że złożoność zagrożeń uniemożliwia oparcie systemu ochrony wyłącznie na klasycznych środkach obronnych. Literatura dotycząca państw bałtyckich dodatkowo wskazuje, że działania hybrydowe mogą łączyć cyberataki, presję polityczną, dezinformację, operacje psychologiczne i zakłócanie funkcjonowania infrastruktury. Problemem jest nie tylko samo wykrycie oddziaływania, lecz również ustalenie, czy określony incydent był wynikiem przypadku, działania przestępczego czy operacji inspirowanej przez państwo[12].

W odniesieniu do regionu Morza Bałtyckiego istotne znaczenie mają zdarzenia dotyczące gazociągów, kabli energetycznych oraz połączeń telekomunikacyjnych. W literaturze incydenty te traktowane są nie tylko jako zagadnienie techniczne, lecz także jako impuls do przebudowy europejskiej polityki ochrony infrastruktury. Przykładami są uszkodzenia infrastruktury Nord Stream w 2022 r., gazociągu Balticconnector w 2023 r. oraz kolejnych kabli energetycznych i komunikacyjnych. Badania dotyczące monitorowania jednostek pływających wskazują na możliwość wykorzystywania luk

11 Zob. Ove Tobias Gudmestad, Thomas Lundberg, „Security and Safe Operations of Offshore Cables and Pipelines" *Ocean Engineering*, 360 (2026), art. 125958.

12 Zob. Gintaras Labutis, „Strengthening the Critical Infrastructures in Lithuania: From Protection Towards Resilience", [w:] *Democratic Resilience in the Baltics*, vol. I, *Resilient Governance and Democratic Stability*, ed. David Schultz, Rasa Smaliukienė, Vidmantė Giedraitytė (Cham: Springer, 2026), 239–257; Darius Štitilis, Marius Laurinaitis, Matt Warren, „Hybrid Cyber Threats: Lithuanian Context" *Journal of Information Warfare*, nr 1 (2024).

w systemie AIS, fałszowania informacji o położeniu lub prowadzenia nietypowych manewrów w pobliżu infrastruktury podmorskiej[13].

Nurt badań nad zagrożeniami hybrydowymi jest jednak w znacznej części skoncentrowany na identyfikacji metod działania potencjalnego przeciwnika. Rzadziej podejmowany jest problem przekładania tej wiedzy na konkretne obowiązki prawne, systemy odpowiedzialności oraz organizacyjne procedury współpracy. Powstaje zatem luka między analizą środowiska zagrożeń a prawnym i instytucjonalnym modelem zarządzania odpornością.

Trzeci obszar literatury dotyczy skutków cyfrowej transformacji sektora morskiego. Porty i infrastruktura offshore wykorzystują obecnie systemy IT, technologie operacyjne, automatykę przemysłową, chmurę obliczeniową, urządzenia Internetu rzeczy, analitykę danych oraz sztuczną inteligencję. Cyfryzacja poprawia efektywność, bezpieczeństwo nawigacji i zdolności logistyczne, ale jednocześnie zwiększa powierzchnię ataku i liczbę zależności między systemami.

ENISA wskazuje, że porty tworzą rozbudowane ekosystemy, w których funkcjonują organy portowe, operatorzy terminali, przedsiębiorstwa żeglugowe, dostawcy usług logistycznych i podmioty publiczne. Zagrożenia dla jednego uczestnika mogą zatem prowadzić do zakłóceń w całym łańcuchu[14]. W raporcie dotyczącym dobrych praktyk dla portów Agencja zwraca uwagę na potrzebę identyfikowania scenariuszy cyberataków, zarządzania podatnościami, ochrony systemów operacyjnych i budowania świadomości personelu.

Badania dotyczące cyberodporności sektora morskiego wskazują natomiast, że jednym z istotnych problemów pozostaje niewystarczający poziom świadomości zagrożeń. Wdrożenie technologii cyfrowych często wyprzedza rozwój kompetencji organizacyjnych, procedur bezpieczeństwa oraz kultury zarządzania ryzykiem[15]. W odniesieniu do inteligentnych portów literatura identyfikuje dodatkowo fragmentację systemów zarządzania, zależności

13 Zob. Mirosław Wielgosz, Marzena Małyszko, „A Method for Early Identification of Vessels Potentially Threatening Critical Maritime Infrastructure" *Applied Sciences*, nr 15 (2025), art. 8716.

14 European Union Agency for Cybersecurity (ENISA), *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector* (Athens: ENISA, 2019).

15 Jasmin Ćelić, Marko Vukšić, Robert Baždarić, Aleksandar Cuculić, „The Challenges of Cyber Resilience in the Maritime Sector: Addressing the Weak Awareness of the Dangers Caused by Cyber Threats" *Journal of Marine Science and Engineering*, nr 4 (2025), art. 762.

cyberfizyczne, zagrożenia dla łańcucha dostaw, czynniki ludzkie i rosnące znaczenie ataków wspieranych przez sztuczną inteligencję[16].

Szczególne miejsce zajmują badania nad bezpieczeństwem systemów nawigacyjnych. Manipulowanie sygnałem GNSS, GPS spoofing, zakłócanie sensorów czy ingerowanie w logikę systemów sterowania może wpływać nie tylko na bezpieczeństwo jednostki, lecz także na stan infrastruktury znajdującej się w pobliżu tras żeglugowych. Proponowane rozwiązania obejmują między innymi wielowarstwową walidację danych pochodzących z GPS, systemów inercyjnych, sonaru i pozostałych sensorów[17].

Istotnym wkładem koncepcyjnym jest także rozwój pojęcia „cyberzdolności żeglugowej" lub cyber-seaworthiness. Autorzy analizujący ten problem wskazują, że tradycyjne rozumienie zdolności statku do bezpiecznej żeglugi nie odpowiada realiom wysokiego poziomu automatyzacji. Współczesna ocena zdolności żeglugowej powinna zatem obejmować również odporność systemów informatycznych i operacyjnych na cyberzagrożenia[18].

3 | Prawne podstawy cyberodporności infrastruktury krytycznej

Podstawowe znaczenie w prawie Unii Europejskiej mają obecnie dyrektywa NIS2[19] oraz dyrektywa CER[20]. NIS2 ustanawia środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, obejmując zakresem między innymi transport morski, porty, energię i infrastrukturę cyfrową.

16 Yunfeng Zhao, Jincheng Gong, Huanhuan Li, Trung Thanh Nguyen, Christian Matthews, Zaili Yang, „Cybersecurity in Smart Port Systems: A Systematic Review and Data-Driven Research Agenda" *Transport Policy*, 187 (2026), art. 104268.

17 Danish Vasan, Mohammad Hammoudeh, Adel F. Ahmed, Hamad Naeem, „Cyber-attacks: Securing Ship Navigation Systems Using Multi-Layer Cross-Validation Defense" *Computers & Security*, 160 (2026), art. 104706.

18 Orestis Schinas, Daniel Metzger, „Cyber-seaworthiness: A Critical Review of the Literature" *Marine Policy*, 151 (2023), art. 105592.

19 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, 80; dalej: dyrektywa NIS2).

20 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, 164; dalej: dyrektywa CER).

Dyrektywa CER koncentruje się natomiast na odporności podmiotów krytycznych i ciągłości usług niezbędnych dla utrzymania podstawowych funkcji społecznych i działalności gospodarczej.

Komplementarność obu regulacji odzwierciedla zmianę europejskiego podejścia: od oddzielnego traktowania ochrony fizycznej i cyberbezpieczeństwa do modelu uwzględniającego wielowymiarowość ryzyka. W praktyce wciąż jednak powstają problemy związane z transpozycją, rozdziałem kompetencji i dostosowaniem krajowych systemów prawnych. Badanie implementacji europejskich regulacji w państwach regionu Morza Bałtyckiego wskazuje na opóźnienia, różnice w sposobie wdrażania i ograniczony poziom harmonizacji[21].

W odniesieniu do bezpieczeństwa morskiego istotne pozostają również regulacje Międzynarodowej Organizacji Morskiej, w tym kodeks ISPS oraz wytyczne dotyczące zarządzania ryzykiem cybernetycznym. Kodeks ISPS ustanawia obowiązki rządów, administracji portowych, armatorów i obiektów portowych w zakresie ochrony, natomiast wytyczne cyberbezpieczeństwa rozwijają podejście oparte na ryzyku.

Literatura prawnicza analizuje zazwyczaj zakres obowiązków podmiotów objętych regulacjami, środki zarządzania ryzykiem, raportowanie incydentów i kompetencje organów nadzorczych. Rzadziej jednak podejmowana jest próba powiązania tych wymagań z wielopoziomową strukturą zarządzania obejmującą poziom strategiczny, operacyjny, techniczny i decyzyjny[22].

Dorobek dotyczący cyberbezpieczeństwa infrastruktury krytycznej rozwija się wokół problematyki bezpieczeństwa systemów informacyjnych, systemów przemysłowych, technologii operacyjnych oraz reagowania na incydenty. Szczególne znaczenie ma integracja systemów IT i OT. Technologie operacyjne wykorzystywane w portach, terminalach, gazociągach, elektrowniach offshore i systemach przesyłowych były pierwotnie projektowane przede wszystkim z myślą o niezawodności i dostępności. Ich połączenie z sieciami teleinformatycznymi, systemami chmurowymi oraz usługami dostawców

21 Manuel Becker, „Transposing EU-Legislation on Critical Infrastructure Protection: Legal Implementation Performance in the Baltic Sea Region" *International Journal of Critical Infrastructure Protection*, 50 (2025), art. 100781.

22 International Maritime Organization, *International Ship and Port Facility Security Code (ISPS Code)*; International Maritime Organization, *Guidelines on Maritime Cyber Risk Management*, MSC-FAL.1/Circ.3.

zewnętrznych zwiększyło powierzchnię ataku i stworzyło nowe zależności cyberfizyczne.

Badania nad przemysłowymi systemami cyberfizycznymi pokazują, że wzrost wzajemnych połączeń między urządzeniami, sensorami i systemami sterowania ograniczył możliwość opierania ochrony na izolacji sieciowej. Współczesne podatności wynikają między innymi z niewłaściwej ochrony granic systemów, przestarzałych komponentów, problemów z aktualizacją oraz zależności od dostawców. To wszystko determinuje możliwość utrzymania ciągłości działania.

W odniesieniu do sektora morskiego istotne są badania Moniny Schwarz, Matthiasa Marxa i Hannesa Federratha. Autorzy przeanalizowali publicznie ujawnione incydenty bezpieczeństwa informacji w sektorze morskim, wskazując, że rzeczywista skala zjawiska może być większa ze względu na niezgłaszanie lub niewykrywanie części zdarzeń. Wyniki ich badań podkreślają znaczenie wymiany informacji o zagrożeniach jako narzędzia wspierającego zapobieganie kolejnym atakom[23].

Na gruncie polskim podstawę instytucjonalną cyberbezpieczeństwa sektora transportu tworzy krajowy system cyberbezpieczeństwa. Obejmuje on między innymi operatorów usług kluczowych, organy właściwe do spraw cyberbezpieczeństwa oraz zespoły CSIRT. Celem systemu jest zapewnienie niezakłóconego świadczenia usług kluczowych przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych oraz zapewnienie obsługi incydentów.

Pojęcie odporności poszerza tradycyjne rozumienie ochrony. System odporny nie musi całkowicie eliminować incydentów, lecz powinien zachować zdolność do[24]:

- przygotowania się na zagrożenie;
- absorpcji skutków incydentu;
- utrzymania najważniejszych funkcji;
- reagowania w warunkach presji;
- szybkiego odtworzenia działalności;
- uczenia się na podstawie doświadczeń;
- adaptacji do zmienionego środowiska.

23 Monina Schwarz, Matthias Marx, Hannes Federrath, „A Structured Analysis of Information Security Incidents in the Maritime Sector", arXiv:2112.06545 (2021).

24 Grzegorz Masik, „Koncepcja odporności: definicje, interpretacje, podejścia badawcze oraz szkoły myśli" *Przegląd Geograficzny*, nr 3 (2022): 279–305.

W literaturze dotyczącej modelowania infrastruktury krytycznej podkreśla się, że nie istnieje jedno uniwersalne podejście pozwalające odwzorować wszystkie cechy, zależności i zachowania złożonych systemów infrastrukturalnych. Wybór metody wymaga uwzględnienia kompromisu pomiędzy szczegółowością analizy, złożonością modelu i możliwością jego praktycznego zastosowania[25].

Dla infrastruktury Morza Bałtyckiego szczególnie istotne są zależności międzysektorowe. Funkcjonowanie portu zależy od energii, łączności, systemów informacyjnych, transportu kolejowego i drogowego, dostaw paliw oraz usług publicznych. Uszkodzenie jednego elementu może więc powodować skutki kaskadowe w innych systemach. Model w zakresie zapewnienia bezpieczeństwa i utrzymania ciągłości działania powinien z tego względu obejmować nie tylko ocenę ryzyka odnoszącą się do pojedynczego operatora, ale również analizę wzajemnych zależności i możliwego rozprzestrzeniania się skutków incydentu.

Współczesny rozwój badań nad infrastrukturą Morza Bałtyckiego wiąże się przede wszystkim ze wzrostem znaczenia podmorskich kabli energetycznych i telekomunikacyjnych, gazociągów oraz infrastruktury offshore. Obiekty te pozostają trudne do obserwowania, są rozproszone na dużych obszarach i niejednokrotnie łączą terytoria kilku państw. Ich uszkodzenie może prowadzić do konsekwencji wykraczających poza sektor, w którym formalnie funkcjonują. Zagrożenia obejmują między innymi[26]:

- celowy sabotaż;
- przypadkowe uszkodzenie kotwicą lub narzędziami połowowymi;
- cyberatak na systemy sterowania i monitorowania;
- ingerencję w dane dotyczące położenia jednostek;
- zakłócanie sygnałów nawigacyjnych;
- wykorzystanie autonomicznych lub zdalnie sterowanych platform;
- działania prowadzone poniżej progu konfliktu zbrojnego.

Polskie instytucje publiczne podkreślają, że uszkodzenie podwodnej infrastruktury krytycznej może negatywnie wpływać na funkcjonowanie całych państw, społeczeństw i gospodarek. Ochrona powinna zatem

25 Uchenna Daniel Ani, Jeremy McKendrick Watson, Madeline Carr, Al Cook, Jason R.C. Nurse, „A Review of the Use and Utility of Industrial Network-Based Open Source Simulators: Functionality, Security, and Policy Viewpoints" *The Journal of Defense Modeling and Simulation*, nr 3 (2022): 263–286.

26 Zob. Mickiewicz, „Morze Bałtyckie w założeniach strategii morskich", 339–365.

obejmować zarówno zagrożenia fizyczne, jak i cybernetyczne. W analizach wskazuje się również na potencjalne zastosowanie sztucznej inteligencji do obserwacji, wykrywania anomalii i wspierania identyfikowania zagrożeń.

16 czerwca 2025 r. Polska, Estonia, Litwa i Łotwa podpisały w Luksemburgu memorandum dotyczące ochrony i odporności infrastruktury energetycznej, ze szczególnym uwzględnieniem infrastruktury podmorskiej. Przyjęte kierunki działań obejmują zapobieganie, wykrywanie zagrożeń, reagowanie, odstraszanie, szybką wymianę informacji oraz wspólne ćwiczenia. Rozwiązania te potwierdzają zasadność wyodrębnienia filarów świadomości sytuacyjnej, współpracy międzyinstytucjonalnej i ciągłego doskonalenia.

Literatura dotycząca zagrożeń hybrydowych podkreśla ich złożony, wielonarzędziowy i niejednoznaczny charakter. W działaniach wymierzonych w infrastrukturę krytyczną mogą jednocześnie występować cyberataki, fizyczne uszkodzenia, operacje informacyjne, presja ekonomiczna, działania wywiadowcze oraz zakłócanie systemów nawigacyjnych[27].

Szczególnym problemem jest utrudniona atrybucja zdarzenia. W pierwszej fazie incydentu organy państwa i operatorzy mogą nie być w stanie ustalić, czy uszkodzenie było wynikiem awarii, błędu człowieka, działania przestępczego, sabotażu czy operacji prowadzonej przez inne państwo. Niepewność ta wpływa na wybór podstawy prawnej reakcji, uruchomienie kompetencji właściwych instytucji oraz sposób komunikowania zdarzenia społeczeństwu.

Istotnym elementem działań hybrydowych może być manipulacja informacją. Fałszywe dane o położeniu statków, zmanipulowane komunikaty techniczne, nieprawdziwe informacje o przyczynach awarii czy skoordynowane działania dezinformacyjne mogą utrudniać ocenę sytuacji i opóźniać reakcję. W tym kontekście odporność informacyjna oznacza nie tylko ochronę integralności danych, lecz również zdolność do oceny ich wiarygodności i utrzymania jakości decyzji.

Polska prezydencja w Radzie Państw Morza Bałtyckiego na lata 2025–2026 wskazała ochronę infrastruktury krytycznej, przeciwdziałanie flocie cieni oraz odporność na zakłócanie sygnału GPS jako istotne obszary współpracy regionalnej.

Podstawowy europejski model cyberodporności infrastruktury krytycznej opiera się na komplementarnym stosowaniu dyrektywy NIS2 i dyrektywy

27 Zob. Jarosław Keplin, „Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej" *De Securitate et Defensione. O Bezpieczeństwie i Obronności*, nr 2 (2022): 54–68.

CER. NIS2 koncentruje się na zarządzaniu ryzykiem cyberbezpieczeństwa, odpowiedzialności organów zarządzających, bezpieczeństwie łańcucha dostaw, obsłudze incydentów, ciągłości działania oraz raportowaniu[28]. CER obejmuje natomiast odporność podmiotów krytycznych wobec zagrożeń fizycznych, naturalnych, terrorystycznych, sabotażowych i innych zdarzeń wpływających na ciągłość usług kluczowych. Obie dyrektywy odzwierciedlają przejście od podejścia sektorowego do modelu uwzględniającego wszystkie rodzaje ryzyka. Nie eliminują jednak problemów wynikających z[29]:

- podziału kompetencji między liczne organy;
- odmiennej transpozycji przepisów w państwach członkowskich;
- transgranicznego charakteru infrastruktury;
- różnic między systemami krajowymi;
- relacji między ochroną fizyczną i cyberbezpieczeństwem;
- ograniczeń w wymianie informacji wrażliwych;
- rozbieżnych obowiązków sektorowych.

W Polsce dodatkowe znaczenie mają ustawa o zarządzaniu kryzysowym[30] oraz ustawa o krajowym systemie cyberbezpieczeństwa[31]. System znajduje się jednak w okresie zmian związanych z wdrażaniem nowych regulacji unijnych. W 2026 r. procedowane były projekty określające minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa[32], ochrony prawnej i ciągłości działania infrastruktury krytycznej oraz nowe kryteria identyfikacji infrastruktury krytycznej.

Przegląd polskiej i zagranicznej literatury prowadzi do wniosku, że istniejący dorobek dostarcza rozbudowanej wiedzy dotyczącej poszczególnych komponentów bezpieczeństwa, jednak nie tworzy jednolitego modelu cyberodporności infrastruktury krytycznej Morza Bałtyckiego. Zidentyfikowano następujące luki:

1. luka integracyjna – brak połączenia perspektywy prawnej, organizacyjnej, technicznej i informacyjnej;

28 Zob. art. 20, 21 i 23 dyrektywy NIS2.

29 Por. dyrektywa CER.

30 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2026 r., poz. 574).

31 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2026 r., poz. 20 ze zm.).

32 Zob. https://cyber.gov.pl/faq.

2. luka regionalna – niedostatek modeli uwzględniających specyfikę Morza Bałtyckiego;
3. luka instytucjonalna – brak precyzyjnego ujęcia odpowiedzialności i przepływu informacji pomiędzy poziomem strategicznym, operacyjnym, technicznym i decyzyjnym;
4. luka informacyjna – ograniczone uwzględnienie wiarygodności informacji, dezinformacji i jakości decyzji;
5. luka cyberfizyczna – niedostateczna integracja ochrony fizycznej infrastruktury z bezpieczeństwem IT, OT i ICS/SCADA;
6. luka wdrożeniowa – brak narzędzia umożliwiającego wspólne stosowanie NIS2, CER, prawa krajowego i standardów zarządzania ryzykiem;
7. luka walidacyjna – niedostatek empirycznych metod pomiaru cyberodporności morskiej infrastruktury krytycznej.

Autorzy artykułu proponują model, który mógłby stanowić odpowiedź na wskazane ograniczenia. Jego zadaniem jest uporządkowanie relacji między regulacjami prawnymi, aktorami systemu bezpieczeństwa, procesami zarządzania ryzykiem, technologiami oraz informacjami wykorzystywanymi przy podejmowaniu decyzji.

Dynamiczny rozwój technologii cyfrowych oraz zmieniający się charakter zagrożeń bezpieczeństwa spowodowały odejście od klasycznego modelu ochrony infrastruktury krytycznej opartego wyłącznie na zabezpieczeniach fizycznych. Współczesne podejście koncentruje się na budowaniu odporności, rozumianej jako zdolność systemu do zapobiegania zagrożeniom, utrzymania ciągłości działania, skutecznego reagowania na incydenty oraz szybkiego odtworzenia zdolności operacyjnych.

W literaturze przedmiotu cyberodporność coraz częściej przedstawiana jest jako element szerszej odporności państwa, obejmującej nie tylko aspekty techniczne, lecz również organizacyjne, prawne, społeczne i ekonomiczne. W odniesieniu do infrastruktury krytycznej Morza Bałtyckiego oznacza to konieczność tworzenia zintegrowanych mechanizmów ochrony uwzględniających współdziałanie administracji publicznej, operatorów infrastruktury, podmiotów odpowiedzialnych za cyberbezpieczeństwo oraz organizacji międzynarodowych.

Tak rozumiana cyberodporność wykracza poza klasyczne zarządzanie bezpieczeństwem informacji. Obejmuje bowiem nie tylko ochronę poufności, integralności i dostępności danych, ale również zapewnienie odporności

procesów decyzyjnych, ciągłości świadczenia usług kluczowych oraz zdolności do funkcjonowania w warunkach długotrwałych działań hybrydowych.

Unia Europejska w ostatnich latach dokonała zasadniczej przebudowy systemu ochrony infrastruktury krytycznej. Dotychczasowy model, koncentrujący się głównie na ochronie fizycznej obiektów infrastrukturalnych, został zastąpiony podejściem uwzględniającym wzajemne zależności pomiędzy bezpieczeństwem fizycznym, cyberbezpieczeństwem oraz odpornością organizacyjną. Jak już wspomniano, podstawowe znaczenie mają obecnie dwie komplementarne regulacje: dyrektywa (UE) 2022/2555 (NIS2) i dyrektywa (UE) 2022/2557 (CER). Ich wspólnym celem jest zwiększenie odporności podmiotów kluczowych wobec zagrożeń zarówno fizycznych, jak i cyfrowych. Rozwiązanie to odzwierciedla zmianę filozofii ochrony infrastruktury krytycznej – z modelu reaktywnego na model oparty na zarządzaniu ryzykiem oraz budowaniu odporności organizacyjnej.

W przypadku infrastruktury Morza Bałtyckiego szczególne znaczenie ma fakt, że znaczna część obiektów infrastrukturalnych ma charakter transgraniczny. Dotyczy to przede wszystkim sieci energetycznych, podmorskich kabli telekomunikacyjnych oraz gazociągów, których funkcjonowanie wpływa jednocześnie na bezpieczeństwo kilku państw członkowskich.

Dyrektywa NIS2[33] wprowadza jakościowo nowe podejście do cyberbezpieczeństwa, odchodząc od modelu opartego wyłącznie na ochronie systemów teleinformatycznych. Centralnym elementem regulacji staje się obowiązek zarządzania ryzykiem cyberbezpieczeństwa obejmujący cały proces funkcjonowania organizacji.

Na operatorów infrastruktury krytycznej nałożono obowiązek wdrożenia odpowiednich środków technicznych, organizacyjnych i proceduralnych uwzględniających między innymi:

- analizę ryzyka,
- bezpieczeństwo łańcucha dostaw,
- zarządzanie incydentami,
- ciągłość działania,
- zarządzanie podatnościami,
- bezpieczeństwo systemów teleinformatycznych,
- szkolenie personelu,

33 Zob. przypis 19.

- nadzór kierownictwa nad cyberbezpieczeństwem.

Istotną nowością jest rozszerzenie odpowiedzialności najwyższego kierownictwa organizacji. Cyberbezpieczeństwo przestaje być wyłącznie zagadnieniem technicznym, stając się elementem corporate governance oraz odpowiedzialności zarządczej.

Komplementarnym elementem europejskiego systemu ochrony jest dyrektywa CER[34], która koncentruje się na odporności podmiotów krytycznych wobec wszelkiego rodzaju zagrożeń, niezależnie od ich źródła. Podejście to zakłada odejście od ochrony pojedynczych obiektów na rzecz zapewnienia ciągłości realizacji usług kluczowych. Tym samym przedmiotem ochrony staje się nie tylko infrastruktura jako taka, ale przede wszystkim zdolność państwa do niezakłóconego wykonywania funkcji publicznych. W odniesieniu do Morza Bałtyckiego rozwiązanie to posiada szczególne znaczenie z uwagi na wzajemne powiązanie infrastruktury energetycznej, telekomunikacyjnej, transportowej oraz cyfrowej.

Na gruncie prawa krajowego system ochrony infrastruktury krytycznej opiera się przede wszystkim na:

- ustawie o zarządzaniu kryzysowym,
- ustawie o krajowym systemie cyberbezpieczeństwa,
- przepisach dotyczących ochrony informacji niejawnych,
- regulacjach sektorowych odnoszących się do gospodarki morskiej,
- przepisach implementujących prawo Unii Europejskiej.

Analiza obowiązujących regulacji prowadzi jednak do wniosku, że rozwiązania prawne pozostają rozproszone pomiędzy liczne akty normatywne oraz organy administracji publicznej. Powoduje to trudności w budowaniu jednolitego modelu zarządzania cyberodpornością infrastruktury krytycznej.

Szczególnie widoczne jest rozdzielenie kompetencji dotyczących bezpieczeństwa fizycznego, cyberbezpieczeństwa, zarządzania kryzysowego oraz bezpieczeństwa morskiego, co utrudnia skuteczne przeciwdziałanie zagrożeniom hybrydowym.

Pomimo znaczącego rozwoju prawa Unii Europejskiej oraz prawa krajowego nadal można wskazać kilka podstawowych problemów systemowych. Po pierwsze, obowiązujące regulacje koncentrują się przede wszystkim na obowiązkach poszczególnych podmiotów, nie tworząc jednolitego modelu współpracy pomiędzy operatorami infrastruktury

34 Zob. przypis 20.

krytycznej, administracją publiczną oraz instytucjami odpowiedzialnymi za cyberbezpieczeństwo. Po drugie, niewystarczająco rozwinięte pozostają mechanizmy wymiany informacji o zagrożeniach pomiędzy sektorem publicznym i prywatnym. Po trzecie, obowiązujące regulacje nie uwzględniają w pełni specyfiki infrastruktury podmorskiej, której funkcjonowanie wykracza poza granice jednego państwa. Po czwarte, brak jest jednolitego modelu oceny cyberodporności infrastruktury krytycznej integrującego wymagania wynikające z NIS2, CER, norm ISO oraz praktyki zarządzania bezpieczeństwem.

To właśnie ta luka uzasadnia potrzebę wskazania modelu, przedstawionego w kolejnej części artykułu.

4 | Zarządzanie ryzykiem hybrydowym jako element cyberodporności

Cyfrowa transformacja sektora morskiego spowodowała, że cyberprzestrzeń stała się pełnoprawnym środowiskiem prowadzenia działań wpływających na bezpieczeństwo państwa. W przeciwieństwie do klasycznych zagrożeń, cyberataki umożliwiają osiągnięcie istotnych skutków operacyjnych bez konieczności użycia siły militarnej. Zakłócenie systemów zarządzania portem, manipulacja danymi nawigacyjnymi, przejęcie kontroli nad systemami automatyki przemysłowej czy czasowe unieruchomienie sieci energetycznych mogą prowadzić do znaczących strat gospodarczych oraz destabilizacji funkcjonowania państwa.

Szczególnie istotnym problemem pozostaje rosnąca integracja technologii operacyjnych z klasycznymi systemami informatycznymi. Integracja ta zwiększa efektywność zarządzania infrastrukturą, jednocześnie jednak rozszerza powierzchnię potencjalnego ataku. W konsekwencji cyberbezpieczeństwo infrastruktury krytycznej nie może być rozpatrywane wyłącznie jako problem techniczny, lecz powinno być analizowane jako element bezpieczeństwa narodowego oraz bezpieczeństwa prawnego.

Bezpieczeństwo morskie przez wiele lat utożsamiano przede wszystkim z ochroną żeglugi, bezpieczeństwem nawigacji, przeciwdziałaniem katastrofom morskim oraz ochroną granic państwowych. Takie ujęcie odpowiadało dominującym zagrożeniom XX wieku, których źródłem były głównie czynniki naturalne, błędy ludzkie, awarie techniczne lub klasyczne konflikty zbrojne. Rozwój gospodarki cyfrowej oraz postępująca integracja

systemów teleinformatycznych z infrastrukturą morską spowodowały jednak zasadniczą zmianę charakteru zagrożeń. Współczesne bezpieczeństwo morskie obejmuje nie tylko ochronę fizyczną infrastruktury, lecz również bezpieczeństwo systemów informacyjnych, sieci teleinformatycznych oraz procesów decyzyjnych wspierających funkcjonowanie państwa i gospodarki.

Proces cyfryzacji infrastruktury morskiej sprawił, że porty, terminale przeładunkowe, farmy wiatrowe offshore, podmorskie sieci energetyczne, gazociągi oraz systemy monitorowania ruchu statków funkcjonują jako złożone systemy cyberfizyczne. W rezultacie zakłócenie integralności, poufności lub dostępności informacji może prowadzić do skutków porównywalnych z fizycznym zniszczeniem infrastruktury. Oznacza to, że bezpieczeństwo informacji staje się jednym z podstawowych warunków zapewnienia bezpieczeństwa morskiego, rozwijając kierunek badań wskazany we wcześniejszych analizach jednego z autorów artykułu dotyczących zależności pomiędzy informacją a bezpieczeństwem działalności człowieka na morzu[35].

Zmiana charakteru zagrożeń powoduje również zmianę sposobu postrzegania bezpieczeństwa państwa. Coraz częściej celem działań przeciwnika nie jest fizyczne zniszczenie infrastruktury, lecz wywołanie zakłóceń funkcjonowania państwa poprzez ingerencję w systemy teleinformatyczne, manipulację informacją lub ograniczenie zdolności decyzyjnych administracji publicznej i operatorów infrastruktury krytycznej.

Morze Bałtyckie stanowi jeden z najbardziej nasyconych infrastrukturą strategiczną akwenów świata. Znajdują się tam podmorskie gazociągi, sieci elektroenergetyczne, kable światłowodowe, terminale LNG, porty o znaczeniu międzynarodowym oraz dynamicznie rozwijająca się infrastruktura odnawialnych źródeł energii. Funkcjonowanie tych obiektów ma zasadnicze znaczenie dla bezpieczeństwa energetycznego, gospodarczego oraz militarnego państw regionu.

Specyfika infrastruktury morskiej powoduje, że jest ona szczególnie podatna na oddziaływanie zagrożeń hybrydowych. Znaczna część infrastruktury znajduje się poza bezpośrednim nadzorem administracji publicznej, często w środowisku trudnym do monitorowania, a jednocześnie jej prawidłowe funkcjonowanie zależy od rozbudowanych systemów

35 Klaudia Skelnik, K. Sobczyńska, Martyna Bartkowska-Dąbrowska, „Wpływ informacji na bezpieczeństwo morskie" *Gospodarka Materiałowa i Logistyka*, nr 12 (2017).

teleinformatycznych oraz automatyki przemysłowej. Powoduje to zatarcie granicy pomiędzy bezpieczeństwem fizycznym a cyberbezpieczeństwem.

Jednocześnie współczesne zagrożenia nie dotyczą wyłącznie pojedynczych obiektów infrastruktury. Coraz częściej ich celem staje się naruszenie ciągłości świadczenia usług kluczowych poprzez jednoczesne oddziaływanie na wiele elementów systemu, co odpowiada logice współczesnych działań hybrydowych.

Najbardziej charakterystyczną cechą współczesnego środowiska bezpieczeństwa jest przenikanie się różnorodnych form oddziaływania. Cyberataki coraz częściej stanowią jedynie jeden z elementów szerszych operacji obejmujących działania dezinformacyjne, presję ekonomiczną, sabotaż infrastruktury, wykorzystanie sztucznej inteligencji do automatyzacji ataków oraz oddziaływanie psychologiczne na społeczeństwo.

W literaturze przedmiotu podkreśla się, że działania hybrydowe są ukierunkowane przede wszystkim na wykorzystanie podatności systemowych przeciwnika. W przypadku infrastruktury krytycznej Morza Bałtyckiego podatności te wynikają z wysokiego poziomu cyfryzacji, transgranicznego charakteru infrastruktury, wielości podmiotów odpowiedzialnych za jej ochronę oraz rozproszenia kompetencji pomiędzy administrację publiczną, operatorów prywatnych i organizacje międzynarodowe[36].

Tak rozumiane zagrożenia wykraczają poza tradycyjne ramy prawa bezpieczeństwa, wymagając integracji instrumentów prawa administracyjnego, prawa Unii Europejskiej, prawa morskiego oraz regulacji dotyczących cyberbezpieczeństwa.

Przedstawione uwarunkowania prowadzą do wniosku, że dotychczasowe modele ochrony infrastruktury krytycznej, oparte przede wszystkim na zabezpieczeniach fizycznych oraz klasycznym zarządzaniu ryzykiem, nie odpowiadają w pełni współczesnym zagrożeniom. Ochrona infrastruktury krytycznej Morza Bałtyckiego wymaga budowania cyberodporności rozumianej jako zdolność do zapobiegania incydentom, ich wykrywania, utrzymania ciągłości działania, skutecznego reagowania oraz szybkiego odtwarzania zdolności operacyjnych.

Tak rozumiana cyberodporność powinna stanowić element szerszego systemu zarządzania bezpieczeństwem obejmującego aspekty prawne, organizacyjne, technologiczne oraz informacyjne. Wymaga to odejścia od

36 Zob. Keplin, „Działania hybrydowe na Morzu Bałtyckim", 54–68.

sektorowego postrzegania cyberbezpieczeństwa na rzecz zintegrowanego modelu governance, uwzględniającego współpracę administracji publicznej, operatorów infrastruktury krytycznej, podmiotów odpowiedzialnych za cyberbezpieczeństwo oraz organizacji międzynarodowych. Właśnie ta potrzeba uzasadnia opracowanie modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego, przedstawionego w dalszej części artykułu.

5 | Model prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego

Przeprowadzona analiza wskazuje, że obowiązujące regulacje prawne tworzą rozbudowany system wymagań dotyczących ochrony infrastruktury krytycznej, jednak nie zapewniają kompleksowego modelu integrującego aspekty prawne, organizacyjne i technologiczne. Zarówno dyrektywa NIS2, jak i dyrektywa CER koncentrują się przede wszystkim na określeniu obowiązków podmiotów kluczowych oraz wymagań dotyczących zarządzania ryzykiem, pozostawiając znaczną swobodę w zakresie wyboru metod ich realizacji.

Zaproponowany przez autorów model nie stanowi alternatywy dla obowiązujących regulacji, lecz narzędzie wspierające ich praktyczną implementację. Integruje wymagania wynikające z prawa Unii Europejskiej, prawa krajowego oraz standardów zarządzania bezpieczeństwem w spójną strukturę zarządczą, umożliwiając operatorom infrastruktury krytycznej budowanie cyberodporności w sposób systemowy i zgodny z zasadą ciągłego doskonalenia. Model ten może być wykorzystywany jako punkt odniesienia przy projektowaniu systemów zarządzania bezpieczeństwem informacji, przygotowywaniu analiz ryzyka, opracowywaniu planów ciągłości działania oraz prowadzeniu audytów zgodności z wymaganiami regulacyjnymi.

Najbardziej innowacyjnym elementem modelu jest włączenie odporności informacyjnej jako odrębnego filaru cyberodporności infrastruktury krytycznej. W dotychczasowych opracowaniach bezpieczeństwo informacji analizowane jest najczęściej przez pryzmat klasycznych atrybutów poufności, integralności i dostępności danych. Takie podejście nie obejmuje jednak zagrożeń wynikających z dezinformacji, manipulacji informacją czy wykorzystania sztucznej inteligencji do wpływania na procesy decyzyjne.

W proponowanym modelu odporność informacyjna oznacza zdolność organizacji do pozyskiwania, oceny i wykorzystywania wiarygodnych informacji w sposób zapewniający ciągłość oraz jakość procesów decyzyjnych. Obejmuje ona zarówno ochronę informacji, jak i budowanie kompetencji organizacyjnych umożliwiających rozpoznawanie manipulacji informacyjnych oraz przeciwdziałanie ich skutkom. Rozszerzenie klasycznego podejścia do bezpieczeństwa informacji o komponent odporności informacyjnej wpisuje się w aktualne kierunki rozwoju badań nad bezpieczeństwem oraz odpowiada na wyzwania związane z rosnącym znaczeniem sztucznej inteligencji i działań hybrydowych.

Głównym założeniem autorów było połączenie perspektywy normatywnej z praktyką zarządzania bezpieczeństwem. W literaturze przedmiotu zagadnienia te są zazwyczaj analizowane odrębnie: badania prawnicze koncentrują się na wykładni przepisów, natomiast nauki o bezpieczeństwie skupiają się na analizie ryzyka, odporności organizacyjnej oraz technicznych aspektach ochrony infrastruktury. Proponowany model zakłada, że skuteczna cyberodporność nie jest wyłącznie efektem zgodności z przepisami prawa ani rezultatem wdrożenia określonych technologii. Jest ona konsekwencją współdziałania regulacji prawnych, właściwego podziału odpowiedzialności, efektywnego zarządzania ryzykiem, współpracy międzyinstytucjonalnej oraz budowania kultury bezpieczeństwa. Takie podejście pozwala ograniczyć ryzyko fragmentaryzacji systemu ochrony infrastruktury krytycznej i wzmacnia zdolność organizacji do reagowania na złożone zagrożenia hybrydowe.

Przedstawiony model ma charakter koncepcyjny i stanowi propozycję integracji istniejących rozwiązań prawnych oraz organizacyjnych. Nie był dotychczas przedmiotem empirycznej weryfikacji w środowisku operatorów infrastruktury krytycznej. Ograniczeniem opracowania jest również dynamiczny rozwój regulacji dotyczących cyberbezpieczeństwa oraz sztucznej inteligencji, który może wpływać na konieczność dalszej aktualizacji modelu. Ponadto specyfika infrastruktury krytycznej Morza Bałtyckiego powoduje, że skuteczność proponowanych rozwiązań zależy od poziomu współpracy międzynarodowej oraz gotowości poszczególnych państw do wymiany informacji i koordynacji działań.

Zdaniem autorów dla budowy tego modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego

Rys. 1. Model prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego



Źródło: opracowanie własne z wykorzystaniem narzędzia ChatGPT

konieczne jest wskazanie siedmiu wzajemnie powiązanych filarów związanych z bezpieczeństwem Morza Bałtyckiego:

1) Legal Governance – zgodność z NIS2, CER, AI Act, UNCLOS i prawem krajowym.
2) Strategic Risk Management – identyfikacja i ocena ryzyka z wykorzystaniem ISO 31000 i ISO/IEC 27005.
3) Cyber Resilience – ochrona systemów IT, OT oraz ICS/SCADA.
4) Maritime Situational Awareness – monitorowanie środowiska morskiego, AIS, VTS, satelitów i systemów wykrywania zagrożeń.
5) Information Resilience – zapewnienie wiarygodności informacji, przeciwdziałanie dezinformacji i odporność procesów decyzyjnych.
6) Interinstitutional Cooperation – współpraca administracji morskiej, operatorów infrastruktury, CSIRT, Marynarki Wojennej, Straży Granicznej, ENISA, EMSA i NATO.
7) Continuous Improvement – audyty, ćwiczenia, testy odporności, analiza incydentów oraz doskonalenie systemu

Na podstawie wyodrębnienia tych filarów autorzy proponują model, który różni się od dotychczasowych koncepcji prezentowanych w literaturze przedmiotu z trzech zasadniczych powodów. Po pierwsze, integruje regulacje prawne z procesami zarządzania bezpieczeństwem, tworząc wspólną płaszczyznę analizy dla nauk prawnych i nauk o bezpieczeństwie. Po drugie, uwzględnia specyfikę infrastruktury krytycznej Morza Bałtyckiego jako systemu transgranicznego, funkcjonującego w środowisku wielopoziomowego zarządzania. Po trzecie, wprowadza kategorię odporności informacyjnej jako jednego z podstawowych elementów cyberodporności infrastruktury krytycznej, rozwijając wcześniejsze ustalenia jednej z autorek dotyczące wpływu informacji na bezpieczeństwo morskie.

Następnie autorzy artykułu przeprowadzili mapowanie poszczególnych filarów modelu na wybrane regulacje prawne determinujące bezpieczeństwo i cyberodporność infrastruktury krytycznej Morza Bałtyckiego. Zestawienie wskazuje, że proponowany model nie stanowi odrębnego od istniejącego systemu regulacyjnego mechanizmu zarządzania, lecz integruje wymagania wynikające z różnych reżimów prawnych w ramach jednej koncepcji zarządzania cyberodpornością. Analiza regulacyjna wskazuje przede wszystkim na wielopoziomowy i międzysektorowy charakter podstaw prawnych cyberodporności. Dyrektywa NIS2 koncentruje się na zarządzaniu ryzykiem cyberbezpieczeństwa, stosowaniu odpowiednich środków zarządzania ryzykiem oraz reagowaniu na incydenty. Dyrektywa CER rozszerza perspektywę o odporność podmiotów krytycznych, podkreślając potrzebę uwzględniania zagrożeń o charakterze fizycznym i organizacyjnym oraz stosowania podejścia opartego na analizie ryzyka. Oba akty należy zatem postrzegać jako regulacje komplementarne, pozwalające na łączenie cyberbezpieczeństwa z szerzej rozumianą odpornością infrastruktury krytycznej. AI Act[37] wprowadza do modelu dodatkowy wymiar związany z wykorzystaniem systemów sztucznej inteligencji. Znaczenie tej regulacji wzrasta wraz z zastosowaniem AI m.in. w analizie danych, monitorowaniu infrastruktury, wykrywaniu anomalii oraz wspomaganiu procesów

37 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. Urz. UE L 2024/1689 z 12.07.2024; dalej: AI Act).

decyzyjnych. Z punktu widzenia wskazanego modelu szczególnego znaczenia nabierają w tym zakresie zarządzanie ryzykiem, jakość i integralność danych, przejrzystość, cyberbezpieczeństwo oraz zapewnienie właściwego poziomu nadzoru człowieka.

Odrębny wymiar regulacyjny tworzą UNCLOS[38] oraz ISPS Code[39], osadzające analizowany model w specyfice środowiska morskiego. Regulacje te pozwalają powiązać cyberodporność z bezpieczeństwem żeglugi, bezpieczeństwem statków i obiektów portowych oraz międzynarodową współpracą w zakresie bezpieczeństwa morskiego. Ma to szczególne znaczenie w regionie Morza Bałtyckiego, gdzie znaczna część infrastruktury krytycznej ma charakter transgraniczny lub jest bezpośrednio związana z przestrzenią morską.

Na poziomie krajowym istotną funkcję pełnią przepisy dotyczące krajowego systemu cyberbezpieczeństwa, które określają obowiązki podmiotów objętych systemem, mechanizmy współpracy oraz zasady reagowania na incydenty. W praktyce oznacza to konieczność przełożenia wymagań europejskich i krajowych na konkretne mechanizmy zarządzania funkcjonujące na poziomie operatora infrastruktury.

Przeprowadzone mapowanie pokazuje jednocześnie, że poszczególne filary modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego nie odpowiadają pojedynczym regulacjom w relacji jeden do jednego. Przeciwnie – każdy z nich znajduje podstawę w kilku wzajemnie uzupełniających się reżimach prawnych. Dotyczy to szczególnie Strategic Risk Governance, Information Resilience oraz Cooperative Security Governance, które wymagają jednoczesnego uwzględnienia regulacji dotyczących cyberbezpieczeństwa, odporności infrastruktury, zarządzania informacją, bezpieczeństwa morskiego oraz współpracy instytucjonalnej.

Tabela potwierdza tym samym zasadność przyjęcia w modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego podejścia zintegrowanego, łączącego *legal governance*,

38 Konwencja Narodów Zjednoczonych o prawie morza, sporządzona w Montego Bay dnia 10 grudnia 1982 r. (Dz. U. z 2002 r., nr 59, poz. 543; dalej: UNCLOS).

39 Międzynarodowy kodeks ochrony statku i obiektu portowego (International Ship and Port Facility Security Code, ISPS Code), przyjęty przez Międzynarodową Organizację Morską w 2002 r. jako uzupełnienie rozdziału XI-2 Międzynarodowej konwencji o bezpieczeństwie życia na morzu (SOLAS).

Tabela 1. Mapowanie modelu do obowiązujących regulacji prawnych

Filar modelu	NIS2	CER	AI Act	UNCLOS / ISPS	Ustawa o KSC
I. Legal Governance	zarządzanie cyberbezpieczeństwem	odporność podmiotów krytycznych	governance AI	bezpieczeństwo żeglugi	obowiązki operatorów
II. Strategic Risk Governance	analiza ryzyka	ocena ryzyka	ocena ryzyka AI	planowanie bezpieczeństwa	szacowanie ryzyka
III. Cybersecurity Management	środki techniczne	ochrona infrastruktury	bezpieczeństwo systemów AI	ochrona systemów portowych	środki organizacyjne i techniczne
IV. Maritime Situational Awareness	monitorowanie incydentów	monitorowanie zagrożeń	monitoring AI	bezpieczeństwo ruchu morskiego	wykrywanie incydentów
V. Information Resilience	bezpieczeństwo informacji	ciągłość usług	transparentność AI	wymiana informacji	bezpieczeństwo informacji
VI. Cooperative Security	współpraca CSIRT	współpraca organów	współpraca nadzorcza	współpraca międzynarodowa	współpraca operatorów
VII. Continuous Improvement	audyty	testowanie odporności	monitoring zgodności	ćwiczenia bezpieczeństwa	doskonalenie SZBI

Źródło: Opracowanie własne na podstawie dyrektyw NIS2, CER, AI Act, UNCLOS, ISPS Code oraz ustawy o krajowym systemie cyberbezpieczeństwa

zarządzanie ryzykiem, cyberbezpieczeństwo, świadomość sytuacyjną, odporność informacyjną, współpracę instytucjonalną oraz ciągłe doskonalenie. Regulacje prawne nie są w takim ujęciu traktowane wyłącznie jako źródło obowiązków compliance, lecz jako jeden z mechanizmów kształtowania odporności całego systemu infrastruktury krytycznej.

Autorzy proponują również podział ról i odpowiedzialności pomiędzy głównymi kategoriami podmiotów uczestniczących w zarządzaniu cyberodpornością infrastruktury krytycznej Morza Bałtyckiego, wykorzystując metodę RACI[40] (Responsible, Accountable, Consulted, Informed). Zastosowanie tego narzędzia pozwala przełożyć założenia modelu BCI-CRGM z poziomu koncepcyjnego na poziom organizacyjny, wskazując podmioty realizujące określone działania, ponoszące odpowiedzialność za ich

40 Zob. Urszula Jeż, „Analiza interesariuszy i jej wpływ na sukces projektu", [w:] *Wybrane zagadnienia zarządzania projektami w przedsiębiorstwach informatycznych*, nr 6, red. Jan Werewka (Kraków: AGH, 2015).

wykonanie, uczestniczące w konsultacjach oraz wymagające zapewnienia odpowiedniego poziomu informacji.

Podstawowym założeniem macierzy jest przyjęcie, że cyberodporność infrastruktury krytycznej stanowi odpowiedzialność rozproszoną, której nie można przypisać wyłącznie operatorowi infrastruktury lub organom administracji publicznej. Operator infrastruktury pozostaje podmiotem odpowiedzialnym przede wszystkim za identyfikację i analizę ryzyka na poziomie operacyjnym, wdrażanie środków bezpieczeństwa, reagowanie w ramach własnych struktur oraz uczestnictwo w ćwiczeniach, audytach i procesach doskonalenia. Wynika to z jego bezpośredniej wiedzy o procesach technologicznych, aktywach, podatnościach oraz potencjalnych skutkach zakłócenia ciągłości działania.

Administracja morska odgrywa szczególną rolę w odniesieniu do fizycznego wymiaru bezpieczeństwa infrastruktury oraz bezpieczeństwa przestrzeni morskiej. Jej funkcje powinny być przy tym postrzegane w powiązaniu z zadaniami innych właściwych organów administracji oraz struktur odpowiedzialnych za zarządzanie kryzysowe.

Istotną funkcję w modelu pełnią również CSIRT[41], które wspierają wykrywanie, analizę, obsługę i koordynację reakcji na incydenty cyberbezpieczeństwa oraz wymianę informacji o zagrożeniach. Z perspektywy BCI-CRGM ich znaczenie polega przede wszystkim na zapewnieniu przepływu informacji pomiędzy poziomem operacyjnym i instytucjonalnym oraz wspieraniu budowania wspólnej świadomości sytuacyjnej.

Minister lub inny właściwy organ administracji publicznej pełni natomiast funkcję związaną z nadzorem, koordynacją oraz kształtowaniem strategicznych warunków funkcjonowania systemu. Dotyczy to zwłaszcza zarządzania kryzysowego, nadzoru nad realizacją obowiązków prawnych, inicjowania lub koordynowania ćwiczeń oraz wykorzystywania wyników audytów i ocen do dalszego doskonalenia systemu bezpieczeństwa.

W modelu uwzględniono ponadto wymiar ponadnarodowy, reprezentowany przez ENISA, EMSA oraz NATO. Rola tych podmiotów nie polega na zastępowaniu krajowych organów lub operatorów, lecz na wspieraniu współpracy, wymiany informacji, budowania zdolności, tworzenia dobrych praktyk oraz rozwijania interoperacyjności działań. Jest to szczególnie istotne w regionie Morza Bałtyckiego, gdzie infrastruktura

41 Zob. https://csirt.gov.pl/.

Tabela 2. Macierz odpowiedzialności (RACI) dla cyberodporności infrastruktury krytycznej Morza Bałtyckiego[42]

Proces	Operator IK	Administracja morska	CSIRT	Minister właściwy	ENISA/EMSA	NATO
Identyfikacja ryzyka	**R**	C	C	I	I	I
Analiza ryzyka	**R**	C	C	A	I	I
Zarządzanie cyberbezpieczeństwem	**R**	C	**A**	I	I	I
Ochrona fizyczna infrastruktury	**R**	**A**	I	C	I	I
Wymiana informacji	C	C	**A**	I	**R**	C
Reakcja na incydent	**R**	C	**A**	I	C	C
Zarządzanie kryzysowe	C	**R**	C	**A**	I	C
Ćwiczenia	**R**	C	C	A	C	C
Audyty	**R**	C	C	**A**	I	I
Doskonalenie systemu	**R**	C	C	A	I	I

Źródło: Opracowanie własne

energetyczna, telekomunikacyjna i transportowa tworzy system wzajemnych zależności przekraczających granice poszczególnych państw.

Macierz RACI wskazuje zatem na potrzebę odejścia od sektorowego i instytucjonalnie izolowanego modelu ochrony infrastruktury na rzecz modelu współodpowiedzialności i skoordynowanego zarządzania. Szczególnego znaczenia nabiera w nim wymiana informacji, ponieważ stanowi element łączący identyfikację ryzyka, świadomość sytuacyjną, reagowanie na incydenty, zarządzanie kryzysowe oraz proces ciągłego doskonalenia.

Przedstawioną macierz należy traktować jako model koncepcyjny, a nie jako normatywne przypisanie kompetencji konkretnym organom. Ostateczny podział odpowiedzialności w przypadku określonego rodzaju infrastruktury powinien każdorazowo wynikać z obowiązujących przepisów prawa krajowego i unijnego, charakteru danego sektora, właściwości organów administracji oraz struktury organizacyjnej operatora. Wartość macierzy polega przede wszystkim na wskazaniu konieczności jednoznacznego określenia odpowiedzialności oraz kanałów współpracy przed wystąpieniem incydentu, a nie dopiero w fazie reagowania kryzysowego.

Na podstawie modelu prawnego i organizacyjnego zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego oraz analizy przeprowadzonej z użyciem macierzy odpowiedzialności, która wykazała konieczność współodpowiedzialności i skoordynowanego zarządzania, autorzy przedstawiają poniżej propozycję założeń do budowy systemu zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego.

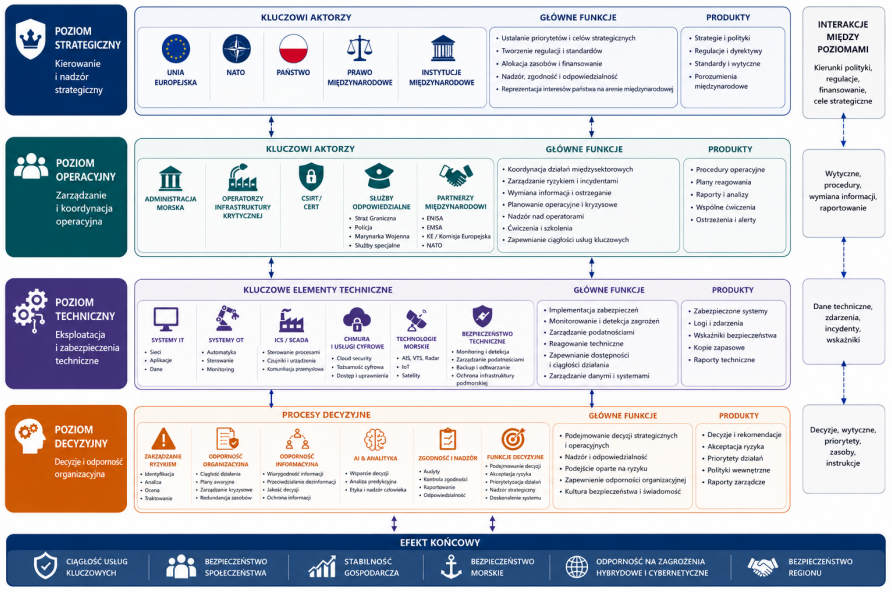
Przedstawiony na poniższym rysunku proces zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego ma charakter ciągły, iteracyjny i adaptacyjny. Jego konstrukcja odzwierciedla założenie, że cyberodporność nie powinna być utożsamiana wyłącznie z ochroną systemów przed wystąpieniem incydentu, lecz obejmuje również zdolność organizacji i systemów infrastruktury krytycznej do przewidywania zagrożeń, absorpcji zakłóceń, reagowania na incydenty, odtwarzania kluczowych funkcji oraz uczenia się na podstawie zaistniałych zdarzeń. Takie ujęcie pozwala traktować cyberodporność infrastruktury krytycznej Morza Bałtyckiego nie jako statyczny zbiór zabezpieczeń technicznych, lecz jako dynamiczną zdolność systemową, łączącą wymiar prawny, organizacyjny, techniczny i zarządczy. W warunkach transgraniczności infrastruktury bałtyckiej oraz wzrastającej skali zagrożeń hybrydowych szczególnego znaczenia nabiera przy tym zdolność do ciągłego uczenia się, adaptacji oraz koordynacji działań pomiędzy operatorami infrastruktury, administracją publiczną i podmiotami odpowiedzialnymi za bezpieczeństwo.

Zaproponowany model obrazuje wielopoziomowy system zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego, oparty na integracji wymiaru strategicznego, operacyjnego, technicznego oraz decyzyjnego. Poszczególne poziomy tworzą wzajemnie powiązany układ odpowiedzialności, przepływu informacji oraz procesów zarządzania ryzykiem, którego celem jest zapewnienie odporności infrastruktury krytycznej na zagrożenia cybernetyczne i hybrydowe.

Poziom strategiczny odpowiada za kształtowanie polityki bezpieczeństwa, tworzenie ram prawnych oraz koordynację międzynarodową z udziałem instytucji Unii Europejskiej, NATO oraz organów państwowych. Na poziomie operacyjnym realizowane są zadania związane z zarządzaniem bezpieczeństwem infrastruktury krytycznej, wymianą informacji

42 Legenda: **R** – Responsible (realizuje); **A** – Accountable (ponosi odpowiedzialność); **C** – Consulted (konsultowany); **I** – Informed (informowany)

Rys. 2. Proces zarządzania cyberodpornością infrastruktury krytycznej Morza Bałtyckiego



Źródło: opracowanie własne z wykorzystaniem narzędzia ChatGPT

o zagrożeniach, reagowaniem na incydenty oraz współpracą pomiędzy administracją publiczną, operatorami infrastruktury i wyspecjalizowanymi podmiotami odpowiedzialnymi za cyberbezpieczeństwo.

Poziom techniczny obejmuje systemy informatyczne (IT), technologie operacyjne (OT), przemysłowe systemy sterowania (ICS/SCADA), technologie morskie oraz rozwiązania chmurowe, stanowiące podstawę funkcjonowania współczesnej infrastruktury krytycznej. Ich zadaniem jest zapewnienie ciągłości działania, wykrywanie zagrożeń, ochrona danych oraz utrzymanie odpowiedniego poziomu bezpieczeństwa technicznego.

Na poziomie decyzyjnym integrowane są wyniki analiz ryzyka, informacje operacyjne oraz dane techniczne w celu podejmowania decyzji strategicznych i operacyjnych. Kluczowe znaczenie mają tutaj procesy zarządzania ryzykiem, odporność organizacyjna i informacyjna, wykorzystanie analityki oraz sztucznej inteligencji przy zachowaniu nadzoru człowieka nad procesem decyzyjnym.

Model zakłada dwukierunkowy przepływ informacji pomiędzy wszystkimi poziomami zarządzania, umożliwiający bieżące monitorowanie zagrożeń,

koordynację działań oraz ciągłe doskonalenie systemu cyberodporności. Efektem funkcjonowania modelu jest zwiększenie odporności infrastruktury krytycznej Morza Bałtyckiego, zapewnienie ciągłości świadczenia usług kluczowych oraz wzmocnienie bezpieczeństwa państwa i regionu.

Przedstawiony model tworzy podstawę do dalszych badań zarówno o charakterze teoretycznym, jak i empirycznym. W pierwszej kolejności zasadne wydaje się opracowanie zestawu wskaźników umożliwiających ocenę poziomu cyberodporności infrastruktury krytycznej oraz odporności informacyjnej operatorów. Pozwoliłoby to na porównywanie poziomu przygotowania organizacji oraz identyfikację obszarów wymagających doskonalenia.

Kolejnym kierunkiem badań powinno być empiryczne zweryfikowanie modelu w wybranych sektorach infrastruktury krytycznej regionu Morza Bałtyckiego, takich jak porty morskie, terminale LNG, infrastruktura energetyczna offshore czy podmorskie sieci telekomunikacyjne. Weryfikacja mogłaby zostać przeprowadzona z wykorzystaniem studiów przypadków, analiz porównawczych oraz badań eksperckich z udziałem przedstawicieli administracji publicznej i operatorów infrastruktury.

Perspektywicznym kierunkiem rozwoju modelu jest również jego rozszerzenie o moduł oceny wykorzystania sztucznej inteligencji w procesach zarządzania bezpieczeństwem oraz analizę wpływu technologii autonomicznych na cyberodporność infrastruktury morskiej.

6 | Wnioski

Transformacja cyfrowa infrastruktury krytycznej Morza Bałtyckiego powoduje, że bezpieczeństwo regionu nie może być analizowane wyłącznie przez pryzmat ochrony fizycznej obiektów. Coraz większego znaczenia nabierają cyberbezpieczeństwo, odporność organizacyjna oraz zdolność do zapewnienia ciągłości funkcjonowania usług kluczowych w warunkach zagrożeń hybrydowych. W konsekwencji skuteczna ochrona infrastruktury krytycznej wymaga zintegrowanego podejścia, łączącego regulacje prawne, zarządzanie ryzykiem, współpracę międzyinstytucjonalną oraz nowoczesne rozwiązania technologiczne.

Przeprowadzona analiza wykazała, że obowiązujące regulacje prawne tworzą solidne podstawy ochrony infrastruktury krytycznej, jednak nie zapewniają jednolitego modelu integrującego wszystkie elementy

cyberodporności. Rozproszenie kompetencji, wielość aktów prawnych oraz transgraniczny charakter infrastruktury Morza Bałtyckiego uzasadniają potrzebę opracowania kompleksowych narzędzi wspierających zarządzanie bezpieczeństwem.

Odpowiedzią na zidentyfikowaną lukę jest przedstawiony przez autorów model, który integruje siedem filarów cyberodporności: governance prawny, zarządzanie ryzykiem, cyberbezpieczeństwo, świadomość sytuacyjną, odporność informacyjną, współpracę międzyinstytucjonalną oraz ciągłe doskonalenie. Jego wartość polega na połączeniu perspektywy nauk prawnych z dorobkiem nauk o bezpieczeństwie oraz stworzeniu ram umożliwiających praktyczną implementację wymagań wynikających z prawa Unii Europejskiej i prawa krajowego.

Szczególnym wkładem niniejszego opracowania jest rozwinięcie koncepcji odporności informacyjnej jako integralnego elementu cyberodporności infrastruktury krytycznej. W warunkach narastających zagrożeń hybrydowych jakość informacji oraz zdolność organizacji do ich krytycznej oceny stają się równie istotne jak zabezpieczenia techniczne czy zgodność z wymaganiami regulacyjnymi. Proponowany model może stanowić podstawę dalszych badań nad pomiarem cyberodporności oraz projektowaniem rozwiązań wspierających bezpieczeństwo infrastruktury krytycznej zarówno w regionie Morza Bałtyckiego, jak i w innych obszarach o strategicznym znaczeniu dla bezpieczeństwa państwa i Unii Europejskiej.

Bibliografia

Ani Uchenna Daniel, Jeremy McKendrick Watson, Madeline Carr, Al Cook, Jason R.C. Nurse, „A Review of the Use and Utility of Industrial Network-Based Open Source Simulators: Functionality, Security, and Policy Viewpoints" *The Journal of Defense Modeling and Simulation* 19, nr 3 (2022): 263–286.

Becker Manuel, „Transposing EU-Legislation on Critical Infrastructure Protection: Legal Implementation Performance in the Baltic Sea Region" *International Journal of Critical Infrastructure Protection* 50 (2025), art. 100781.

Bueger Christian, Tobias Liebetrau, „Critical Maritime Infrastructure Protection: What's the Trouble?" *Marine Policy* 155 (2023), art. 105772.

Ćelić Jasmin, Marko Vukšić, Robert Baždarić, Aleksandar Cuculić, „The Challenges of Cyber Resilience in the Maritime Sector: Addressing the Weak Awareness of the Dangers Caused by Cyber Threats" *Journal of Marine Science and Engineering*, nr 4 (2025), art. 762.

European Union Agency for Cybersecurity (ENISA), *Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector*. Athens: ENISA, 2019.

Gac Miłosz, „Flota Bałtycka w polityce bezpieczeństwa morskiego Rosji: historia i współczesność" *Rocznik Bezpieczeństwa Międzynarodowego*, nr 2 (2024): 37–62.

Gac Miłosz, „Wpływ wojny w Ukrainie na politykę bezpieczeństwa morskiego NATO w basenie Morza Bałtyckiego" *De Securitate et Defensione. O Bezpieczeństwie i Obronności*, nr 1 (2025): 7–26.

Gudmestad Ove Tobias, Thomas Lundberg, „Security and Safe Operations of Offshore Cables and Pipelines" *Ocean Engineering*, 360 (2026), art. 125958.

Jeż Urszula, „Analiza interesariuszy i jej wpływ na sukces projektu", [w:] *Wybrane zagadnienia zarządzania projektami w przedsiębiorstwach informatycznych*, nr 6, red. Jan Werewka. Kraków: AGH, 2015.

Keplin Jarosław, „Działania hybrydowe na Morzu Bałtyckim. Zarys problemu dla bezpieczeństwa Rzeczypospolitej Polskiej" *De Securitate et Defensione. O Bezpieczeństwie i Obronności*, nr 2 (2022): 54–68.

Labutis Gintaras, „Strengthening the Critical Infrastructures in Lithuania: From Protection Towards Resilience", [w:] *Democratic Resilience in the Baltics*, vol. I, *Resilient Governance and Democratic Stability*, ed. David Schultz, Rasa Smaliukienė, Vidmantė Giedraitytė. Cham: Springer, 2026.

Liebetrau Tobias, Christian Bueger, „Advancing Coordination in Critical Maritime Infrastructure Protection: Lessons from Maritime Piracy and Cybersecurity" *International Journal of Critical Infrastructure Protection* 46 (2024), art. 100683.

Makowski Andrzej, „Dilemmas Faced in Developing Small Navies" *Naval War College Review*, nr 1 (2023), art. 7.

Masik Grzegorz, „Koncepcja odporności: definicje, interpretacje, podejścia badawcze oraz szkoły myśli" *Przegląd Geograficzny*, nr 3 (2022): 279–305.

Mickiewicz Piotr, „Bałtyk jako obszar występowania najpoważniejszych zagrożeń dla bezpieczeństwa energetycznego Polski" *Teologia Polityczna Co Tydzień*, nr 430 (2024).

Mickiewicz Piotr, „Morze Bałtyckie w założeniach strategii morskich i polityk bezpieczeństwa narodowego państw bałtyckich. Wnioski dla koncepcji bezpieczeństwa morskiego RP" *Studia Bezpieczeństwa Narodowego*, nr 1 (2014): 339–365.

Schinas Orestis, Daniel Metzger, „Cyber-seaworthiness: A Critical Review of the Literature" *Marine Policy*, 151 (2023), art. 105592.

Schwarz Monina, Matthias Marx, Hannes Federrath, „A Structured Analysis of Information Security Incidents in the Maritime Sector", arXiv:2112.06545 (2021).

Skelnik Klaudia, Katarzyna Sobczyńska, Martyna Bartkowska-Dąbrowska, „Wpływ informacji na bezpieczeństwo morskie" *Gospodarka Materiałowa i Logistyka*, nr 12 (2017): 387–400.

Štitilis Darius, Marius Laurinaitis, Matt Warren, „Hybrid Cyber Threats: Lithuanian Context" *Journal of Information Warfare*, nr 1 (2024): 131–142.

Szubrycht Tomasz, *Bałtyckie wymiary bezpieczeństwa*. Gdynia: Wydawnictwo Akademickie AMW, 2010.

Szubrycht Tomasz, „Sojusznicza odpowiedź na zagrożenia na Morzu Bałtyckim" *Bezpieczeństwo Narodowe*, nr 1 (2025): 49–76.

Vasan Danish, Mohammad Hammoudeh, Adel F. Ahmed, Hamad Naeem, „Cyber-attacks: Securing Ship Navigation Systems Using Multi-Layer Cross-Validation Defense" *Computers & Security*, 160 (2026), art. 104706.

Wielgosz Mirosław, Marzena Małyszko, „A Method for Early Identification of Vessels Potentially Threatening Critical Maritime Infrastructure" *Applied Sciences*, nr 15 (2025), art. 8716.

Zhao Yunfeng, Jincheng Gong, Huanhuan Li, Trung Thanh Nguyen, Christian Matthews, Zaili Yang, „Cybersecurity in Smart Port Systems: A Systematic Review and Data-Driven Research Agenda" *Transport Policy*, 187 (2026), art. 104268.

This article is published under a Creative Commons Attribution 4.0 International license.
For guidelines on the permitted uses refer to
https://creativecommons.org/licenses/by/4.0/legalcode