

Revista Sextante

ISSN : 2665-3923

Vol: 30 No: 01 (2024)

Strategic Intelligence and Information-Sharing Mechanisms in Maritime Threat Prevention

Oluwaseun T. Adeyemi

Department of Maritime Intelligence and Security Studies, Gulf of Guinea Institute for Maritime Security Research, Lagos, Nigeria

Article History

Received June, 06th , 2024

Accepted June, 07th , 2024

Published June, 08th, 2024



© 2024 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

Preventing maritime threats depends on knowing what is happening at sea, who is involved, and what is likely to happen next. This article examines the role of strategic intelligence and information sharing mechanisms in the prevention of maritime threats such as piracy, trafficking, terrorism, illegal fishing, and hostile naval activity. It reviews the conceptual foundations of maritime intelligence, adapts the intelligence cycle to the maritime domain, and surveys the sources of information available at sea and ashore. It then analyses how fusion and analysis produce maritime domain awareness, how states and organisations structure information sharing, and which legal, political, and trust related barriers constrain cooperation. The article also considers experience from regional arrangements and the technical and governance challenges of handling shared data securely. Drawing on intelligence studies, security cooperation scholarship, and maritime surveillance research, the analysis finds that prevention improves when intelligence is timely, analytically rigorous, and shared through trusted channels, but that sovereignty concerns, classification rules, technical incompatibility, and cognitive bias limit performance. The article concludes with recommendations for building interoperable, trusted, and well governed information sharing systems that support early action at sea.

Keywords: maritime intelligence, information sharing, threat prevention, maritime domain awareness, security cooperation

INTRODUCTION

The maritime domain is vast, lightly policed, and characterised by enormous volumes of legitimate activity in which illicit behaviour can hide. Cargo ships, tankers, fishing vessels, ferries, and pleasure craft move continuously across oceans, and only a tiny fraction of them pose any threat. Finding that fraction in time to act is the central challenge of

maritime threat prevention. Patrol vessels and aircraft are scarce and cannot be everywhere, so their effective use depends on intelligence that tells them where to look and what to look for. Intelligence is more than raw information. Lowenthal defines it as information that has been collected, processed, and analysed to meet the needs of decision makers, and he stresses that its purpose is to reduce uncertainty and support policy and action (Lowenthal, 2017). In the maritime context, strategic intelligence addresses questions about patterns, intentions, networks, and vulnerabilities over longer horizons, while operational and tactical intelligence supports specific missions and encounters. No single state or agency possesses all the information needed. Vessels cross jurisdictions, networks span regions, and relevant data are held by navies, coast guards, customs services, port authorities, shipping companies, insurers, and international organisations. Prevention therefore depends on sharing. Walsh argues that states cooperate on intelligence when they face common threats and can build mechanisms that reduce the risk of exploitation or betrayal, but that sharing is always constrained by concerns about sources, methods, and relative advantage (Walsh, 2010). This article examines how strategic intelligence and information sharing contribute to maritime threat prevention. It proceeds through nine thematic sections covering conceptual foundations, the intelligence cycle, sources and collection, analysis and fusion, sharing architectures, barriers, regional experience, technology and data governance, and recommendations. A summary and a list of references follow.

Conceptual Foundations of Maritime Intelligence:

Maritime intelligence encompasses the knowledge needed to understand the maritime environment and the actors within it. It includes information about vessels and their ownership, crews, cargoes, routes, and behaviour; about ports and infrastructure; about criminal and terrorist networks that use the sea; about the capabilities and intentions of foreign naval and paramilitary forces; and about environmental and economic conditions that shape maritime activity. It is useful to distinguish levels. Tactical intelligence supports immediate operations, such as the identification of a suspect vessel or the location of a smuggling rendezvous. Operational intelligence supports campaigns and patrol planning, for example by identifying hotspots and seasonal patterns. Strategic intelligence addresses structural questions, such as how a criminal network is financed, how a rival state's maritime posture is evolving, or where regional vulnerabilities lie. Prevention relies heavily on the strategic level, because it aims to stop threats before they materialise rather than merely to respond. Bueger describes maritime security as a field linking national security, marine safety, the blue economy, and resilience, which implies that the relevant information is held by many communities with different purposes (Bueger, 2015). Maritime intelligence therefore draws on both classified sources and open and commercial information. The traditional separation between military intelligence and civil law enforcement information is increasingly blurred, which raises organisational and legal questions. Betts argued, in his study of surprise attack, that failures of intelligence often arise not from lack of information but from organisational and psychological obstacles to interpreting and acting on it (Betts, 1982). This insight frames the whole discussion. Effective maritime intelligence requires not only collection but also sound analysis, timely dissemination, and decision makers willing to act on warning.

The Intelligence Cycle in the Maritime Domain:

The intelligence cycle is the standard model of how intelligence is produced. It begins with direction, in which decision makers state their requirements. Collection follows, in which sources and sensors are tasked. Processing converts raw data into usable form. Analysis interprets the material, and dissemination delivers products to users. Feedback from users then refines future requirements. Lowenthal notes that the cycle is a simplification, since in practice the steps overlap and interact, but it remains a helpful framework (Lowenthal, 2017). Applied to the maritime domain, direction must reflect the diversity of users, from naval commanders to coast guard patrol leaders, customs officers, and policymakers. Requirements may include identifying vessels of interest, mapping smuggling routes, understanding the structure of fishing fleets, or assessing the intentions of a foreign navy. Clear priorities are essential, because the volume of maritime data is large and attention is limited. Collection in the maritime domain is complicated by geography and the mobility of targets. Vessels may change names, flags, and transponder behaviour, and they may operate in areas far from coastal sensors. Processing involves cleaning and correlating data from many sources, including vessel registries, port records, and sensor tracks, which may be inconsistent or incomplete. Analysts must connect fragments of information to form a picture of activity and intent. Dissemination is particularly important for prevention, because information has value only if it reaches those who can act in time. A warning that arrives after a vessel has left a patrol area is of little use. Maritime intelligence therefore needs fast, reliable channels, appropriate formats, and the right level of classification so that operational users can receive it. Feedback is equally vital, since patrol results and interdiction outcomes reveal which intelligence was accurate and which was not.

Sources and Collection Disciplines at Sea:

Maritime intelligence draws on several collection disciplines. Human sources provide insight into networks, plans, and local conditions, and they may include informants, port workers, fishermen, seafarers, and officials. Signals intelligence, where lawful, can reveal communications and electronic emissions. Imagery from satellites, aircraft, and

drones shows vessel positions, ports, and activities. Open source information includes news, social media, shipping databases, and academic and industry reports. A distinctive source in the maritime domain is the data generated by commercial shipping itself. The automatic identification system broadcasts vessel identity, position, course, and speed, and is received by shore stations and satellites worldwide. Kazemi and colleagues showed that open data, including vessel tracking and other public information, can be used to detect anomalies in maritime surveillance, offering a low cost way to enhance awareness (Kazemi et al., 2013). Port state control records, cargo manifests, crew lists, and insurance information add further layers. Each source has limitations. Human sources may be unreliable or compromised. Technical sources can be evaded, as when vessels switch off transponders or falsify data. Open information may be inaccurate or deliberately misleading. Imagery may be unavailable when and where it is needed. Corroboration across independent sources is therefore the best protection against error and deception. Percy and Shortland's study of piracy in Somalia illustrates the importance of understanding networks rather than only incidents. They showed how financiers, local facilitators, and onshore support systems sustained piracy, which meant that information about these elements was as valuable as tracking of skiffs at sea (Percy and Shortland, 2013). This lesson applies to other threats as well, since the vessels at sea are often the visible end of a much larger system.

Analysis, Fusion, and Maritime Domain Awareness:

Analysis transforms information into insight. In the maritime domain, analysts examine patterns of life, such as normal routes and behaviours of fishing fleets, ferries, and merchant shipping, so that deviations stand out. Anomaly detection techniques use algorithms to flag unusual movements, such as loitering in remote areas, sudden course changes, unexplained rendezvous, or gaps in tracking data. Riveiro, Pallotta, and Vespe reviewed maritime anomaly detection and noted that methods range from statistical models to machine learning, and that their value depends on data quality, the definition of normality, and the integration of human judgement (Riveiro et al., 2018). Fusion combines information from different sources and agencies into a coherent picture. A fused picture might link a vessel's track with its ownership history, previous port calls, crew details, and intelligence about associated networks. This integration reveals connections that individual sources cannot. The resulting maritime domain awareness, meaning an effective understanding of everything in the maritime domain that could affect security, safety, or the economy, underpins prevention. Human analysis remains indispensable. Heuer's study of the psychology of intelligence analysis showed that analysts are subject to biases such as confirmation bias, anchoring, and mirror imaging, and that structured analytic techniques, such as testing competing hypotheses and challenging assumptions, can reduce their effect (Heuer, 1999). Wohlstetter's classic study of the Pearl Harbor warning illustrated how signals can be present but lost among noise, so that clear patterns appear only in hindsight (Wohlstetter, 1962). These lessons are directly relevant to maritime surveillance, where noise is extensive. Good analysis also communicates uncertainty. Products should state the confidence level, the basis of judgements, and alternative explanations, so that decision makers can weigh them appropriately. Warning intelligence, designed to alert leaders to emerging threats, should be distinguished from current reporting and given priority for rapid dissemination. Establishing analytic standards and training across agencies helps ensure that shared products are credible and comparable.

Information-Sharing Architectures and Mechanisms:

Information sharing can be organised in several ways. Bilateral arrangements link two states or agencies through agreements that specify what is shared, how, and for what purposes. They allow tailored protection of sensitive material but do not scale easily. Multilateral arrangements connect many participants through common centres or networks, which broaden coverage but require agreed rules and trust among all members. Hybrid models combine a central hub with bilateral channels for more sensitive exchanges. Fusion centres and information sharing centres are a common architectural feature. These are facilities where liaison officers from several agencies or countries work together to collect, analyse, and disseminate maritime information. Their advantages include speed, personal relationships, and the ability to clarify ambiguities in real time. Till observes that modern sea power is exercised in a context of good order at sea that requires cooperation among navies, coast guards, and civil agencies, and shared centres provide a practical mechanism for such cooperation (Till, 2018). Sharing mechanisms also differ in the type of information exchanged. Some centres focus on unclassified data such as vessel positions and incident reports, which can be shared widely, including with shipping companies and other civil partners. Others handle classified assessments among a limited circle of partners. Tiered models allow different levels of access, so that a broad community receives general awareness while a narrower group exchanges sensitive intelligence. Standards and procedures make sharing work. Common data formats, shared vocabularies, agreed reporting templates, and protocols for handling and protecting information reduce friction. Clear rules about who may use the information, for what purpose, and whether it may be passed to third parties help preserve trust. Regular exercises, joint training, and liaison exchanges give participants practice in using the mechanisms before a crisis tests them.

Legal, Political, and Trust Barriers to Sharing:

Despite the evident benefits, sharing is hard. Lefebvre examined the difficulties and dilemmas of international intelligence cooperation and noted that states fear compromising sources and methods, worry that partners may leak or misuse information, and are reluctant to reveal what they do and do not know (Lefebvre, 2003). Intelligence services are also culturally inclined to protect information, and bureaucratic habits of secrecy persist even where formal agreements exist. Walsh argues that states are more willing to share when they can verify that partners comply with agreed rules and when the costs of defection are high, which suggests that institutional design, including monitoring and reciprocity, matters for durable cooperation (Walsh, 2010). Where partners are unequal in capability, the stronger may fear giving away advantage while the weaker may fear dependence or surveillance. Legal constraints add complexity. National laws regulate the collection and transfer of personal data, the use of intelligence as evidence in court, and the sharing of classified material. Differences in legal systems may prevent information gathered by one agency from being used by another, and rules on privacy and data protection can restrict cross border exchange. Military and civilian agencies may operate under different authorities, further complicating domestic sharing. Political relationships and sovereignty sensitivities also matter. Neighbouring states with disputes may hesitate to share information that could affect their claims. Concerns that shared surveillance data could reveal weaknesses or be used for coercion can deter participation. Capacity gaps limit participation by states with limited technical means. The figure below presents an illustrative comparison of the relative severity of common barriers to maritime information sharing, as discussed in the literature, expressed on a standardised index from zero to one hundred. The values are stylised to show relative magnitude and should not be read as measured data.

Experience in Regional Information Sharing:

Regional experience offers practical lessons. In Southeast Asia, littoral states and user states developed cooperative arrangements to improve safety and security in the busy straits linking the Indian and Pacific Oceans. Bateman, Raymond, and Ho emphasised that such cooperation depended on respect for the sovereignty of coastal states and on practical measures such as information exchange and coordinated patrols, rather than on any supranational authority (Bateman et al., 2006). Information sharing arrangements built around reporting and liaison have supported trust among participants. In the Western Indian Ocean, the response to piracy involved navies from many countries, regional states, and international organisations. Percy and Shortland's analysis of the piracy business showed that the effectiveness of response depended on understanding the networks behind the attacks, which required intelligence from multiple sources and cooperation between military, law enforcement, and financial authorities (Percy and Shortland, 2013). Regional information centres and coordination mechanisms helped deconflict patrol areas and share incident data with the shipping industry, which in turn adjusted its protective measures. In West Africa, regional frameworks have sought to link coastal states in sharing information on piracy, trafficking, and illegal fishing, with support from international partners. Challenges include uneven capacity, limited sensor coverage, and the difficulty of translating shared data into patrol action. Experience suggests that sharing is most effective when it is connected to operational capability, such as interdiction assets and prosecution mechanisms, so that information leads to consequences. Across regions, several common features appear. Successful mechanisms usually start with unclassified information that is easy to share and gradually build trust before moving to more sensitive exchange. They depend on personal relationships among liaison officers. They benefit from neutral hosting or shared governance, and they connect to the commercial shipping community, which is both a source and a user of information. Where mechanisms exist only on paper, without staff, resources, and political backing, they do not influence behaviour.

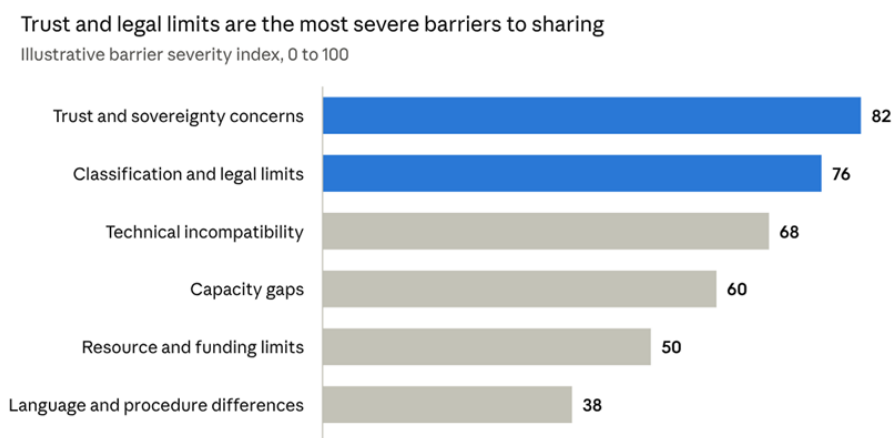
Technology, Data Governance, and Security of Shared Information:

Technology enables sharing on a scale unimaginable a generation ago. Secure networks, web based platforms, and standardised data exchange formats allow many participants to contribute and access information quickly. Cloud services offer storage and analytical tools, while automated alerts can notify partners when a vessel of interest approaches their waters. Analytical tools, including those that detect anomalies, help to filter large volumes of data and focus human attention, as Riveiro and colleagues describe (Riveiro et al., 2018). Technology also brings challenges. Heterogeneous systems with different data models complicate integration, and legacy systems may not interoperate. Data quality varies, and errors can propagate when shared. Overreliance on automated indicators may generate false alarms or encourage complacency. Kazemi and colleagues noted that the usefulness of open data for surveillance depends on understanding its limitations and combining it with other sources (Kazemi et al., 2013). Data governance is essential. Participants need clear policies on ownership, access, retention, correction, and deletion of data, as well as accountability for misuse. Provenance information, which records where data came from and how reliable it is, helps users judge its value. Privacy and human rights protections must be respected, particularly where data concern individuals such as crew members and migrants. Security of shared systems is itself a concern. Networks that connect many participants create attack surfaces, and a breach at one partner could expose the information of all. Strong authentication, encryption, segmentation, and monitoring are needed, together with agreed incident response

procedures. Trust in the security of the system is a precondition for willingness to share, which means that technical protection and cooperation reinforce each other.

Recommendations and Future Directions:

Several recommendations follow from the analysis. First, states and organisations should clarify requirements, identifying the decisions that intelligence is meant to support and the information that is needed. Without clear priorities, collection and sharing may be extensive but unfocused. Second, they should invest in analysis as well as collection, including training in structured techniques to counter the biases that Heuer and Betts describe (Heuer, 1999; Betts, 1982). Third, they should build tiered, interoperable sharing architectures that start with unclassified information and expand as trust grows, using common standards and liaison based fusion centres. Fourth, they should address legal and policy barriers through agreements that define purposes, protections, and handling rules, and through national reforms that enable appropriate domestic sharing among military and civil agencies. Fifth, they should connect information sharing to action, ensuring that warnings reach operational forces and that interdiction, prosecution, and regulatory responses are available. Sixth, they should engage the commercial maritime community, whose vessels, ports, and companies generate and use much of the relevant data. Seventh, they should embed strong data governance and cybersecurity so that participants can trust the system. Bueger's observation that maritime security spans many actors and purposes supports a broad, inclusive approach to partnership (Bueger, 2015). Looking ahead, advances in satellite constellations, artificial intelligence, and sensors will increase the volume and speed of maritime information, while adversaries will adapt by concealing and spoofing signals. Research should evaluate the effect of sharing mechanisms on actual threat prevention, develop methods for measuring trust, and examine how cooperation can be sustained under political strain. The central insight is that intelligence prevents threats only when it is shared in time, with the right people, and with the confide



Summary:

This article has examined strategic intelligence and information sharing mechanisms in maritime threat prevention. Maritime intelligence draws on human, technical, and open sources, and its production follows a cycle of direction, collection, processing, analysis, and dissemination adapted to the mobility and scale of the sea. Fusion and analysis create maritime domain awareness, but analytic biases and noise can obscure warning. Information sharing through bilateral, multilateral, and tiered arrangements multiplies the reach of national efforts, yet it is constrained by concerns about sources and methods, legal and political barriers, capacity gaps, and technical incompatibility. Regional experience shows that trust grows through practical cooperation, liaison relationships, and a link between information and operational action. Strong data governance, security, and analytic standards are essential. States and organisations that invest in rigorous analysis, interoperable and trusted sharing mechanisms, and the capacity to act on warning are best positioned to prevent maritime threats before they materialise.

References:

- Bateman, S., Raymond, C. Z., and Ho, J. (2006). *Safety and Security in the Malacca and Singapore Straits: An Agenda for Action*. Singapore: Institute of Defence and Strategic Studies.
- Betts, R. K. (1982). *Surprise Attack: Lessons for Defense Planning*. Washington, DC: Brookings Institution Press.
- Bueger, C. (2015). What is maritime security? *Marine Policy*, 53, 159–164.

- Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency.
- Kazemi, S., Abghari, S., Lavesson, N., Johnson, H., and Ryman, P. (2013). Open data for anomaly detection in maritime surveillance. *Expert Systems with Applications*, 40(14), 5719–5729.
- Lefebvre, S. (2003). The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and CounterIntelligence*, 16(4), 527–542.
- Lowenthal, M. M. (2017). *Intelligence: From Secrets to Policy* (7th ed.). Thousand Oaks: CQ Press.
- Percy, S., and Shortland, A. (2013). The business of piracy in Somalia. *Journal of Strategic Studies*, 36(4), 541–578.
- Riveiro, M., Pallotta, G., and Vespe, M. (2018). Maritime anomaly detection: A review. *WIREs Data Mining and Knowledge Discovery*, 8(5), e1266.
- Till, G. (2018). *Seapower: A Guide for the Twenty-First Century* (4th ed.). London: Routledge.
- Walsh, J. I. (2010). *The International Politics of Intelligence Sharing*. New York: Columbia University Press.
- Wohlstetter, R. (1962). *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.