

Revista Sextante

ISSN : 2665-3923

Vol: 34 No: 01 (2026)

Cyber Threat Intelligence and National Security: Emerging Challenges for Maritime States

Rafael Castellanos-Nakamura

Centre for Maritime Security and Cyber Policy Studies Atlantic Institute of Strategic Affairs, Lisbon, Portugal

Article History

Received June, 11th, 2026

Accepted June, 12th, 2026

Published June, 13th, 2026



© 2026 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

Maritime states depend on the sea for trade, energy, communication, food, and defense, and each of these functions is now mediated by digital systems that can be targeted by hostile actors. Cyber threat intelligence, the structured collection and analysis of information about adversary capabilities, intentions, and activities, has become a central instrument for protecting national security in this environment. This article presents an integrative conceptual review of the challenges that cyber threat intelligence poses and addresses for maritime states. It examines conceptual foundations, the maritime threat landscape, actors and attribution, intelligence collection and sharing, protection of ports and vessels, undersea cables and satellite and navigation systems, law and international cooperation, naval operations and deterrence, and capacity building. A conceptual graph compares estimated cyber exposure with defensive preparedness across maritime domains, suggesting that undersea infrastructure, navigation systems, offshore energy, and port operations show the widest gaps. The article concludes that maritime states need integrated, intelligence-driven, and cooperative approaches that connect civil and naval stakeholders, public and private owners, and national and allied institutions.

Keywords: cyber threat intelligence, national security, maritime states, critical infrastructure, cyber deterrence

INTRODUCTION

The maritime domain carries the great majority of global trade by volume, hosts critical energy and communication infrastructure, and provides the arena in which naval forces project power and protect national interests. Maritime states, those whose prosperity, security, and identity are closely tied to the sea, therefore have a particular stake in the integrity of maritime systems. Scholars of maritime security have argued that the sea has long been neglected in security analysis, a condition sometimes described as sea blindness, even though events at sea can have profound consequences for economies and societies (Bueger & Edmunds, 2017; Till, 2018). Over recent decades, maritime

activity has become deeply digital. Ports rely on terminal operating systems, automated cranes, and electronic customs processing. Ships depend on satellite navigation, electronic charts, integrated bridge systems, and remote monitoring. Offshore platforms, wind farms, and pipelines are managed through industrial control systems, and nearly all international data traffic crosses the seabed through fiber-optic cables. Naval forces rely on networked sensors, command systems, and satellite communications. This digitalization yields efficiency and awareness, but it also creates avenues for disruption, espionage, and coercion that do not respect geography or the traditional distinction between civil and military spheres (Tam & Jones, 2019). Cyber threat intelligence has emerged as a response. By collecting and analyzing information about adversary tools, infrastructure, tactics, and intentions, defenders can anticipate attacks, prioritize protection, and respond more effectively (Tounsi & Rais, 2018). Frameworks such as the intrusion kill chain and adversary behavior matrices have given analysts shared languages for describing threats (Hutchins, Cloppert, & Amin, 2011; Strom et al., 2018). However, the maritime context presents distinctive difficulties, including fragmented ownership, international operation, reliance on legacy and operational technology, and the political sensitivity of attribution and response. This article examines the role of cyber threat intelligence in national security for maritime states and the emerging challenges that shape its use. Drawing on literature from strategic studies, maritime security, cybersecurity, and international law, it proceeds through thematic sections that address conceptual foundations, the threat landscape, actors and attribution, intelligence processes, infrastructure protection, undersea and space-enabled systems, law and cooperation, naval operations and deterrence, and capacity building. A summary then draws together the main conclusions and recommendations for policymakers, naval planners, and industry.

Conceptual Foundations of Cyber Threat Intelligence and Maritime Security:

Cyber threat intelligence can be defined as evidence-based knowledge about existing or emerging threats to information systems, including context, mechanisms, indicators, implications, and actionable advice. It operates at several levels. Strategic intelligence informs senior decision makers about adversary intent and long-term trends; operational intelligence describes campaigns and the likely timing and form of attacks; tactical intelligence provides details about techniques and procedures; and technical intelligence supplies indicators such as malicious addresses and file signatures that can be used for detection. Tounsi and Rais (2018) emphasize that the value of intelligence depends on its relevance, timeliness, accuracy, and actionability, and that raw data alone does not constitute intelligence. National security in the maritime context involves protecting the state, its people, and its interests from threats arising at or from the sea. Till (2018) describes the sea as a resource, a means of transportation and exchange, a means of information, and a domain of power and dominion, and each of these roles is now exposed to cyber risk. Bueger and Edmunds (2017) call for a broad understanding of maritime security that includes safety, economic, environmental, and human dimensions alongside traditional naval concerns. Cyber threat intelligence therefore serves a wide community, from navies and coast guards to port authorities, shipping companies, and energy operators. Cyberspace has distinctive characteristics that complicate security thinking. Offensive operations can be conducted at low cost and from a distance, defenders must protect many points while attackers need find only one weakness, and the effects of an operation can be difficult to predict. Buchanan (2017) describes a cybersecurity dilemma in which defensive intrusions to gather intelligence may be perceived as offensive preparation, creating a risk of unintended escalation. Maritime states must therefore consider how their intelligence activities are interpreted by others, and how to maintain credibility and restraint while still acquiring the knowledge necessary to defend.

The Maritime Cyber Threat Landscape:

The maritime cyber threat landscape includes a wide variety of targets and effects. Ports may be disrupted through attacks on terminal systems, scheduling, and customs processing, causing delays that ripple through supply chains. Ships may suffer manipulation or loss of navigation and communication systems, disruption of cargo and propulsion control, or theft of commercial information. Offshore platforms and energy infrastructure may be affected through industrial control systems. Tam and Jones (2019) present a model-based framework for assessing maritime cyber risk, highlighting the interdependence of ship, port, and shore systems and the importance of considering both threat and consequence. Several features make the maritime sector especially vulnerable. Ships operate for decades, so legacy systems that were never designed with security in mind remain in service. Connectivity is often limited and expensive, which complicates patching and monitoring. Crews are small and may lack specialized cyber training. Equipment and software are supplied by many vendors, creating complex supply chains and potential points of compromise. Operational technology that controls physical processes tends to prioritize availability and safety over security, and it is increasingly connected to corporate networks and the internet for remote maintenance and efficiency. The consequences of attacks can extend well beyond the immediate victim. A major port outage affects manufacturers, retailers, and consumers far inland. Disruption of navigation data in congested waters could cause collisions or groundings with environmental and human costs. Attacks on energy infrastructure may affect national supply and prices. For naval forces, compromise of logistics and maintenance systems could degrade readiness without any visible attack. Maritime

cyber threats thus blend criminal, commercial, and strategic dimensions, and the line between them may be unclear at the moment an incident occurs.

Threat Actors, Motivations, and Attribution Challenges:

Threat actors in the maritime domain range from criminal groups seeking financial gain, through hacktivists pursuing political causes, to state-sponsored organizations pursuing espionage, pre-positioning, and coercion. Criminals have targeted shipping and logistics companies with ransomware and have exploited cargo systems to facilitate smuggling. State actors are interested in naval capabilities, shipbuilding and defense industry information, port data, and the possibility of holding critical infrastructure at risk in a crisis. The boundaries between these groups are fluid, since states may use criminal proxies or tolerate their activities, and techniques developed by states often spread to criminals. Attribution, the process of identifying who is responsible for an operation, is a perennial difficulty. Rid and Buchanan (2015) argue that attribution is not only a technical problem but a process involving technical, operational, and strategic analysis, in which the level of confidence required depends on the decision to be made. Forensic evidence can be ambiguous, adversaries may mimic one another or reuse tools, and intelligence sources that support confident attribution may be too sensitive to disclose. For maritime states, delays and uncertainty in attribution complicate responses, particularly when an incident could be a malfunction, a criminal act, or the opening move of a state campaign. Intentions are as important as capabilities, yet harder to determine. Lindsay (2013) shows through analysis of the Stuxnet operation that sophisticated operations demand extensive intelligence, resources, and tailored engineering, which limits their scalability but also demonstrates the potential of cyber means to affect physical systems. Maritime states should therefore avoid both complacency and alarmism, grounding their assessments in evidence about what adversaries have done and what they would need to do to achieve particular effects. Intelligence that links actors, motives, and observed behaviors enables more proportionate and credible defensive priorities.

Intelligence Collection, Analysis, and Sharing Frameworks:

Effective cyber threat intelligence follows a cycle of direction, collection, processing, analysis, dissemination, and feedback. Sources include network telemetry, malware analysis, open-source information, commercial feeds, information shared by partners, and intelligence from classified collection. Analysts use frameworks to structure what they learn. The intrusion kill chain of Hutchins, Cloppert, and Amin (2011) models the stages of an attack from reconnaissance to action on objectives, enabling defenders to disrupt campaigns at multiple points, while the adversary tactics and techniques knowledge base described by Strom and colleagues (2018) provides a common taxonomy of observed behaviors. Sharing is crucial, because no single organization sees the whole picture. In the maritime sector, information sharing and analysis centers, port community systems, and naval and coast guard networks can pool indicators and lessons learned. However, sharing is hindered by competition, concerns about liability and reputation, classification, and mistrust between governments and industry. Standardized formats and protocols for exchanging indicators can reduce friction, but trust relationships and clear rules about use and protection of shared information remain decisive. Maritime states should consider structures that allow intelligence to flow in both directions between government agencies and operators of critical infrastructure. Quality and relevance are persistent concerns. Large volumes of low-value indicators can overwhelm analysts and provide a false sense of security, whereas intelligence tailored to the maritime context, such as threats to particular classes of vessel systems or port technologies, is scarce. Automation and machine learning can assist in processing and correlation, but they require careful validation and can themselves be targeted by deception. Integration of cyber intelligence with other forms of maritime domain awareness, including surveillance of vessel movements and anomalies, offers the possibility of a more complete understanding of threats and their potential effects on operations.

Protection of Ports, Vessels, and Critical Maritime Infrastructure:

Protecting ports, vessels, and associated infrastructure requires a layered approach that combines governance, technology, and human factors. The International Maritime Organization (2017) adopted a resolution encouraging administrations to ensure that cyber risks are appropriately addressed in safety management systems, bringing cyber risk management into the established culture of maritime safety. This approach recognizes that cyber incidents can have safety consequences and that the shipping industry already has experience in managing risk through systematic processes, audits, and continuous improvement. Technical measures include network segmentation between operational and corporate systems, secure configuration, patch management where feasible, access control, monitoring, and backup and recovery capabilities. Cyber threat intelligence informs these measures by identifying which vulnerabilities are being actively exploited and which techniques are relevant to maritime systems, allowing scarce resources to be directed to the highest risks. Vendor management is also important, since compromised updates or remote maintenance channels can provide adversaries with access. Procurement requirements for security by design can improve the baseline of new equipment over time. Human and organizational factors are equally significant. Crew awareness training, clear procedures for responding to anomalies, and the ability to operate manually when automated systems fail are essential, particularly where navigation or propulsion is concerned. Exercises that simulate cyber incidents at ports

and on ships help organizations test response plans and relationships. Because many ports and shipping companies are privately owned, governments must find ways to encourage investment in security, through regulation, incentives, and support, without imposing burdens that are unrealistic for smaller operators. Resilience, the ability to continue essential functions and recover quickly, should be treated as an objective alongside prevention.

Undersea Cables, Satellite Links, and Navigation Systems:

Undersea cables carry the vast majority of international data traffic and are critical to finance, commerce, and government communications. They are vulnerable to physical damage, whether accidental or deliberate, and their landing stations and management systems are exposed to cyber compromise. Maritime states with significant cable landings must consider the protection of these assets in cooperation with owners, who are largely commercial. Intelligence about activities near cable routes, including unusual vessel behavior, supports early warning, and combined cyber and physical monitoring can strengthen protection. Diversity of routes and rapid repair capacity are important components of resilience. Satellite systems underpin maritime communications, positioning, navigation, timing, remote sensing, and vessel tracking. Satellite navigation signals are weak and can be jammed or spoofed, with documented incidents affecting ships in several regions. Disruption or manipulation of timing and position data can cascade into other systems that depend on them. Resilient approaches include use of multiple constellations, complementary terrestrial and inertial systems, receivers designed to detect anomalies, and crew training to recognize and respond to suspicious indications. Intelligence on interference activity helps inform guidance to mariners and the development of mitigation measures. These systems illustrate the interdependence of cyber, physical, and electromagnetic domains. Defending them requires cooperation among telecommunications, space, maritime, and defense agencies, which often have separate mandates and cultures. Maritime states should map dependencies, identify critical nodes, and develop contingency plans for degraded operation. Because many of the infrastructures concerned are transnational, unilateral measures are insufficient, and engagement with allies, industry, and international organizations is needed to establish norms and practices that reduce the risk of disruption.

Law, Policy, and International Cooperation:

International law applies to state conduct in cyberspace, but its application to specific maritime scenarios remains contested. Questions include when a cyber operation constitutes a use of force or armed attack, how sovereignty applies to systems and infrastructure, what due diligence obligations states have to prevent their territory from being used for harmful operations, and how the law of the sea, which governs freedom of navigation and the protection of cables, relates to cyber activity. Ambiguity may give states room for maneuver, but it also increases the risk of misinterpretation and escalation, which is particularly relevant at sea where military and civil vessels operate in proximity. National policy must align legal authorities, institutional responsibilities, and capabilities. Many maritime states divide responsibilities among naval, coast guard, transport, intelligence, and cyber agencies, and incidents that cross jurisdictions can fall between them. Clear coordination mechanisms, designated points of contact, and shared situational awareness help to avoid gaps. Legislation that enables information sharing with the private sector while protecting privacy and commercial confidentiality is an important enabler. Reporting requirements for significant incidents provide data for analysis and improve collective understanding of threats. International cooperation is indispensable. Alliances and partnerships allow states to share intelligence, coordinate responses, conduct joint exercises, and develop common standards. Norms of responsible behavior, confidence-building measures, and mechanisms for communication during crises can reduce the risk of misunderstanding. Nye (2017) argues that deterrence in cyberspace works through multiple mechanisms, including denial, entanglement, norms, and the threat of punishment, rather than through punishment alone. Maritime states, many of which depend on open and secure sea lanes, share an interest in strengthening such mechanisms and in promoting behavior that preserves the integrity of the maritime commons.

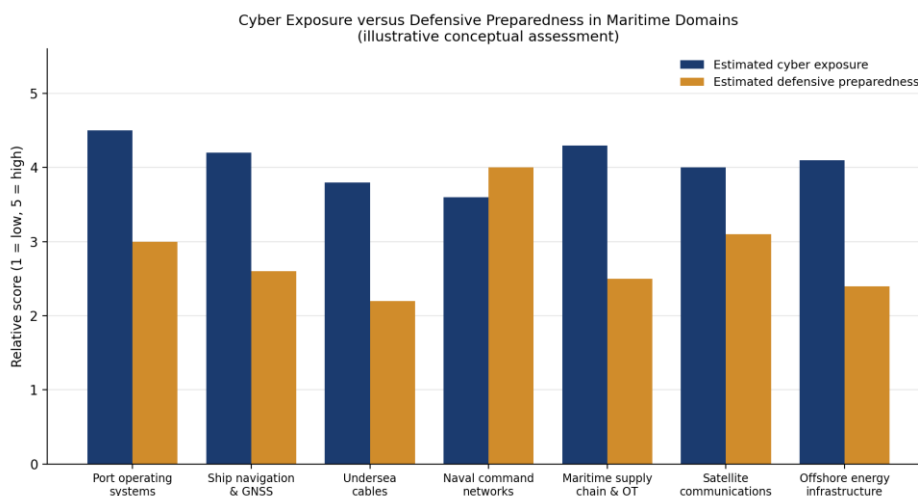
Naval Operations, Deterrence, and Strategic Stability:

For navies, cyber threat intelligence is integral to operations. Modern warships are networked systems of sensors, weapons, communications, and propulsion, and their effectiveness depends on trusted data and secure links. Intelligence about adversary cyber capabilities informs design, operations, and tactics, including how to operate when networks are contested. Navies must also consider their dependence on shore infrastructure, such as ports, logistics, and maintenance systems, which are often managed by civilian organizations and may be more exposed than the ships themselves. Training and exercises should reflect the expectation that cyber interference will be part of any serious conflict. Deterrence in cyberspace is difficult because attribution can be uncertain, thresholds are ambiguous, and effects can be unpredictable. Nye (2017) emphasizes that denial by building resilient systems that reduce the benefit of attack, and entanglement through interdependence that raises the costs of aggression, are important complements to retaliation. Healey (2013) documents the history of conflict in cyberspace and shows how states have adapted their approaches over time. For maritime states, credible resilience, together with the capacity to respond across domains, contributes to deterrence by convincing adversaries that cyber operations will not deliver decisive advantage. Strategic stability is a

further concern. Intelligence collection and pre-positioning in adversary systems may be defensible as preparation, yet may be perceived as hostile, particularly when directed at command and control or critical infrastructure. Buchanan (2017) warns that such dynamics can produce spirals of insecurity. Maritime states should therefore weigh the benefits of intrusive intelligence against its risks, develop channels for crisis communication, and consider restraint measures concerning especially sensitive systems such as nuclear command and control and civilian safety-critical infrastructure.

Capacity Building, Workforce, and Future Directions:

Capacity building is a long-term challenge. Skilled analysts, engineers, and operators are scarce, and the maritime sector competes with other industries for talent. Education programs that combine maritime knowledge with cyber expertise are limited, and many seafarers and port workers have received little formal cyber training. Maritime states should invest in specialized curricula, professional development, and career paths in both military and civilian organizations, and should encourage cooperation among universities, industry, and government in research and training. Smaller and developing maritime states may require external assistance, which also serves the collective interest because weak links in the global maritime network can expose all participants. Technological developments will reshape both threats and defenses. Autonomous and remotely operated vessels will increase dependence on communications and software, raising the stakes of cyber security. Artificial intelligence may assist both attackers and defenders, accelerating discovery of vulnerabilities and automating detection and response. Quantum computing may eventually undermine current cryptographic methods, creating a need for long-term planning for migration to quantum-resistant approaches. Increased use of satellite constellations, offshore renewable energy, and digital ports will add new dependencies and attack surfaces that should be considered during design rather than after deployment. Future research should examine the effectiveness of different information sharing models in the maritime sector, methods for assessing and communicating systemic risk, the interplay of cyber and physical threats to undersea and offshore infrastructure, and the strategic effects of intelligence activities on stability. Empirical studies of incidents, including lessons from exercises, are needed to move beyond speculation. Collaboration among practitioners and scholars in security studies, engineering, law, and maritime affairs will be essential to develop approaches that protect the maritime commons while sustaining the openness on which maritime prosperity depends.



Summary:

Cyber threat intelligence has become indispensable for maritime states seeking to protect national security in an increasingly digital maritime environment. The analysis shows that threats extend across ports, ships, offshore energy, undersea cables, and satellite-enabled systems, that actors and motives are diverse and difficult to attribute, and that effective defense depends on intelligence that is timely, relevant, and shared across government, industry, and allies. Legal ambiguity, fragmented responsibilities, and the cybersecurity dilemma add further complexity to policy and operations. The conceptual graph in this article suggests that the largest gaps between exposure and preparedness lie in undersea infrastructure, navigation systems, offshore energy, supply chain and operational technology, and port systems, and it should be read as an illustrative framework rather than a measurement. Recommendations include integrating cyber risk into maritime safety and security management, building trusted two-way intelligence sharing between public and private actors, investing in resilience and the ability to operate in degraded conditions,

strengthening international norms and cooperation, and developing a skilled workforce. Pursued together, these measures can help maritime states safeguard their security and prosperity without contributing to instability.

References:

- Bueger, C., & Edmunds, T. (2017). Beyond seablindness: A new agenda for maritime security studies. *International Affairs*, 93(6), 1293–1311.
- Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.
- Healey, J. (Ed.). (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80–106.
- International Maritime Organization. (2017). Resolution MSC.428(98): Maritime cyber risk management in safety management systems. International Maritime Organization.
- Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404.
- Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.
- Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.
- Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy*. The MITRE Corporation.
- Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18, 129–163.
- Till, G. (2018). *Seapower: A guide for the twenty-first century* (4th ed.). Routledge.
- Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212–233.