

Revista Sextante

ISSN : 2665-3923

Vol: 33 No: 01 (2025)

Maritime Domain Awareness and the Protection of Critical Coastal Infrastructure

Samuel Kiprono-Henriksen

Institute for Coastal Infrastructure Security and Resilience, Mombasa, Kenya

Article History

Received Dec, 11th , 2025

Accepted Dec, 12th , 2025

Published Dec, 13th, 2025



© 2025 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license

<https://creativecommons.org/licenses/by/4.0>

Abstract

Critical coastal infrastructure, including ports, energy installations, submarine cables, pipelines and naval facilities, underpins trade, energy supply, communications and national security, yet it is exposed to a wide range of deliberate, accidental and natural threats arising from the open and shared maritime environment. This article examines the relationship between maritime domain awareness and the protection of critical coastal infrastructure. Drawing on situation awareness theory, maritime security studies, infrastructure interdependency research and work on anomaly detection and resilience, it analyses the infrastructure at stake, the threat landscape, sensors and data fusion, analytics for early warning, interagency coordination, legal frameworks and resilience. The analysis indicates that protection is strongest when awareness is integrated across agencies and operators, supported by diverse sensors and analytics, anchored in clear legal and policy arrangements and complemented by resilience planning. Limitations include uneven coverage, institutional barriers, false alarms and limited evidence of effectiveness. An illustrative figure summarises expected protection outcomes under isolated and integrated approaches.

Keywords: maritime domain awareness, critical infrastructure, coastal security, early warning, resilience

INTRODUCTION

Coastal zones concentrate a large share of the world's population, economic activity and strategic assets. Ports, terminals, offshore platforms, submarine cables, pipelines, coastal power stations, desalination plants, naval bases and communication nodes form a network of infrastructure on which trade, energy supply, data flows and national defence depend. The disruption of such assets, whether by deliberate attack, accident, natural hazard or cyber intrusion, can have consequences far beyond the immediate site, affecting supply chains, public services and security (Rinaldi et al., 2001). Protecting this infrastructure is difficult because the maritime approaches to it are open, extensive and shared by many users. Vessels of all kinds move through coastal waters, and the boundary between lawful and hostile activity is

often unclear until an incident occurs. Effective protection depends on knowing what is happening in the surrounding maritime space with enough detail and timeliness to anticipate, deter and respond. This capability is commonly described as maritime domain awareness, and it has become a central concept in maritime security policy (Bueger, 2015). This article examines the relationship between maritime domain awareness and the protection of critical coastal infrastructure. It reviews the conceptual foundations of awareness, the infrastructure at stake and the threats it faces, the sensors, data systems and analytics that provide awareness, and the organisational, legal and resilience dimensions of protection. It also considers limitations and future directions. The analysis is conceptual and integrative, and the figure presented is an illustrative synthesis rather than a report of new empirical data.

Conceptual Foundations of Maritime Domain Awareness:

Maritime domain awareness is usually defined as the effective understanding of anything associated with the maritime domain that could affect security, safety, the economy or the environment. It is not merely a matter of collecting data but of producing understanding that supports decisions. This links the concept to the theory of situation awareness, which describes three levels, namely the perception of relevant elements in the environment, the comprehension of their meaning, and the projection of their status into the near future (Endsley, 1995). Maritime domain awareness at an organisational level aims to achieve these levels across many actors and large areas. The concept has evolved with the broadening of maritime security. Analysts note that maritime security links safety, economic development, human security and seapower, and that it requires collaboration among agencies that traditionally worked separately (Bueger, 2015). Awareness is therefore inherently multi-agency and multi-purpose, supporting naval operations, coast guard enforcement, port management, environmental protection and disaster response with a shared picture of the maritime environment. A narrow focus on military threats would neglect many risks to coastal infrastructure. The idea of seablindness, the tendency of governments and publics to overlook the importance of the sea and the activities that take place there, helps to explain why awareness has often been inadequate. A research agenda on this theme argues that maritime issues deserve greater attention because of their central role in global society (Bueger & Edmunds, 2017). For infrastructure protection, overcoming seablindness means recognising that assets that are physically at the edge of national territory, or beneath the sea, are nonetheless integral to economic and national security.

Critical Coastal Infrastructure and Its Strategic Importance:

Critical infrastructure is commonly defined as the assets, systems and networks whose incapacity or destruction would have a debilitating effect on security, the economy, public health or safety. In coastal areas, it includes ports and container terminals, which handle the bulk of international trade, energy infrastructure such as oil and gas terminals, liquefied natural gas facilities, offshore wind farms and platforms, coastal power plants, and water facilities such as desalination plants. It also includes naval and coast guard bases, shipyards, navigational aids and communication facilities. Submarine cables and pipelines form a special category. Submarine cables carry most intercontinental data traffic, and pipelines transport energy across seas, yet these assets are largely invisible to the public and difficult to monitor. Research on the security politics of the global submarine cable network shows that this hidden infrastructure has become a focus of strategic concern, because its protection is complicated by diffuse ownership, limited redundancy at some landing points and uncertain legal responsibilities (Bueger & Liebetrau, 2021). The importance of these assets lies not only in their individual value but in their interdependence. Infrastructure systems depend on each other, so that disruption in one can cascade into others, for instance when an attack on a port affects fuel supply, power generation and transport networks simultaneously (Rinaldi et al., 2001). Understanding such interdependencies is a prerequisite for effective protection, as it reveals which nodes are most critical and where awareness should be concentrated. It also underlines the need for cooperation between operators, who may hold different pieces of information.

Threat Landscape and Vulnerabilities:

Critical coastal infrastructure faces a wide range of threats. Deliberate threats include terrorism, sabotage, piracy and armed attack, the use of small boats, swimmers or unmanned vehicles to approach facilities, mining and blocking of channels, smuggling and the infiltration of persons or materials. State-sponsored actors may conduct hybrid operations, including covert damage to underwater infrastructure, interference with navigation signals or ambiguous harassment designed to avoid attribution. Criminal activities such as theft and trafficking can also exploit port vulnerabilities and undermine security. Cyber threats are increasingly important. Port operations, vessel traffic management, energy control systems and logistics networks all rely on digital technology, which creates vulnerabilities to ransomware, data manipulation and intrusion. Policy research on maritime cybersecurity indicates that evolving technology has broadened the attack surface in shipping and that regulatory and organisational responses are still developing (Tam & Jones, 2019). A cyber incident may be difficult to distinguish from a technical fault, and its effects may spread quickly across interconnected systems. Accidents and natural hazards are equally significant. Ship collisions with terminals and offshore structures, groundings, fires, explosions and chemical releases can cause severe damage, and storm surges, tsunamis, sea-level rise and extreme weather threaten coastal installations. Complex, tightly coupled systems are prone to failures that arise from unexpected interactions among components, which means that accidents may be an inherent

feature of such systems rather than the result of simple human error (Perrow, 1984). Domain awareness should therefore address safety and environmental risk as well as security threats.

Sensor Networks, Data Fusion and Information Systems:

Maritime domain awareness is built from many data sources. Coastal radar and electro-optical systems monitor approaches to ports and installations, automatic identification system receivers provide the identity and movement of cooperative vessels, satellite imagery and radar offer wide-area coverage, and acoustic sensors, hydrophone arrays and sonar monitor activity under the water. Unmanned aerial and underwater vehicles can extend coverage and inspect infrastructure, while environmental sensors measure weather, sea state and water quality. Each source has limits in range, reliability and vulnerability to deception. The central task is to integrate these sources into a coherent picture. Data fusion combines observations from different sensors and databases to identify and track objects, resolve inconsistencies, estimate uncertainty and support the comprehension of events. Information systems provide common operating pictures accessible to different agencies, with access controls appropriate to the sensitivity of data. Standards for data formats, communication protocols and metadata are essential if systems from different agencies and suppliers are to work together. Design of these systems should respond to the specific needs of infrastructure protection. Coverage must be concentrated around high-value assets and their approaches, including submarine corridors, while still maintaining wider awareness of traffic patterns. Redundancy and diversity of sensors reduce the risk that a single failure or deception will blind operators, and the systems themselves must be hardened against cyber attack. Persistent coverage of remote or underwater assets may require autonomous platforms and fixed sensor networks, with attention to cost, maintenance and data management.

Analytics, Anomaly Detection and Early Warning:

Raw data do not by themselves provide awareness, and analytics are required to convert them into warning. Machine learning and statistical methods are used to model normal patterns of maritime traffic and to detect deviations that may signal threat or distress. Research has demonstrated how large archives of vessel movements can be used to learn typical routes and behaviour, enabling the detection of anomalies and the prediction of vessel paths (Pallotta et al., 2013). Such models can highlight, for example, a vessel loitering near a cable landing or approaching an offshore platform in an unusual manner. A review of maritime anomaly detection describes the variety of techniques available, from rule-based and statistical approaches to machine learning, and stresses the importance of context, of integrating human knowledge and of managing the trade-off between detection and false alarms (Riveiro et al., 2018). In infrastructure protection, geofencing and alerting around critical assets, combined with behavioural analysis and risk-based prioritisation, allow limited response resources to be focused where they are most needed. Predictive analytics may also support planning by identifying patterns of vulnerability or recurring activity. Early warning is the purpose of these tools, and its value depends on time. A warning that arrives after the event offers little benefit, whereas one that arrives with sufficient lead time allows interception, evacuation, closure of channels or activation of protective measures. Analytics should therefore be judged by their contribution to decisions in operational conditions, including the reliability of alerts, the clarity of presentation and the ability of operators to understand why an alert was generated. Analysts must remain part of the loop, interpreting results and bringing contextual intelligence that algorithms lack.

Interagency Coordination and Information Sharing:

The protection of coastal infrastructure involves many organisations, including navies, coast guards, port authorities, customs and border agencies, police, environmental and transport regulators, infrastructure owners and operators, and, in some cases, international partners. Each holds part of the information needed for awareness, and each has different mandates, cultures and legal constraints. Fragmentation of responsibility is one of the most common reasons for gaps in awareness, because information held by one agency may not reach another that could use it. Coordination mechanisms include joint operations or fusion centres where representatives of different agencies work together, shared information platforms, memoranda of understanding, common procedures for incident reporting and joint exercises. Trust is a precondition for sharing, and it is built through repeated cooperation, clear rules on the use and protection of information, and demonstrated benefit to all participants. Private operators of ports and energy facilities, who own much critical infrastructure, must be included, requiring arrangements that protect commercial confidentiality while enabling timely exchange of security-relevant information.

Legal and Policy Frameworks for Infrastructure Protection:

Protecting coastal infrastructure takes place within a legal framework that defines what states may do and where. The law of the sea establishes zones of jurisdiction, including internal waters, the territorial sea, the contiguous zone and the exclusive economic zone, and grants coastal states differing rights and duties in each (United Nations, 1982). Within territorial waters a state has wide authority to regulate and control activity, but in the exclusive economic zone and on the high seas its powers are more limited, which complicates the monitoring and protection of offshore installations and submarine cables. Submarine cables and pipelines illustrate the difficulties. The law provides for freedom to lay cables and pipelines and obliges states to take measures against their wilful or negligent damage, but enforcement is hard

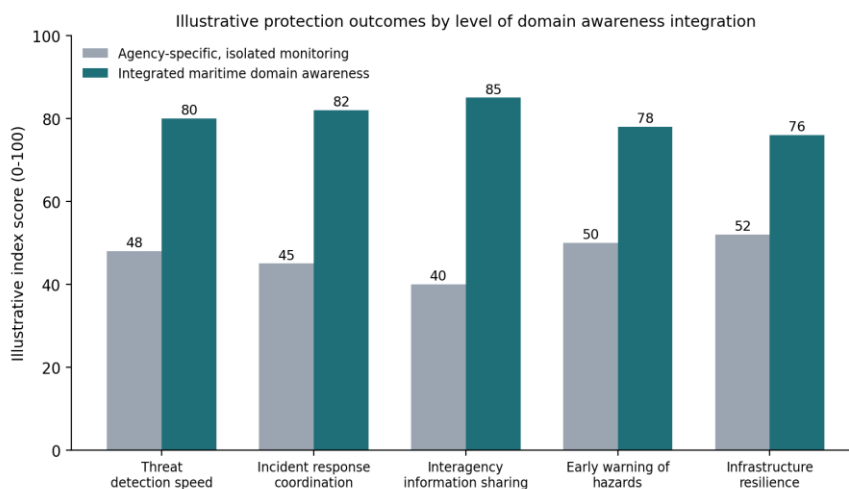
when incidents occur far from shore and attribution is uncertain. Domestic law governs the security of ports and facilities, including requirements for assessments, security plans, access control and reporting, and international standards on ship and port facility security provide a common baseline. Gaps and inconsistencies among jurisdictions can nonetheless be exploited. Policy frameworks must also address data and privacy. Surveillance of vessels and coastal areas generates large amounts of data, and its collection, retention and sharing must comply with national law and with respect for rights. Clear policies on data governance, accountability and oversight help to maintain public trust and reduce legal risk. National strategies for critical infrastructure protection, maritime security and cybersecurity should be aligned, assign responsibilities clearly and be supported by resources and regular review.

Resilience, Response and Recovery:

Awareness and protection cannot eliminate all risk, so resilience is an essential complement. Resilience is the ability of a system to prepare for, absorb, recover from and adapt to adverse events. Researchers have argued that managing risk alone is insufficient for complex systems, and that planning should focus on the capacity to withstand and recover from disruption, including through redundancy, flexibility and rapid restoration (Linkov et al., 2014). For coastal infrastructure this means designing facilities, networks and procedures that can continue to function in degraded conditions. Response capability depends on the speed and coordination of action once a warning or incident occurs. Plans should define roles and authorities, specify triggers for protective measures such as vessel exclusion, channel closure or evacuation, and ensure that resources such as patrol craft, firefighting vessels, divers, salvage and pollution response are available. Domain awareness supports response by providing real-time information on the location and movement of vessels and hazards, and by allowing commanders to track the effects of their actions. Recovery and learning complete the cycle. Restoration of port operations, energy supply and data connectivity may require alternative routes, spare equipment and agreements with partners. After incidents, structured reviews should identify lessons and update procedures, since complex systems are likely to experience unexpected failures. Exercises and simulations that involve all relevant agencies and private operators test plans, build relationships and reveal weaknesses before real events occur, and are among the most effective means of improving preparedness.

Challenges, Limitations and Future Directions:

Several challenges limit the effectiveness of maritime domain awareness for infrastructure protection. Coverage is uneven, particularly for remote, underwater and open-ocean areas, and sensors can be degraded by weather, clutter and deliberate deception. Data volumes can overwhelm analysts, and false alarms may erode confidence in alerts. Institutional barriers, including turf rivalry, classification rules, incompatible systems and legal restrictions, impede sharing. Funding is often directed toward visible hardware rather than to integration, training and maintenance, which are equally vital. Conceptual and evidential limitations also exist. Awareness is a means rather than an end, and there is a risk that investments in surveillance are justified by their technical impressiveness rather than their contribution to protection. Evidence on the effectiveness of awareness initiatives in preventing or mitigating incidents is limited, and counterfactual evidence of deterrence is hard to obtain. Over-reliance on technology may foster complacency, and adversaries will adapt to evade detection. Programmes should therefore be evaluated critically and designed to accommodate change. Future directions include broader fusion of commercial, governmental and open-source data, greater use of artificial intelligence for analysis and prediction, deployment of persistent autonomous sensors for seabed and offshore monitoring, and the use of digital twins to model infrastructure and test responses. Strengthening international cooperation, especially for transboundary infrastructure such as cables and pipelines, will be essential, as will inclusion of private operators in security arrangements. Research should concentrate on measuring the effectiveness of awareness, understanding interdependencies and developing governance models that balance security, commerce and rights.



Summary:

Maritime domain awareness is a foundation for protecting critical coastal infrastructure. By integrating data from radar, identification systems, satellites, acoustic sensors and autonomous platforms, applying analytics to detect anomalies and provide early warning, and sharing information among navies, coast guards, port authorities and infrastructure operators, awareness allows threats and hazards to be anticipated, deterred and managed. The protection of ports, energy facilities and submarine cables is particularly dependent on understanding interdependencies and on cooperation across public and private actors. Awareness alone is not sufficient. Effective protection also requires clear legal and policy frameworks, secure and resilient information systems, response plans and exercises, and the ability to recover quickly from disruption. Limitations include uneven coverage, institutional fragmentation, false alarms, vulnerability to deception and limited evidence of effectiveness. Future work should develop integrated and secure data fusion, measure the contribution of awareness to protection, strengthen international cooperation for transboundary assets and design governance that balances security, commercial interests and rights.

References:

- Bueger, C. (2015). What is maritime security? *Marine Policy*, 53, 159–164.
- Bueger, C., & Edmunds, T. (2017). Beyond seablindness: A new agenda for maritime security studies. *International Affairs*, 93(6), 1293–1311.
- Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, 42(3), 391–413.
- Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), 32–64.
- Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., et al. (2014). Changing the resilience paradigm. *Nature Climate Change*, 4, 407–409.
- Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. *Entropy*, 15(6), 2218–2245.
- Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.
- Riveiro, M., Pallotta, G., & Vespe, M. (2018). Maritime anomaly detection: A review. *WIREs Data Mining and Knowledge Discovery*, 8(5), e1266.
- Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25.
- Tam, K., & Jones, K. (2019). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, 4(1), 25–60.
- Till, G. (2013). *Seapower: A guide for the twenty-first century* (3rd ed.). Routledge.
- United Nations. (1982). *United Nations Convention on the Law of the Sea*. United Nations.